



E-Notice

2014-CH-15338

CALENDAR: 11

To: DRINKER BIDDLE REATH LLP
191 N WACKER#3700
CHICAGO,, IL 60606

NOTICE OF ELECTRONIC FILING

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS

MARTINEZ FREDDY vs. CHICAGO POLICE DEPARTMENT
2014-CH-15338

The transmission was received on 07/02/2015 at 12:12 PM and was ACCEPTED with the Clerk of the Circuit Court of Cook County on 07/02/2015 at 1:36 PM.

ANSWER/RESPONSE/REPLY (Plaintiff's Response to Defendant's Motion to Dismiss)

EXHIBITS (Exhibit 1)

EXHIBITS (Exhibit 1-A (Part 1))

EXHIBITS (Exhibit 1-A (Part 2))

EXHIBITS (Exhibit 1-A (Part 3))

EXHIBITS (Exhibit 1-A (Part 4))

EXHIBITS (Exhibit 1-A (Part 5))

EXHIBITS (Exhibit 1-B)

EXHIBITS (Exhibit 1-C)

EXHIBITS (Exhibit 1-D)

EXHIBITS (Exhibit 1-E)

EXHIBITS (Exhibit 1-F)

EXHIBITS (Exhibit 1-G)

EXHIBITS (Exhibit 1-H)

EXHIBITS (Exhibit 1-I)

EXHIBITS (Exhibit 1-J)

EXHIBITS (Exhibit 1-K)

EXHIBITS (Exhibit 1-L)

EXHIBITS (Exhibit 1-M)

EXHIBITS (Exhibit 1-N)
EXHIBITS (Exhibit 1-O)
EXHIBITS (Exhibit 1-P)
EXHIBITS (Exhibit 1-Q)
EXHIBITS (Exhibit 1-R)
EXHIBITS (Exhibit 1-S)
EXHIBITS (Exhibit 1-T)
EXHIBITS (Exhibit 1-U)
EXHIBITS (Exhibit 1-V)
EXHIBITS (Exhibit 1-W)
EXHIBITS (Exhibit 1-X)
EXHIBITS (Exhibit 1-Y)
EXHIBITS (Exhibit 1-Z)
EXHIBITS (Exhibit 1-AA)
EXHIBITS (Exhibit 1-AB)
EXHIBITS (Exhibit 1-AC)
EXHIBITS (Exhibit 1-AD)
EXHIBITS (Exhibit 1-AE)
EXHIBITS (Exhibit 1-AF)
EXHIBITS (Exhibit 1-AG)
EXHIBITS (Exhibit 1-AH)
EXHIBITS (Exhibit 1-AI)
EXHIBITS (Exhibit 1-AJ)
EXHIBITS (Exhibit 1-AK)
EXHIBITS (Exhibit 1-AL)
EXHIBITS (Exhibit 1-AM)
EXHIBITS (Exhibit 1-AN)
EXHIBITS (Exhibit 1-AO)
EXHIBITS (Exhibit 1-AP)
EXHIBITS (Exhibit 1-AQ)
EXHIBITS (Exhibit 1-AR)
EXHIBITS (Exhibit 1-AS)
EXHIBITS (Exhibit 1-AT)
EXHIBITS (Exhibit 1-AU)
EXHIBITS (Exhibit 2)
EXHIBITS (Exhibit 2-A)
EXHIBITS (Exhibit 2-B)

EXHIBITS (Exhibit 2-C)
EXHIBITS (Exhibit 2-D)
EXHIBITS (Exhibit 3)
EXHIBITS (Exhibit 4)
EXHIBITS (Exhibit 5)
EXHIBITS (Exhibit 6)
EXHIBITS (Exhibit 7)
EXHIBITS (Exhibit 8)
EXHIBITS (Exhibit 9)
EXHIBITS (Exhibit 10)

Filer's Email: matt@loevy.com
Filer's Fax: (312) 243-5902
Notice Date: 7/2/2015 1:36:57 PM
Total Pages: 1024

DOROTHY BROWN
CLERK OF THE CIRCUIT COURT
COOK COUNTY
RICHARD J. DALEY CENTER, ROOM 1001
CHICAGO, IL 60602

(312) 603-5031
courtclerk@cookcountycourt.com

FREDDY MARTINEZ,)	
)	
Plaintiff,)	2014 CH 15338
)	
v.)	Hon. Kathleen Kennedy
)	
CHICAGO POLICE DEPARTMENT,)	
)	
Defendant.)	

PLAINTIFF'S RESPONSE TO DEFENDANT'S MOTION TO DISMISS

The legislature and courts of this state have consistently and repeatedly made clear that left unchecked, government will operate in secrecy to the detriment of the public. Efforts by government generally, and the CHICAGO POLICE DEPARTMENT specifically, to hide information from the public based on conclusory affidavits and expansive interpretations of FOIA exemptions have been firmly and loudly rejected by reviewing courts and lawmakers alike. Despite the overwhelming weight of authority establishing these principles, CPD asks this Court to dismiss this case, without the opportunity for any discovery, on the basis of generic, one-size-fits-all affidavits and in derogation of the requirement that exemptions be read narrowly and in light of the statutory presumption of disclosure.

It falls to this Court to uphold the important principle that access to information under FOIA “is necessary to enable the people to fulfill their duties of discussing public issues fully and freely, making informed political judgments and monitoring government to ensure that it is being conducted in the public interest.” 5 ILCS 140/1. While CPD, the FBI, and Harris Corporation summon the frequent bogeymen of “national security” and “terrorism,” this Court may not and must not accept these bare assertions, which are devoid of supporting detail,

contradicted by a wealth of public information and expert testimony, and made before MARTINEZ has had any opportunity to conduct discovery to test the veracity of the claims. It is not in spite of, but especially because of, the nature of the surveillance at issue in this case and the possibility of abuse by CPD (a department with a long history of illegal and unconstitutional surveillance), that these principles of transparency must be upheld.

I. LEGAL STANDARDS

A. Motions to Dismiss Under 2-619

A Section 2-619 motion to dismiss is “a drastic means of disposing of litigation and should be allowed only when the right of the moving party is clear and free from doubt.” *Levine v. Ebi, LLC*, 2013 IL App (1st) 121049, ¶ 19 (reversing dismissal order). A Section 2-619 motion requires that the movant admit the plaintiff’s well-pled allegations and all reasonable inferences from those allegations. *McMackin v. Weberpal Roofing, Inc.*, 2011 IL App (2d) 100461, ¶ 19. The motion must be denied where there is a genuine issue of material fact. *E.g., Springfield Heating and Air Conditioning, Inc. v. 3947-55 King Drive at Oakwood LLC.*, 387 Ill. App. 3d 906, 909 (2009). All evidence and pleadings must be taken in the light most favorable to the non-movant. *E.g., McMackin*, 2011 IL App (2d) 100461, ¶ 19. Where the relevant facts are solely within a defendant’s knowledge, “a complaint which is as complete as the nature of the case allows is sufficient,” and discovery should be permitted. *Yuretich v. Sole*, 259 Ill. App. 3d 311, 313 (1994) (reversing order granting motion to dismiss).

B. Freedom of Information Act

The General Assembly and Illinois courts have long recognized that government secrecy is rarely appropriate and often abused:

We are not surprised that governmental entities, including the United States Attorney generally prefer not to reveal their activities to the public. If this were not a truism, no FOIA would be needed. Our legislature enacted the FOIA in

recognition that (1) blanket government secrecy does not serve the public interest and (2) transparency should be the norm, except in rare, specified circumstances. The legislature has concluded that the sunshine of public scrutiny is the best antidote to public corruption, and Illinois courts are duty-bound to enforce that policy.

Better Gov't Ass'n v. Blagojevich, 386 Ill. App. 3d 808, 818 (2008) (requiring disclosure of federal grand jury subpoenas).

Because of this truism, the FOIA statute and interpreting caselaw impose a demanding standard on public bodies seeking to keep records from the public, no matter what the exemption or the nature of the issues. First, every public record is presumed by law to be open to the public, and so a public record may only be withheld if a specific statutory exemption applies and is proven by clear and convincing evidence. 5 ILCS 140/1.2; *Day v. City of Chicago*, 388 Ill. App. 3d 70, 73 (2009) (reversing trial court order granting motion to dismiss and collecting cases setting forth demanding standard to withhold records). Second, a public body asserting an exemption must “provide a detailed justification for its claimed exemption, addressing the requested documents specifically and in a manner allowing for adequate adversary testing.” *Id.* at 74 (quoting and citing *Ill. Ed. Ass'n v. Ill. State Bd. of Ed.*, 204 Ill. 2d 456, 464 (2003)). Public bodies may not treat exemption language “as some talisman, the mere utterance of which magically casts a spell of secrecy over the documents at issue. Rather, the public body can meet its burden only by providing some objective indicia that the exemption is applicable under the circumstances.” *Id.* at 75. In *Day*, for example, the Illinois Appellate Court reversed the trial court for accepting inadequate affidavits from multiple CPD officials:

The three affiants also fail to explain how disclosure of any of the documents at issue would specifically obstruct the remaining investigation of Irving's murder. It is impossible to tell from the affidavits whether the investigation into aspects of the crime “other than Mr. Day's arrest and conviction” is actually “pending,” as required by section 7(1)(c)(i). ***

Although Lieutenant Gibson said “seemingly innocuous information may prove

valuable to an at-large perpetrator in discerning the nature of the ongoing police investigation,” he never suggested in his affidavit that a specific living “at-large perpetrator” is currently under active investigation. Simply saying there is an “ongoing criminal investigation because the case has not been cleared,” with little additional explanation, is not “objective indicia” sufficient to show the ongoing investigation exemption applies.

The sweeping generalities found in McCarthy’s, Sandoval’s, and Lieutenant Gibson’s affidavits are not the type of “detailed justifications” that lend themselves to “adequate adversary testing” necessary to support the claimed ongoing-investigation exemption. We do not see the “detailed explanation” found by the trial court.

Id. at 76-77 (internal citation omitted). The Appellate Court made clear, in no uncertain terms, that granting a motion to dismiss based on such deficient affidavits is reversible error:

These affidavits are one-size-fits-all, generic and conclusory. ***

That is rubber stamp judicature. We decline to take part in it. The City is asking us, as it did the trial court, to take the affiants’ word for it. For us to do so would be an abdication of our responsibility.

Id. at 80.

In addition to the requirement that the government prove every exemption claim for every record by clear and convincing evidence with a detailed factual justification, the government must also prove that it undertook a “thorough search” for responsive records and either produced or asserted an exemption over each one. *BlueStar Energy Servs., Inc. v. Ill. Commerce Comm’n*, 374 Ill. App. 3d 990, 996-97 (2007). It must identify the “search terms and the type of search performed” and “identify the searched files and describe at least generally the structure of the agency’s file system which renders any further search unlikely to disclose additional relevant information.” *El Badrawi v. Dept. of Homeland Security*, 583 F. Supp. 2d 285, 298 (D. Conn. 2008). A search must be “reasonably calculated to uncover all relevant documents.” *Tarullo v. U.S. Dept. of Defense*, 170 F. Supp. 2d 271, 274 (D. Conn. 2001).

II. HISTORY OF ILLEGAL SURVEILLANCE BY CPD

This case involves CPD's efforts to keep secret information about its use of powerful surveillance equipment with the potential for significant abuse. CPD's arguments cannot be viewed in isolation, but must be considered in their proper context.

For decades, CPD and the FBI targeted law-abiding people and organizations for illegal surveillance and infiltration because of their political activities. As described by the Seventh Circuit:

From the 1920s to the 1970s the intelligence division of the Chicago Police Department contained a unit nicknamed the 'Red Squad' which spied on, infiltrated, and harassed a wide variety of political groups that included but were not limited to left- and right-wing extremists. Most of the groups *** were not only lawful, and engaged in expressive activities protected by the First Amendment, but also harmless.

Alliance to End Repression v. City of Chicago, 237 F.3d 799, 801 (7th Cir. 2001).¹ CPD's targets included social workers, clergy, churches, and peace organizations engaged in legal and Constitutionally protected activities. *Alliance to End Repression v. City of Chicago*, 561 F. Supp. 537, 540, 570 (N.D. Ill. 1982); *Alliance to End Repression v. City of Chicago*, 627 F. Supp. 1044, 1046 (N.D. Ill. 1985). CPD recorded its targets, compiling 1,760 reports on the Chicago Peace Council alone, and distributed false information and testimony to newspapers and the government about them. *Alliance to End Repression*, 627 F. Supp. at 1046-47, 1051.

CPD and its Red Squad also infiltrated target organizations by sending informants to join the groups, take executive and board member positions, and participate in the groups' top-level decisions and even their legal teams. *Id.* at 1046; *Alliance to End Repression v. Rochford*, 75 F.R.D. 435, 437 (N.D. Ill. 1976). When CPD's informants learned about the planned suit, CPD

¹ "Courts may take judicial notice of matters which are commonly known or of facts which, while not generally known, are readily verifiable from sources of indisputable accuracy." *People v. Brown*, 2015 IL App (1st) 122940, ¶ 86, reh'g denied (May 12, 2015).

destroyed documents. *Alliance to End Repression*, 75 F.R.D. at 440. In 1982, a federal district court entered a sweeping and long-lasting consent decree “imposing detailed restrictions on the CPD’s investigative activities.” *ACLU of Ill. v. City of Chicago*, No. 75 C 3295, 2008 WL 4450304, at *1 (N.D. Ill. Sept. 30, 2008). Among other things, the decree barred “systematic investigation and record keeping about political and social action organizations unrelated to criminal conduct.” *Alliance to End Repression*, 561 F. Supp. at 561. The decree remained in effect for nearly three decades, dissolving just six years ago, and as late as 2008, Judge Gottschall of the Northern District of Illinois wrote:

In a post-9/11 world, government investigations of the activities of citizens and groups have gained new purchase, with concomitant concerns for the free exercise of civil liberties guaranteed by the Constitution. Although the specific activities by the CPD’s disbanded “Red Squad” that gave rise to the original consent decree and the MCD belong to the past, the needs of the people to be protected from organized and systematic surveillance of their lawful activities, as well as from illegal harassment and arrest based upon lawful political associations, remain a source of vital concern to the court and to the country in general.

ACLU of Ill., 2008 WL 4450304, at *4 n.3.

CPD’s surveillance operations have not ended. Records that MARTINEZ obtained from CPD under FOIA indicate that CPD in fact continues to conduct intelligence operations into political groups, including groups protesting police misconduct. Ex. 1-A; *see also* Ex. 1-B. As discussed in the following section, many people, organizations, and United States Senators are concerned about the use of cell site simulators and fear that cell site simulators can be used to create databases identifying people who attend political protests, among other Constitutionally troubling practices.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 6 of 31

III. CELL SITE SIMULATORS AND THEIR CONTROVERSIAL USE AND DETERIORATING SECRECY

While CPD, Harris, and local and federal law enforcement agencies around the country have gone to great lengths to conceal information about cell site simulators² and how they are being used, details have slowly emerged. There is no real dispute that the equipment is being widely deployed and allows for the interception of cell phone communications and location tracking. Ex. 1-C; Ex. 1-D. Cell site simulators force devices up to several kilometers away to disclose their subscriber IDs and other information to the police without the knowledge or consent of the device's owner. Ex. 1-E at 2-3; Ex. 1-C; Ex. 1-D; Ex. 1-F; Ex. 1-G; Ex. 1-H; Ex. 1-I. Police also appear to be using cell site simulators to capture the content of cellular communications. Ex. 1-J at 6; Ex. 1-K; Ex. 1-F. Law enforcement is even deploying cell site simulator technology in the U.S. on airplanes flown over major U.S. cities to collect data. Ex. 1-L; Ex. 1-M.

To operate, a simulator mimics a legitimate cellular tower and sends commands to all devices in a given area that force devices to disclose their subscriber IDs to the simulator, and thus, to the police. Ex. 1-J at 11-13; *see also* Ex. 1-F; Ex. 1-N; Ex. 1-O. What law enforcement agencies, including CPD, do with the data that they collect is being hidden from the public, making it impossible to have a robust public debate on an issue with serious First and Fourth Amendment and Illinois statutory privacy implications. *Riley v. California*, 134 S. Ct. 2473, 2494-95 (2014) (“Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans ‘the privacies of life,’ *Boyd, supra*, at 630, 6 S.Ct. 524. The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for

² “Stingray” is the commercial name for a popular Harris cell site simulator but has become a generic term for any cell site simulator. This brief uses the terms interchangeably.

which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.”); *Tracey v. Florida*, 152 So.3d 504, 524 (Oct. 16, 2014) (“We cannot overlook the inexorable and significant fact that, because cell phones are indispensable to so many people and are normally carried on one’s person, cell phone tracking can easily invade the right to privacy in one’s home or other private areas, a matter that the government cannot always anticipate and one which, when it occurs, is clearly a Fourth Amendment violation.”); 725 ILCS 168 (prohibiting use of location tracking without a probable-cause warrant).

A publicly available police training manual purchased online provides substantial technical details of how cell site simulators work and are used based on information that the author describes as “publicly available” and not “law enforcement sensitive techniques”:

Cell phone tracking and the use of site emulators are commonly known within our field by the code word ‘Triggerfish’ or ‘Stingray.’ The equipment works by emulating a cell tower and querying the particular serial number of a given device and measuring the signal strength to the device. This allows the operators to locate the device and, hopefully, its user. *** Depending on the configuration, the equipment is also capable of capturing the unique serial numbers of all devices in a certain area. This assists investigators to isolate a suspect’s previously unknown cell device.

To be used effectively, Triggerfish relies on an operational pen register to locate the cell tower and sector the device most recently used. The Triggerfish team will then go to the area the cell phone sector covers and try to locate the device. In my experience, the equipment is extremely accurate but relies on skilled technicians operating the device, a responsive and competent surveillance element, some degree of intelligence regarding the suspect’s associates, and an active cell phone associated with your target.

Ex. 1-P; *see also*, e.g., Ex. 1-I; Ex. 1-J.

Use of cell site simulators appears to be very widespread across the country and growing. Recently released information indicates that the Baltimore police deployed stingrays 4,300 times in less than a decade. Ex. 1-Q. The ACLU identified over 1,800 uses of stingrays by the subset

of Florida law enforcement agencies for whom information was available. Ex. 1-R. The criminal cases that have brought stingrays to the public's attention have not been cases of national security. Ex. 1-Q; Ex. 1-S; Ex. 1-T. At least one Florida police department purchased cell site simulators on an "emergency" no-bid basis for the purpose of spying on political activists. Ex. 1-U.

Secrecy around stingrays has extended even to law enforcement representations to the courts. Judges in Tacoma, Washington learned in 2014 that they had been unknowingly "authorizing" stingray use; the pen register applications presented to them by Tacoma detectives contained no mention of stingray technology. Ex. 2 at ¶ 13; *see also* Ex. 1-V. The federal government has sought court authorization for stingray operations without informing judges of its intent to use stingrays and without explaining the technology. Ex. 1-E at 9-19. Documents show that the U.S. Marshals office instructed police in Florida not to provide courts with information on stingrays, and police there falsely referred to obtaining information from use of stingray surveillance as having been "received information from a confidential source regarding the location of a suspect." Ex. 1-W. Law enforcement officials are even letting accused criminals go free or plead to reduced sentences rather than disclose details about the role that cell site simulators played in an investigation. Ex. 2 at ¶ 14; *see also* Ex. 1-F; Ex. 1-G; Ex. 1-Q.

Just a few months ago, the Committee on the Judiciary of the U.S. Senate sent a letter to the U.S. Attorney General and the Secretary of the Department of Homeland Security questioning the Constitutionality of the federal government's use of cell site simulator technology. Ex. 1-X ("[W]e are concerned about whether the FBI and other law enforcement agencies have adequately considered the privacy interests of other individuals who are not the targets of the interception, but whose information is nevertheless being collected when these

devices are being used.”). Senator Bill Nelson raised similar Constitutional and privacy concerns in an inquiry to the FCC. Ex. 1-Y.

Courts have also begun to address cell site simulator issues after years of law enforcement successfully keeping its practices secret. This year, a New York court ruled that Erie County should not have withheld or redacted documents about stingrays including the county’s purchase orders and justification memoranda, a procedural manual, and the county’s non-disclosure agreement with the FBI. *New York Civil Liberties Union v. Erie County Sheriff’s Office*, 47 Misc.3d 1201(A), 2015 N.Y. Slip Op. 50353(U), at **10-13 (S. Ct. of Erie County, NY March 17, 2015) (attached as Ex. 3). The court there held:

In essence, [the FBI’s] instructions are to conceal from the public the existence, technological capabilities, or uses of the device. Indeed, the Sheriff’s Office is instructed, upon the request of the FBI, to seek dismissal of a criminal prosecution (insofar as the Sheriff’s Office may retain influence over it) in lieu of making any possibly compromising public or even case-related revelations of any information concerning the cell site simulator or its use. If that is not an instruction that affects the public, nothing is.

Id. at *11. In another decision, a North Carolina judge, upon a newspaper’s petition and with the eventual consent of local police, unsealed applications made to judges by local police in hundreds of criminal cases involving stingray use; the applications were shown to contain only boilerplate language about phone data, and no specific reference to stingray technology. Ex. 1-Z; Ex. 1-AA. Charlotte Police will now disclose greater information about stingray use and will routinely unseal court orders in closed cases. Ex. 1-AB. Last year, a federal court in California ordered the release of portions of a manual for federal prosecutors entitled “Electronic Surveillance Non-Wiretap.” *ACLU of N. Cal. v. Dept. of Justice*, 12-cv-04008-MEJ, 2014 WL 4954277, at *12 (N.D. Cal. Sept. 30, 2014). That same court recently ordered the release of a sealed order for stingray use and information regarding how the federal government is using stingrays. *ACLU of N. Cal. v. Dept. of Justice*, No. 13-cv-03127-MEJ, 2015 WL 3793496, at

**1, 15 (N.D. Cal. June 17, 2015).

While law enforcement and Harris have attempted to impose near-total secrecy over cell site simulator usage, Harris and others have disclosed substantial information in their publicly available patent filings as part of efforts to obtain patent protection for these devices. The patent laws require that an inventor disclose sufficient information about an invention to allow one of skill in the relevant field to make and use the invention.³ A search of Google's online database of U.S. and foreign patents and applications for the term "IMSI catcher" produced 94 results. Ex. 1-AC. Harris owns a number of patents that appear to relate to cell site simulators, including at least:

"Multi-Channel Cellular Communications Intercept System," which claims in its abstract to be a "multi-channel cellular communications intercept system for monitoring and then intercepting communications between a mobile unit and a base station in one cell of a cellular telephone system";

"Remote Mobile Monitoring and Communication System," which claims in its abstract to be a "system and method for monitoring the location and/or presence of an object/person within a desired area" using a "mobile base station" that "may be transported to an arbitrary site";

"Apparatus and Method for Tracking and Communicating with a Mobile Radio Unit," which claims in its abstract to facilitate "determining the location of at least one mobile radio unit and displaying on a computer display an object identifier corresponding to the mobile radio unit";

"Wireless Communications System Including a Wireless Device Locator and Related Methods," which claims in its abstract to use "a plurality of location finding signals to target [a] wireless communications device from among" other devices; and

³ 3 Annotated Patent Digest § 20:42 ("Under the first prong of the enablement requirement, the patent specification must provide sufficient teaching so one of skill in the art can make the claimed invention.") (attached as Ex. 4); 3 Annotated Patent Digest § 20:44 ("As the second prong of the enablement requirement, a patent specification must teach one of skill in the art how to use the claimed invention.") (attached as Ex. 5); The Choice Between Patent Protection and Trade Secret Protection: A Legal and Business Decision, 84 J. Pat. & Trademark Off. Soc'y 371, 377 (2002) ("Patent and trade secret law can be viewed as alternative bodies of law for protecting certain types of inventions. Consequently, an inventor will often have to make a choice or election between the type of protection to rely on.").

“Communication Network for Detecting Uncooperative Communications Device and Related Methods,” which states in its Background of the Invention that “[i]n government, municipal, and law enforcement applications, there is sometimes a desire to track a communications device,” and describes a number of existing systems over which the invention claims to be an improvement.

Ex. 1-AD - Ex. 1-AH. Thus, it appears that Harris and others have disclosed a significant amount of highly technical information for their own purposes already, notwithstanding the parade of horrors that CPD and Harris claim would result.

IV. GLOBAL FAILURES BY CPD TO MEET ITS BURDEN

A. CPD Has Not Established An Adequate Search For Records

Especially given the nature of the records at issue, it is crucial that CPD conduct a thorough search for records, as the law requires. To support its claim that it performed a sufficient search, however, CPD relies solely on the affidavit of Sergeant Costa. The affidavit states that Costa has only been in his Tech Lab assignment since August 2012, yet records produced under FOIA indicate that CPD first acquired cell site simulators in 2005. Exhibit 1-AI. Costa did not speak with any of his predecessors or otherwise do anything to determine where further records might be located. Inadequate recordkeeping controls at CPD have been well documented, including the storage of critical files in obscure basement locations and the homes of individual officers.⁴

In addition, the Costa affidavit makes clear that the Tech Lab is limited to equipment

⁴ *Fields v. City of Chicago*, No. 10 C 1168, 2014 WL 477394, at *6-7 (N.D. Ill. Feb. 6, 2014) (“The term [‘street files’] is a reference to a practice that the Chicago Police Department once had of maintaining investigative records that were withheld from the state’s attorney and therefore unavailable as a source of exculpatory information that might induce him not to prosecute or, failing that, would at least be available to defense counsel under *Brady v. Maryland*[.] The practice was supposedly eliminated by police department internal rules just before Fields’s first trial. . . . During discovery in the present case, however, a file of over a hundred pages of police reports concerning the Smith/Hickman murders was located in a nondescript file cabinet at the Area 1 police station, along with files relating to other murders.” (internal quotation omitted)); Ex. 1-AJ at 110 n.649 (“In response, according to Walsh, he then locked the file in a cabinet in his Area 3 office and later took the file home and placed it in his personal safe for some period of time, until William Bazarek (First Assistant General Counsel to CPD) told him that keeping an original homicide file at his home was not a good decision.”); *id.* at 110 n.648 (describing long-missing files in Koschman investigation).

“used by the various divisions within the Bureau of Organized Crime,” that the search was limited to “the Tech Lab’s files for documents relating to cell site simulator equipment and the possible deployment of such devices by CPD officers,” and that Costa was only asked to locate documents “in the Tech Lab’s possession.” CPD Memo. at 4; CPD Memo. Ex. 3. No explanation is provided for why other repositories were not searched, such as each BOC division, the top CPD leadership, the CPD legal department, other operational departments (including but not limited to those responsible for First Amendment sensitive investigations) and unsanctioned repositories. Ex. 1-AK. While Costa’s affidavit states that “to the best of my knowledge, CPD Bureaus other than the Bureau of Organized Crime do not possess cell site simulator equipment,” this statement is not at all definitive and is unsurprising given that Costa’s experience with the equipment is limited to the BOC, rendering CPD’s logic completely circular. Moreover, Costa’s affidavit admits that it leaves out undisclosed relevant facts about CPD’s search for records. CPD Memo. Ex. 3 at ¶ 6. Because CPD failed to establish a thorough search for records, its motion to dismiss must be denied.

B. The Affidavits Should Be Categorically Rejected As Inadequate To Establish Any Exemption Claims⁵

Courts have repeatedly made clear that conclusory affidavits do not establish FOIA exemptions. Despite this clear and consistent caselaw (including caselaw criticizing CPD specifically), CPD does not provide a single affidavit from anyone knowledgeable about any CPD investigations or use of cell site simulator equipment. Rather, CPD relies solely on the affidavits of an FBI agent based in Virginia and a Harris employee apparently responsible for sales to attempt to establish its exemption claims. Costa’s affidavit—the only CPD affidavit—is limited to discussing the search for responsive records and does not address the factual predicates

⁵ This section is limited to the facial invalidity of the affidavits. Contradictory evidence is addressed in the specific sections below.

for any of the claimed exemptions. No further analysis is required to deny CPD's motion because exemption claims must be proven by clear and convincing evidence through detailed affidavits. 5 ILCS 140/1.2; *Day*, 388 Ill. App. 3d at 73.

As for Morrison's affidavit, it is replete with flaws and conclusory claims lacking foundation. Morrison states that the FBI "has always asserted that cell site simulators are exempt from discovery" and discusses what the FBI has done "as a matter of policy." CPD Memo. Ex. 5 at ¶¶ 3, 5. Contrary to the implication of these statements, the FBI is not the law, and the positions it takes and policies it promulgates are irrelevant to what the Illinois FOIA requires. And as discussed above, the Senate Judiciary Committee has questioned the FBI's practices.

Further, Morrison's affidavit is not specific to the particular equipment owned by CPD or the way in which CPD has deployed it, and there is no indication that he is even aware of the specific equipment at issue or has ever spoken to anyone at CPD about anything. Morrison nonetheless makes the conclusory claim that "disclosure of what appears to be innocuous information about the use of cell site simulators would provide adversaries with critical information" that would allow them to "take countermeasures designed to thwart the use of this technology" and makes a completely unexplained and unproven claim of "national security." *Id.* at ¶¶ 4, 6. These broad, conclusory, unsubstantiated, "take-my-word-for-it" claims are nearly identical to those soundly rejected by the Appellate Court in *Day*, the acceptance of which would amount to "rubber stamp judicature." 388 Ill. App. 3d at 76 (rejecting conclusory statement by police officer that "seemingly innocuous information may prove valuable to an at-large perpetrator in discerning the nature of the ongoing police investigation").

Nor are Morrison's talismanic conclusions about what qualifies as "homeland security information" or "US munitions" up to the standards of *Day*. In fact, there is no indication of his

qualifications even to make these statements, particularly given that the FBI has no jurisdiction over export controls and that the affidavit attaches no supporting evidence for its legal conclusions. Ex. 1-AL. Finally, and clearly demonstrating the boilerplate nature of the affidavit, Morrison has submitted nearly identical affidavits in other cases in other states, including in the Erie County case in which the court ordered the release of information. Ex. 1-AM.

CPD also relies on an affidavit submitted by Harris Corporation—the company who profits from the sale of cell site simulators and has made clear that its motivation is to inhibit competition, to the detriment of taxpayers, in the market for equipment claimed to be essential to national security. CPD cites to no authority applying a presumption of good faith to the affidavits of private, profit-motivated companies with a clear bias in suppressing information for commercial reasons.⁶ Moreover, trade secret claims are highly fact intensive and generally unsuitable for resolution by way of affidavits or dispositive motions. *See Learning Curve Toys, Inc. v. PlayWood Toys, Inc.*, 342 F.3d 714, 723 (7th Cir. 2003) (“The existence of a trade secret ordinarily is a question of fact [and] requires an ad hoc evaluation of all the surrounding circumstances. For this reason, the question of whether certain information constitutes a trade secret ordinarily is best ‘resolved by a fact finder after full presentation of evidence from each side.’” (internal citations omitted)).

Even if the Harris affidavit was entitled to any weight, it is replete with fatal problems.

⁶ 5 U.S.C. § 552(a)(4)(B) (“In addition to any other matters to which a court accords substantial weight, a court shall accord substantial weight to an affidavit of an agency concerning the agency’s determination as to technical feasibility under paragraph (2)(C) and subsection (b) and reproducibility under paragraph (3)(B).”) (emphasis added); *BlueStar Energy Servs., Inc.*, 374 Ill. App. 3d at 997 (“Affidavits submitted by an agency are accorded a presumption of good faith.”) (quoting and citing *Carney v. U.S. Dept. of Justice*, 19 F.3d 807, 812 (2d Cir. 1994) (internal quotation omitted)); *Matter of Wade*, 969 F.2d 241, 246 (7th Cir. 1992) (discussing when “[g]overnment affidavits” are “sufficient to sustain claims of document exemption.”); *ACLU v. U.S. Dept. of Defense*, 628 F.3d 612, 619 (D.C. Cir. 2011) (describing when an “agency’s affidavit” can provide the basis for summary judgment). Further, for the purposes of preserving a related issue for appeal, MARTINEZ contends that *BlueStar* was improperly decided even as to government affidavits because it relied on federal cases that were relying on specific federal statutory language regarding this presumption that does not exist in the Illinois statute.

There is no foundation for Rimelli's purported expert opinion about the potential harm to Harris if the alleged trade secrets were disclosed or the "competitive advantage" that would be lost if even the "layout and ease-of-use of the user interface" was disclosed. Rimelli is not even an executive level employee and the affidavit is silent on his education and or other credentials that would allow him to make such broad expert claims. Nor does he provide any basis to opine upon export control regulations or to claim that executive decision makers at Harris would find it "difficult [but not impossible] for Harris to continue providing equipment to the CPD" if this Court orders release of any stingray information, which implausibly implies that Harris would give up hundreds of thousands of dollars in sales to CPD and put national security at risk if it does not get its way.

Because none of the affidavits meet the necessary standards, and because all of the exemption claims rely on the affidavits, CPD's motion to dismiss must be denied.

C. MARTINEZ Has Prevailed In Defeating CPD's Willful and Improper Refusal to State What Records Exist or Not

In its FOIA denial, CPD refused to disclose whether any records responsive to any requests even exist, thus leaving the public with no idea whether CPD has actually deployed any cell site simulators, analyzed Constitutional issues, obtained any court orders, or issued any policies and procedures to govern use of cell site simulators, etc. Compl. Ex. B at 1 ("Upon review, the City of Chicago has determined that your Request must be denied, as the requested records, to the extent they may exist, are exempt from release under the following provisions of the Illinois FOIA." (emphasis added)). Nothing in the Illinois FOIA statute permits a public body to refuse to state whether responsive records exist or to make exemption claims over hypothetical records. 5 ILCS 140/9.

In response to this litigation, CPD has finally acknowledged what records it has and does

not have, and those statements make clear that CPD has deployed cell site simulators, often in improper reliance on pen register orders that CPD refuses to produce, and that CPD has no policies or procedures to govern when the equipment may be used or any analysis of Constitutional issues associated with use of the equipment. CPD Memo. Ex. 3. By obtaining this information, MARTINEZ has at least partially prevailed, and will pursue his claims for attorney fees and civil penalties once issues regarding the production of records have been resolved. CPD's motion fails to address this issue in any way.

V. CPD HAS FAILED TO ESTABLISH ANY SPECIFIC EXEMPTION CLAIM

A. Request 1: "Documents sufficient to show, for each individual occurrence, when, where, how, why, and by whom Chicago Police deployed any devices commonly known as IMSI catchers"

CPD has identified as responsive to this request and allegedly exempt: (1) court orders and applications for court orders; (2) Harris manuals and guides; and (3) internal purchase justification memoranda. CPD has failed to establish any of its litany of exemption claims.

1. Court Orders and Applications

i. Pen Register Statute

CPD first argues that the court orders it obtained under the pen register statute were ordered to remain under seal. CPD Memo. at 6. CPD acknowledges that the orders need only remain under seal "until otherwise ordered by the court," yet CPD has refused to ask the issuing courts to remove the seals so that the orders and applications may be produced under FOIA (subject to any FOIA exemptions) or to produce enough of the orders to at least identify the courts and judges involved. CPD takes this position even though it does not contend that the orders contain information exempt under FOIA Section 7(1)(d)(i) (information that would "interfere with pending or actually and reasonably contemplated law enforcement proceedings"), and as such, there does not appear to be any basis for a continued seal. *See Skolnick v. Altheimer*

& Gray, 191 Ill. 2d 214, 230 (2000) (“The common law right of access to court records is essential to the proper functioning of a democracy[.]”) (internal citations omitted); *ACLU of N. Cal.*, 2015 WL 3793496, at **15-16 (ordering release of sealed federal stingray search warrant in closed investigation). To the extent there is discrete information within the orders and applications that is actually exempt, it can be redacted, but the public has an interest and right in learning, among other things, whether CPD has misled courts to obtain these orders and in what types of cases they are being used. *ACLU of N. Cal.*, 2015 WL 3793496, at *16.

In addition, the pen register statute upon which CPD relies is inapplicable to the use of cell site simulators, and the prohibition in that statute on disclosure of an “order authorizing or approving the installation and use of a pen register or a trap and trace device,” 18 U.S.C. 3123(d)(1), does not apply to the installation and use of a cell site simulator and so is irrelevant. A pen register is a device that records the numbers dialed by a particular telephone; a trap and trace device records the incoming numbers to a telephone. Ex. 2 at ¶ 8; Ex. 1-AN at 5-6. Cell site simulators, however, can capture a cell phone’s unique serial number, its location, and the content of calls, text messages, and web pages visited, all without the knowledge of the phone carrier. Ex. 2 at ¶¶ 9-12; Ex. 1-AO at 144-148. While pen registers and trap and trace devices only capture information from a single source, *In re the Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d 747, 750 (S.D. Tex. 2012), cell site simulators collect data from every other mobile device in range. Ex. 2 at ¶¶ 15-18; Ex. 1-AO at 145–46. Because the data-collecting abilities of cell site simulators so greatly exceed those of pen registers and trap and trace devices, court orders for pen registers and trap and trace devices are inappropriate to permit the use of cell site simulators. Ex. 2 at ¶ 20; *In re Pen Register & Trap & Trace Device*, 890 F. Supp. 2d at 752 (denying

government's application for pen register or trap and trace device for stingray because "a pen register does not apply to this type of electronic surveillance."); Ex. 2-C at 81-82 (stingray devices are ill-suited for "extremely low" pen register standard).

Further, the pen register statute authorizes orders issued to state law enforcement based on a mere relevance standard but only "unless prohibited by State law." 18 U.S.C. 3122(a)(1). The Illinois Constitution specifically protects the public from unreasonable "interceptions of communications by eavesdropping devices or other means" and states that "[n]o warrant shall issue without probable cause, supported by affidavit particularly describing the place to be searched and the persons or things to be seized." Ill. Const. Art. I, § 6. The Illinois Freedom From Location Surveillance Act, made effective as of August 26, 2014, states that

a law enforcement agency shall not obtain current or future location information pertaining to a person or his or her effects without first obtaining a court order based on probable cause to believe that the person whose location information is sought has committed, is committing, or is about to commit a crime or the effect is evidence of a crime, or if the location information is authorized under an arrest warrant[.]

725 ILCS 168/10. The secrecy provisions of the pen register statute are irrelevant.

ii. Unique or Specialized Investigative Techniques

CPD next contends that the orders and applications reveal "unique or specialized investigative techniques other than those generally used and known" under FOIA Section 7(1)(d)(v). The use of cell site simulators generally and by CPD specifically is well known, including the manner in which the devices operate. CPD concedes this, but argues that under *Catledge v. Mueller*, 323 Fed. Appx. 464 (7th Cir. 2009), this does not defeat its exemption claim. CPD Memo. at 6-7. To the contrary, the federal FOIA exemption at issue in that case was materially different from Section 7(1)(d)(v): there was no federal FOIA statutory requirement that the information show "unique or specialized investigative techniques other than

those generally used and known.” *Compare Catledge*, 323 Fed. Appx. at 466-467, with 5 ILCS 140/7(1)(d)(v). When the federal FOIA and state FOIA differ in material ways, Illinois courts do not follow federal decisions. *Better Gov’t Ass’n*, 386 Ill. App. 3d at 815 (For over 200 years, “Congress has not seen fit to specifically restrict the behavior of subpoena recipients. . . . [T]hose [federal] courts that have decided that Congress’ failure to act was the result of an oversight have taken it upon themselves to correct this oversight by judicially amending Rule 6(e)(2). We disagree with this course of action and decline to follow it.”). Nor do Illinois courts stray from the clear text of statutory exemptions. *Id.*; *Fagel v. Dep’t of Transp.*, 2013 IL App (1st) 121841, ¶ 35 (“[W]e agree with the circuit court’s observations that the function of the courts is to interpret the statute as it is written” despite any perceived policy concerns.); *Pritza v. Village of Lansing*, 405 Ill. App. 3d 634, 645 (2010) (court must not legislate where the language of the statute is plain and certain). As a federal court recently found with regard to similar federal records ordered to be produced, “the public in general knows that the government possesses and utilizes such cell phone technology in its investigations to locate and obtain information about the cell-phone holder,” and so the related federal exemption did not apply. *ACLU of N. Cal.*, 2015 WL 3793496, at **12-13.

Finally, CPD’s claims about supposed “countermeasures” is unfounded on the merits. As discussed above, the Morrison affidavit does not nearly meet the exacting standards set forth by the courts of this state. *Day v. City of Chicago*, 388 Ill. App. 3d 70, 73 (2009). Even if it did, however, both an expert affidavit and publicly available information make clear that technical countermeasures already exist and the release of the information typically found in pen register applications and orders would not tell criminals anything that is not already widely known. Ex. 1-AP; Ex. 2 at ¶¶ 27-28.

2. Harris Operator Manuals and Quick Reference Guide

i. Trade Secrets

CPD argues that every single word on every single page in every single Harris manual and guide provided to CPD is a trade secret, the release of which would result in significant competitive harm to Harris. In doing so, CPD contends that protecting Harris from competition is more important than the public's right to know the extent of electronic surveillance by a police department with a long history of illegal surveillance against political dissenters. CPD is wrong: trade secret protection is not absolute and must be balanced against the public interest in disclosure. *Alpha School Bus Co., Inc. v. Wagner*, 391 Ill. App. 3d 722, 740 (2009) (“The protection of trade secrets must be balanced against conflicting social and economic interests.”); *see also* Restatement (Third) of Unfair Competition § 39 (1995) (“The subject matter and scope of trade secret protection is necessarily limited by the public and private interest in access to valuable information.”); *cf. Pub. Citizen Health Research Grp. v. Food & Drug Admin.*, 704 F.2d 1280, 1288-89 (D.C. Cir. 1983) (narrowly defining “trade secret” under federal FOIA); *Anderson v. Dep’t of Health & Human Servs.*, 907 F.2d 936, 944 (10th Cir. 1990) (same). The public interest here is tremendous given the local and national interest (including the interest of the U.S. Senate Judiciary Committee) in monitoring government surveillance for Constitutional abuses.

Even if Harris’ commercial interests in secrecy outweighed the public’s interest in disclosure, the cited exemption only protects trade secrets that were “furnished [to the government] under a claim that they are proprietary, privileged or confidential.” 5 ILCS 140/7(1)(g). Harris claims only that it marked four of the manuals as confidential; the remaining responsive records are ineligible for protection under this exemption. CPD Memo. Ex. 4 at ¶ 3.

Moreover, CPD has failed to prove that the records qualify as trade secrets under Illinois law. Courts consider the following elements in determining what qualifies as a trade secret:

(1) the extent to which the information is known outside of the plaintiff's business; (2) the extent to which it is known by the employees and others involved in the plaintiff's business; (3) the extent of measures taken by the plaintiff to guard the secrecy of the information; (4) the value of the information to the plaintiff and to the plaintiff's competitors; (5) the amount of effort or money expended by the plaintiff in developing the information; and (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.

Alpha School Bus, 391 Ill. App. 3d at 740.

CPD has failed to establish any of these factually intensive elements. As discussed above, information about cell site simulators has been disseminated already to obtain patent protection and is otherwise well-known. With regard to the second element, Harris provides no details whatsoever as to its internal controls over these alleged trade secrets. With regard to the third element, Harris has not adequately guarded the secrecy of the manuals because its customer, CPD, has no written protocols in place to govern access to these manuals and has no logs of which employees have ever viewed them. Ex. 1-AQ at 4. Nor, given the number of CPD officers convicted or having pled guilty to crimes of theft and dishonesty, would release of such allegedly sensitive information to CPD generally, absent background checks, monitoring, and tight controls of access on an officer-by-officer basis, qualify as sufficient measures to retain trade secret status.⁷ Under the fifth factor, Harris makes only conclusory claims about the "expense" of developing these manuals and provides no specifics. And under the final element, patent disclosures by definition must allow any competitor to duplicate the technology.

⁷ See, e.g., *United States v. Watts*, 12-CR-87, Dkt. # 90, at 22-26 (N.D. Ill. Nov. 4, 2014) (transcript of sentencing hearing of former Chicago Police Officer Ronald Watts, who pled guilty to corruption charges of shaking down drug dealers for protection money in the course of his official duties) (attached as Ex. 6); *Green v. London*, 11-CV-7067, Dkt. # 104, at ¶ 65 (N.D. Ill. Dec. 17, 2014) (admission by Chicago Police Officer Sylshina London to perjury conviction) (attached as Ex. 7); *United States v. Burge*, 711 F.3d 803, 806 (7th Cir. 2013) cert. denied, 134 S. Ct. 315 (2013) (affirming conviction of former Chicago Police Commander Jon Burge for obstruction of justice and perjury); Ex. 1-AR at 1 ("An analysis of five decades of news reports reveals that since 1960, a total of 295 Chicago Police officers have been convicted of serious crimes, such as drug dealing, beatings of civilians, destroying evidence, protecting mobsters, theft and murder."); *United States v. Handardt*, 00-CR-853, Dkt. # 1 (indictment against high-ranking CPD officer for jewelry theft enterprise that included gathering information from law enforcement databases) (N.D. Ill. Oct. 19, 2000) (attached as Ex. 8); *United States v. Handardt*, 00-CR-853, Dkt. # 236 (guilty plea) (N.D. Ill. Oct. 25, 2001) (attached as Ex. 9).

CPD attempts to ignore these requirements under Illinois law in favor of an obsolete test only requiring a showing that release would either inflict substantial competitive harm or make it more difficult for CPD to induce people to submit similar information in the future, relying on *BlueStar Energy Services, Inc. v. Illinois Commerce Commission*. CPD Memo. at 8. That decision turned on the legislative history of the prior and broader version of the exemption. *BlueStar*, 374 Ill. App. 3d 990, 995 (2007); Pub. Act 96-542 (eff. Jan. 1, 2010) (amending 5 ILCS 140/7) (narrowing amendment to trade secret provision). Further, the *BlueStar* test itself came from a federal decision interpreting federal FOIA, 374 Ill. App. 3d at 995, which applies not to technical information of the sort at issue here, but rather, to the distinct category of “commercial or financial information.” Fed. Info. Manual (2d ed.), § 8.4 (attached as Ex. 10) (distinguishing between the two types of claims and describing “fairly narrow scope” of trade secret exemption). Technical manuals (CPD concedes that the records include only “technical information,” CPD Memo. at 8) are not “commercial or financial” and therefore would not be subject to the test CPD proposes even if *BlueStar* remained good law. In fact, the FCC has already produced a redacted copy of a 2010 StingRay and KingFish User Manual in response to a FOIA request,⁸ contrary to CPD’s claim that the entire manuals must be withheld as trade secrets. FCC Resp. to FOIA Control No. 2014-669, available at <http://www.scribd.com/doc/259987684/FCC-FOIA-StingRay-KingFish-User-Manual-2010>.

Even if the manuals were commercial and financial information and even if the federal FOIA test applied to them, CPD has still failed to make the required showing on the merits. The Harris affidavit makes only broad and conclusory claims with no detailed factual support, and it defies common sense that a competitor could compete with Harris simply by knowing the information provided to operators of the device. Similarly, that Harris would give up hundreds

⁸ MARTINEZ does not concede that FCC’s redactions were proper.

of thousands of dollars in contracts with CPD and put “national security” at risk by denying CPD access to its allegedly critical technology if this Court orders the information released is simply implausible.

ii. Valuable Formulae

It is similarly implausible that user manuals and guides would contain actual algorithms, software code, schematic designs, or other such detailed technical information, as opposed to basic information about how to operate the equipment. CPD offers no evidence to support this exemption claim, and makes only a footnote argument that does not overcome the presumption of disclosure by clear and convincing evidence. This tagalong claim should be rejected.

iii. ITAR

CPD claims federal law specifically prohibits the production of stingray manuals and guides to a U.S. citizen under FOIA. CPD’s argument fails for multiple reasons.

Section 7(1)(a) only exempts records “specifically prohibited from disclosure” by a state or federal law. 5 ILCS 140/7(1)(a); *Better Govt. Ass’n*, 386 Ill. App. 3d at 818 (federal grand jury subpoenas not specifically prohibited from disclosure under federal criminal rules; “our legislature has authorized exemptions to the FOIA’s expansive disclosure policy when a given disclosure is not just prohibited ‘by federal or State law or rules and regulations adopted under federal or State law’ but *specifically* so prohibited” (emphasis in original)). While such state or federal law or regulation need not specifically mention FOIA, there must still be a specific prohibition against disclosure of the records. *Id.*; *S. Illinoisan v. Ill. Dept. of Pub. Health*, 218 Ill. 2d 390, 427 (2006) (narrowly construing Section 7(1)(a) exemption as applied to Cancer Registry legislation).

While it is difficult to determine from CPD’s conclusory ITAR claims and Morrison’s conclusory affidavit exactly what provision of ITAR CPD claims to prevent the disclosure of the

manuals to MARTINEZ, as best as MARTINEZ can decipher, CPD claims that 22 U.S.C. § 2778(b)(2) and 22 C.F.R. § 123.1 prohibit “exporting” any “defense articles” without a license. CPD Memo. at 11. CPD claims that the manuals are “technical data” under 22 C.F.R. § 120.17, and while CPD does not cite to any provision under ITAR prohibiting the export of technical data (as opposed to defense articles), MARTINEZ does not dispute that 22 C.F.R. § 120.6 defines defense article to include technical data. Under 22 C.F.R. § 120.17, however, on which CPD specifically relies, “export” is defined, in relevant part, to mean: “(4) Disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad[.]” The regulations simply do not prohibit the distribution of technical data to a U.S. citizen such as MARTINEZ. *See New York Civil Liberties Union*, 47 Misc.3d 1201(A), at *10 (“The Court instead is convinced by petitioner’s argument that the disclosure of public records pursuant to New York’s Freedom of Information Law . . .—even records concerning respondent’s ownership and use of a cell site simulator device that itself may or may not be subject to arms/munitions or defense technology export restrictions—does not amount to the actual export of such arms, munitions, or defense technology.”); Ex. 1-AS at ¶¶ 15-16.

Even if ITAR prohibited the distribution of technical data to a U.S. citizen, however, CPD would still need to prove that the manuals are “technical data.” That term is defined in 22 C.F.R. § 120.10(a)(1) to include “[i]nformation . . . which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation.” CPD does not explain which specific sub-provision of this definition it contends to apply to the manuals, but presumably it relies on “operation . . . of defense articles” and “instructions or documentation.” CPD has not shown that

the manuals are such technical data, as opposed to “basic marketing information on function or purpose or general system descriptions of defense articles,” which are specifically excluded from the definition of technical data. 22 C.F.R. § 120.10(a)(5); *see also Karn v. U.S. Dept. of State*, 925 F. Supp. 1, 13 (D.D.C. 1996); *United States v. Edler Indus.*, 579 F.2d 516, 520-21 (1978); Preamble to Revisions of ITAR (Final Rule), 49 Fed. Reg. 47,682, 47,683 (Dec. 6, 1984) (explaining that “technical data” in ITAR has a narrow applicability); *id.* at 47683 (“The Department’s long-standing practice of regulating only information that is directly related to defense articles . . . remains unchanged.”).

Nor has CPD shown that the devices themselves, whose operations are allegedly shown in the manuals, are “defense articles,” and without such a showing, the manuals cannot qualify as technical data subject to any export controls. CPD cites broadly to Category XI of 22 C.F.R. § 121.1 without specifying the specific provision under which each of the relevant cell site simulators allegedly falls or any documentation to prove its assertion, *see* 22 C.F.R. § 120.4 (describing paperwork and procedures for commodity jurisdiction determinations), and as discussed above, there is no foundation for Morrison’s claims about ITAR. In fact, there is abundant evidence that cell site simulators are not defense articles subject to ITAR. The affidavit of an actual expert on ITAR states that cell site simulators are likely not regulated under ITAR. Ex. 1-AS. Records obtained from the U.S. Department of Commerce, Bureau of Industry and Security, indicate that cell site simulators are regulated not under ITAR, but rather, under the Export Administration Act. Ex. 1-AT; *see also* Ex. 1-AS at ¶ 8. Finally, Harris’ sale of this allegedly highly sensitive military equipment and manuals to local law enforcement and CPD’s lack of any written procedures governing access to the manuals or equipment or any logs of who has accessed the manuals or equipment are completely inconsistent with the proposition that the

manuals are subject to arms export regulations. Ex. 1-AS at ¶ 11; Ex. 1-AQ at 3-4; Ex. 1-AU at 3; CPD Memo. Ex. 2 at ¶ 5. And as discussed above, it appears that Harris has already disclosed substantial information regarding its devices to obtain patent protection and the FCC has released a redacted copy of at least one Harris manual. For these reasons, CPD has failed to show that the manuals and guides are specifically prohibited from disclosure to MARTINEZ under ITAR.

iv. Unique or Specialized Investigative Techniques

For the same reasons that CPD failed to show that court orders and applications satisfy this exemption claim, so too does the claim as to the Harris manuals fail.

v. Security Measures

Just as the manuals do not show investigative techniques, they also do not show any vulnerability assessments or security measures. Nor has CPD even attempted to show in its footnote argument, CPD Memo. at 12 n.4, that the manuals are designed “to identify, prevent, or respond to potential attacks upon a community’s population or systems, facilities, or installations, the destruction or contamination of which would constitute a clear and present danger to the health or safety of the community,” or “the extent that disclosure could reasonably be expected to jeopardize the effectiveness of the measures or the safety of the personnel who implement them or the public.” 5 ILCS 140/7(1)(v). CPD’s sole purported justification for this exemption—“because the cell site simulator equipment may be used in terrorism investigations”—would render CPD’s policies, procedures, manuals, etc. on nearly every aspect of policing exempt merely because the information might also be used in terrorism investigations.

3. Internal Purchase Request and Purchase Justification Memoranda

i. The Records Are Per Se Non-Exempt

The FOIA statute and Illinois Constitution both require, in no uncertain terms and with no exceptions, that records related to the obligation, receipt, and use of public funds are subject to disclosure, period. Ill. Const. Art. VIII, § 1(c) (“Reports and records of the obligation, receipt and use of public funds of . . . units of local government . . . are public records available for inspection by the public according to law.”); 5 ILCS 140/2.5 (“All records relating to the obligation, receipt, and use of public funds of . . . units of local government . . . are public records subject to inspection and copying by the public.”). As CPD concedes, the memoranda “recommend that CPD purchase certain cell site simulator equipment” using public funds. CPD Memo. at 13. Therefore, they cannot be exempt.

ii. Deliberative Process

Contrary to CPD’s assertion, the deliberative process exemption is not so broad as to swallow up all “preliminary memoranda in which actions were formulated.” CPD Memo. at 13. The exemption “protects the opinions that public officials form while creating government policy.” *Kalven v. City of Chicago*, 2014 IL App (1st) 121846, ¶ 24. It does not apply to “factual material.” *Id.* To be exempt, the information must “reflect the give and take of the deliberative process.” *Id.* (citation omitted). To the extent the memoranda became CPD’s final decision on whether to purchase cell site simulators (which is not a “government policy” anyway), they cannot be exempt. *Id.*; *see also Am. Immigration Council v. U.S. Dep’t of Homeland Sec.*, 905 F. Supp. 2d 206, 218 (D.D.C. 2012).

CPD offers no evidence to support its claim that the memoranda are “preliminary” or used to formulate any actions. Even if it did, at most, this exemption would allow CPD to redact the opinions themselves, not factual or other information. 5 ILCS 140/7(1) (“When a request is

made to inspect or copy a public record that contains information that is exempt from disclosure under this Section, but also contains information that is not exempt from disclosure, the public body may elect to redact the information that is exempt.”). Factual information such as descriptions of previous or planned use of the equipment (the very information the requests sought) are not exempt under the deliberative process exemption.

iii. Unique Investigative Techniques, ITAR, and Trade Secrets

For the same reasons CPD failed to establish that these exemptions apply to the court orders and applications or manuals, so too has CPD failed to establish the exemptions as to the memoranda.

B. Request 2: “All court orders for any instances in which police deployed IMSI catchers”

As discussed above with regard to Request Number 1, CPD has failed to prove any exemption claims as to court orders or applications.

C. Request 3: “All formal or informal policies, procedures, orders, directives, or other such records that pertain to when, why, where, how and by whom IMSI catchers may be deployed”

As discussed above, MARTINEZ has prevailed with regard to CPD’s admission, in response to this litigation, that it has no written policies or procedures that pertain to when cell site simulators may be used. As also discussed above, CPD has failed to establish any exemption claims regarding the purchase justification memoranda that are responsive to this request.

D. Request 4: “All records discussing the constitutionality of deploying IMSI catchers”

As discussed above, MARTINEZ has prevailed with regard to CPD’s admission, in response to this litigation, that it has no such records.

E. Request 5: “All records explaining what happens to data collected by Chicago Police IMSI catchers”

Given the Constitutional implications of cell site simulator use, it is implausible that CPD has no policies or procedures that indicate what data can be collected or stored under what circumstances, and as explained above, CPD has not shown that it has undertaken an adequate search for these records. For example, CPD should be able to provide redacted versions of the data it has collected so that the public can understand the general volume and frequency of such data collection and storage (*i.e.*, whether CPD collects data from a small number of targets or from a large volume of people, including, for example, the subscriber IDs of every person in the vicinity of a protest much as it conducts other surveillance of political protesters). In fact, the pen register statute requires CPD to **keep** such records. 18 U.S.C. § 3123(a)(3)(A) (requiring law enforcement to keep a record of the officers who installed the device, when it was installed, the configuration of the device, and “any information which has been collected by the device”). As discussed above, CPD has a history of illegal surveillance of protest groups and continues to target them for intelligence operations, and CPD has failed to show that it undertook a reasonable search for these or any records. The issues at stake in this case are far too important to accept CPD’s inadequate affidavits or arguments without providing MARTINEZ the opportunity to test them fully.

VI. CONCLUSION

The General Assembly and courts of this state have time and time again made clear that information is crucial to a free society and the ability of the public to monitor government to ensure that it is being conducted in the public interest and in compliance with Constitutional rights. MARTINEZ respectfully asks the Court to uphold these principles and deny CPD’s motion to dismiss.

RESPECTFULLY SUBMITTED,



Attorneys for Plaintiff
FREDDY MARTINEZ

Matthew Topic
LOEJV & LOEJV
312 North May St., Suite 100
Chicago, IL 60607
(312) 243-5900
matt@loevy.com
Atty. No. 41295

July 2, 2015

CERTIFICATE OF SERVICE

This is to certify that on July 2, 2015, I served the foregoing Plaintiff's Response to Defendant's Motion to Dismiss on all counsel of record via electronic mail.

/s/ Matthew Topic

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 31 of 31

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

FREDDY MARTINEZ,)
)
Plaintiff,) 2014 CH 15338
)
v.) Hon. Kathleen Kennedy
)
CHICAGO POLICE DEPARTMENT,)
)
Defendant.)

DECLARATION OF CAROLINE HIRST

1. My name is Caroline Hirst.
2. I am over the age of 18 and legally competent to execute this declaration.
3. I am employed as a paralegal at Loevy & Loevy.
4. Attached as Exhibit 1-A to this declaration is a true and correct copy of a letter our office received from Drinker Biddle & Reath on May 15, 2015, in regards to FOIA Request 15-02264.
5. Attached as Exhibit 1-B to this declaration is a true and correct copy of an article from the Chicago Reader titled “Chicago police are spying on citizens” which I accessed from this site: <http://www.chicagoreader.com/chicago/chicago-police-spying-surveillance-first-amendment-protesters-nato/Content?oid=16893815>.
6. Attached as Exhibit 1-C to this declaration is a true and correct copy of an article from The Wall Street Journal titled “How ‘Stingray’ Devices Work” which I accessed from this site: <http://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work/>.
7. Attached as Exhibit 1-D to this declaration is a true and correct copy of the Motion to Suppress transcript in the matter of *State of Florida v. James L. Thomas*, Case No. 2008-

CF-3340A, which I accessed from this site:

https://www.aclu.org/files/assets/100823_transcription_of_suppression_hearing_complete_0.pdf.

8. Attached as Exhibit 1-E to this declaration is a true and correct copy of the *Amici Curiae* Memorandum of ACLU and ACLU of Maryland In Support of Defendant Robert Harrison's Motions to Compel Disclosure of and to Suppress Evidence Related to the Government's Use of a Cell Site Simulator in the matter of *United States of America v. Robert Harrison*.
9. Attached as Exhibit 1-F to this declaration is a true and correct copy of an article from The New York Times titled "A Police Gadget Tracks Phones? Shhh! It's Secret" which I accessed from this site: http://www.nytimes.com/2015/03/16/business/a-police-gadget-tracks-phones-shhh-its-secret.html?_r=0.
10. Attached as Exhibit 1-G to this declaration is a true and correct copy of an article from The Guardian titled "Stingray Spying: FBI's secret deal with the police hides phone dragnet from courts" which I accessed from this site: <http://www.theguardian.com/us-news/2015/apr/10/stingray-spying-fbi-phone-dragnet-police>.
11. Attached as Exhibit 1-H to this declaration is a true and correct copy of an article from the Riverfront Times titled "Stung" which I accessed from this site:
http://blogs.riverfronttimes.com/dailyrft/2015/05/st_louis_police_have_used_stingray_technology_for_years--they_just_wont_talk_about_it.php?page=all.
12. Attached as Exhibit 1-I to this declaration is a true and correct copy of a paper titled "IMSI Catcher" written by Daehyun Strobel and published on July 13, 2007 which I

accessed from this site:

https://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf

13. Attached as Exhibit 1-J to this declaration is a true and correct copy of an article from the Harvard Journal of Law & Technology titled “Your Secret StingRay’s No Secret Anymore: the Vanishing Government Monopoly over Cell Phone Surveillance and its Impact on National Security and Consumer Privacy.”
14. Attached as Exhibit 1-K to this declaration is a true and correct copy of an article from Ars Technica titled “Meet the Machines that steal your phone’s data” which I accessed from this site: <http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/1/>.
15. Attached as Exhibit 1-L to this declaration is a true and correct copy of an article from The Wall Street Journal titled “Americans’ Cellphones Targeted in Secret U.S. Spy Program” which I accessed from this site: <http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533>.
16. Attached as Exhibit 1-M to this declaration is a true and correct copy of an article from the Associated Press titled “FBI Confirms Wide-Scale Use of Surveillance Flights Over U.S. Cities” which I accessed from this site:
http://www.huffingtonpost.com/2015/06/02/fbi-surveillance-flights_n_7490396.html.
17. Attached as Exhibit 1-N to this declaration is a true and correct copy of an article from Wired titled “Feds Admit Stingrays Can Disrupt Cell Service of Bystanders” which I accessed from this site: <http://www.wired.com/2015/03/feds-admit-stingrays-can-disrupt-cell-service-bystanders/>.

18. Attached as Exhibit 1-O to this declaration is a true and correct copy of an article from The Baltimore Sun titled “Baltimore judge allows police use of Stingray phone tracking in murder case” which I accessed from this site:
<http://www.baltimoresun.com/news/maryland/crime/blog/bs-md-ci-stingray-new-disclosures-20150420-story.html>.
19. Attached as Exhibit 1-P to this declaration is a true and correct copy of an excerpt from the book titled Cell Phone Investigations which was written by Aaron Edens and published in 2014.
20. Attached as Exhibit 1-Q to this declaration is a true and correct copy of an article from The Baltimore Sun titled “Baltimore Police used secret technology to track cellphones in thousands of cases” and a court document available with the article which I accessed from the link at the footnote of the exhibit.
21. Attached as Exhibit 1-R to this declaration is a true and correct copy of an article titled “ACLU-Obtained Documents Reveal Breadth of Secretive Stingray Use in Florida” which I accessed from this link: [https://www.aclu.org/blog/free-future/aclu-obtained-documents-reveal-breadth-secretive-sting](https://www.aclu.org/blog/free-future/aclu-obtained-documents-reveal-breadth-secretive-stingray-use-florida?redirect=blog/national-security-technology-and-liberty/aclu-obtained-documents-reveal-breadth-secretive-sting).
22. Attached as Exhibit 1-S to this declaration is a true and correct copy of an article from The News Tribune titled “Stingray snared him, now he helps write rules for surveillance device” which I accessed from this site:
http://www.thenewstribune.com/2015/03/23/3705105_stingray-snared-him-now-he-helps.html?rh=1.

23. Attached as Exhibit 1-T to this declaration is a true and correct copy of an article from the Tallahassee Democrat titled “Unsealed transcript illuminates TPD ‘stingray’ use” which I accessed from this site:

<http://www.tallahassee.com/story/news/local/2014/06/04/unsealed-transcript-illuminates-tpd-stingray-use/9996751/>.

24. Attached as Exhibit 1-U to this declaration is a true and correct copy of a Purchasing memorandum which I accessed from this site, which is linked to the ACLU website:

<http://cdn.arsTechnica.net/wp-content/uploads/2013/09/miami-dade.pdf>

25. Attached as Exhibit 1-V to this declaration is a true and correct copy of an article from The News Tribune titled “Tacoma police change how they seek permission to use cellphone tracker” which I accessed from this site:

http://www.thenewstribune.com/2014/11/15/3488642_tacoma-police-change-how-they.html?sp=99/289&rh=1.

26. Attached as Exhibit 1-W to this declaration is a true and correct copy of an article from Wired titled “Emails Show Feds Asking Florida Cops to Deceive Judges” which I accessed from this site: <http://www.wired.com/2014/06/feds-told-cops-to-deceive-courts-about-stingray/>.

27. Attached as Exhibit 1-X to this declaration is a true and correct copy of an article titled “Leahy & Grassley Press Administration On Use of Cell Phone Tracking Program” which I accessed from this site: <http://www.grassley.senate.gov/news/news-releases/leahy-grassley-press-administration-use-cell-phone-tracking-program>.

28. Attached as Exhibit 1-Y to this declaration is a true and correct copy of a press release from the Senator Bill Nelson titled “Lawmakers must grapple with privacy questions

raised by new surveillance technology” which I accessed from the site listed on the footnote of the exhibit.

29. Attached as Exhibit 1-Z to this declaration is a true and correct copy of a Consent Order Granting Motion and Petition for Access to Sealed Court Records in the Special Proceeding Case No. 14-S-004984.
30. Attached as Exhibit 1-AA to this declaration is a true and correct copy of an article from Ars Technica titled “Local judge unseals hundreds of highly secret cell tracking court records” which I accessed from this site: <http://arstechnica.com/tech-policy/2014/11/local-judge-unseals-hundreds-of-highly-secret-cell-tracking-court-records>.
31. Attached as Exhibit 1-AB to this declaration is a true and correct copy of an article from The Charlotte Observer titled “Secrecy Lifts in CMPD StingRay phone tracking” which I accessed from this site:
<http://www.charlotteobserver.com/incoming/article10435436.html>.
32. Attached as Exhibit 1-AC to this declaration is a true and correct copy of a Google search for the keyword “IMSI catcher” that our office conducted on June 25, 2015.
33. Attached as Exhibit 1-AD to this declaration is a true and correct copy of United States Patent No. 5,428,667.
34. Attached as Exhibit 1-AE to this declaration is a true and correct copy of United States Patent No. 5,870,029.
35. Attached as Exhibit 1-AF to this declaration is a true and correct copy of United States Patent No. 6,771,969.

36. Attached as Exhibit 1-AG to this declaration is a true and correct copy of United States Patent No. 7,110,779.
37. Attached as Exhibit 1-AH to this declaration is a true and correct copy of United States Patent No. 8,792,464.
38. Attached as Exhibit 1-AI to this declaration is a true and correct copy of Defendant's Notice of Supplemental Production in Response to FOIA Request in the matter of *Freddy Martinez v. Chicago Police Department*, Case No. 2014 CH 09565.
39. Attached as Exhibit 1-AJ to this declaration is a true and correct copy of a report by the Special Prosecutor Dan K. Webb titled "The Death of David Koschman" which I accessed from this site :
<http://www.law.northwestern.edu/legalclinic/macarthur/projects/police/documents/SpecialProsecutorReportKoschmanSept182013Feb42014.pdf>
40. Attached as Exhibit 1-AK to this declaration is a true and correct copy of a report by the Chicago Police Department providing an organizational overview which I accessed from this site:
<https://portal.chicagopolice.org/portal/page/portal/ClearPath/About%20CPD/CPD%20Organization/DeptOrgChartMar12.pdf>.
41. Attached as Exhibit 1-AL to this declaration is a true and correct copy of the U.S. Department of State Directorate of Defense Trade Controls internet page titled "The International Traffic in Arms Regulations (ITAR)" which I accessed from this site:
https://www.pmddtc.state.gov/regulations_laws/itar.html.
42. Attached as Exhibit 1-AM to this declaration is a true and correct copy of two affidavits by Bradley S. Morrison.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 7 of 9

43. Attached as Exhibit 1-AN to this declaration is a true and correct copy of an article from the ACLU of Northern California titled “Stingrays The Most Common Surveillance Tool the Government Won’t Tell You About” which I accessed from this site:

https://law.duke.edu/sites/default/files/ccjpr/nw-stingrays_-_guide_for_defense_attorneys.pdf.

44. Attached as Exhibit 1-AO to this declaration is a true and correct copy of an article authored by Stephanie Pell and Christopher Soghoian from the Yale Journal of Law & Technology titled “A Lot More than a Pen Register, and Less than a Wiretap: What the StingRay Teaches Us about How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities.”

45. Attached as Exhibit 1-AP to this declaration is a true and correct copy of the website article titled “Snoop Snitch” which I accessed from this site:

<https://opensource.srlabs.de/projects/snoopsnitch>.

46. Attached as Exhibit 1-AQ to this declaration is a true and correct copy of a letter that our office received from Drinker Biddle & Reath on February 5, 2015, in regards to FOIA Request 15-0098.

47. Attached as Exhibit 1-AR to this declaration is a true and correct copy of the Anti-Corruption Report Number 7 titled “Crime, Corruption, and Cover-ups in the Chicago Police Department,” which I accessed from this site: http://polis.uic.edu/docs/default-source/chicago_politics/anti-corruption_reports/policecorruption.pdf?sfvrsn=2

48. Attached as Exhibit 1-AS to this declaration is a true and correct copy of the affidavit of Robert Clifton Burns in the matter of *New York Civil Liberties Union v. Erie County Sheriff's Office*, Index No. I2014-000206.

49. Attached as Exhibit 1-AT to this declaration is a true and correct copy of a letter sent to our office by United States Department of Commerce, Bureau of Industry and Security in regards to FOIA Request BIS 15-031.

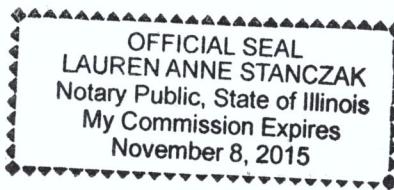
50. Attached as Exhibit 1-AU to this declaration is a true and correct copy of a letter our office received from Drinker Biddle & Reath on January 22, 2015, in regards to FOIA Request 15-0003.

Under penalty of perjury, I affirm that the statements in this declaration are true and correct to the best of my knowledge.



Caroline Hirst

DATE: 7/2/15



Law Offices

191 N. Wacker Drive
Suite 3700
Chicago, IL
60606-1698

(312) 569-1000
(312) 569-3000 fax
www.drinkerbiddle.com

CALIFORNIA
DELAWARE
ILLINOIS
NEW JERSEY
NEW YORK
PENNSYLVANIA
WASHINGTON D.C.
WISCONSIN

VIA E-MAIL

Matthew Topic
Loevy & Loevy
312 N. May Street
Suite 100
Chicago, Illinois 60607
matt@loevy.com

Re: NOTICE OF RESPONSE
REQUEST RECEIVED: April 22, 2015
FOIA FILE NO.: 15-2264

Dear Mr. Topic:

The City of Chicago has retained Drinker Biddle & Reath LLP to assist in responding to an Illinois Freedom of Information Act request you submitted to the Chicago Police Department (“CPD”) on behalf of Freddy Martinez on April 22, 2015, a copy of which is attached. A timely extension was sought, and you agreed to provide an extension of time for CPD’s response to and including May 15, 2015. CPD is now timely responding.

Your request has been reviewed by CPD and Drinker Biddle & Reath LLP, and documents responsive to your request have been searched for and produced by the Office of Legal Affairs. CPD hereby responds to your request as follows:

1. All First Amendment Worksheets.

The enclosed documents are responsive to this request.

Section 7(1) of FOIA provides that “[w]hen a request is made to inspect or copy a public record that contains information that is exempt from disclosure under this Section, but also contains information that is not exempt from disclosure, the public body may elect to redact the information that is exempt. The public body shall make the remaining information available for inspection and copying.” Portions of the enclosed documents have been redacted under the following exemptions:

Section 7(1)(d)(iv) of FOIA exempts from disclosure records of “any law enforcement . . . agency for law enforcement purposes . . . to the extent that disclosure would . . . unavoidably disclose . . . confidential information furnished only by a

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-1538
Jeffrey D. Perconti CALENDAR: 11
312-569-1361 Dire PAGE 1 of 20
312-569-336 CIRCUIT COURT OF
eff.perconti@cofcourts.org COOK COUNTY, ILLINOIS
CHANCERY DIVISION
CLERK DOROTHY BROWN

Matthew Topic

May 15, 2015

Page 2

confidential source.” Portions of the enclosed documents disclose information provided by a confidential source. Accordingly, these portions of the enclosed responsive documents have been redacted pursuant to Section 7(1)(d)(iv).

Section 7(1)(c) exempts from disclosure “[p]ersonal information contained within public records, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.” The responsive documents provide the identities of individuals and organizations of individuals who were the potential subjects of investigations but were not charged with criminal offenses. The disclosure of such information would be “highly personal or objectionable to a reasonable person and . . . the subject’s right to privacy outweighs any legitimate public interest in obtaining the information.” 5 ILCS 140/7(c); *see also* 2010 PAC 8057 (Ill. Att’y Gen. PAC Req. Rev. Ltr., issued September 9, 2010, at 1-2 (police report that did not result in criminal charges was exempt under Section 7(1)(c) because disclosure would result in a violation of privacy)). Accordingly, this identification information has been redacted from the enclosed responsive documents.

2. *Records sufficient to show the rank and bureau, department, division, etc. of each officer involved in preparing, reviewing, approving or denying, and implementing each worksheet.*

The enclosed documents are responsive to this request. Included in the enclosed documents is CPD Special Order S02-02-01, which includes an explanation of the approval process for “Investigations Directed at First Amendment-Related Information.” This directive includes an explanation of the tracking number on CPD’s First Amendment Worksheet, which includes the requesting unit number. This directive and the enclosed First Amendment Worksheets and related documents are responsive to this request.

To the extent this request seeks information beyond what is included on the face of the enclosed responsive documents, the request is a question to which no response is required under FOIA. While FOIA requires a public body to produce documents, (See 5 ILCS 140/3(a) (“Each public body shall make available to any person for inspection or copying all public records, except as otherwise provided in section 7 of this Act”)), FOIA does not require a public body to provide answers to questions or create documents. *See Chicago Tribune Co. v. Dep’t of Fin. & Prof’l Regulation*, 2014 IL App. (4th) 130427, ¶ 33 (4th Dist. 2014); *Kenyon v. Garrels*, 184 Ill.App.3d 28, 32 (4th Dist. 1989). Here, to the extent this portion of the request seeks information regarding the identification of any CPD officer who participated “in preparing, reviewing, approving or denying, and implementing each worksheet” beyond those listed in the enclosed First Amendment Worksheets and related documents, it seeks an answer to a question to which CPD is not required to respond to under FOIA.

DrinkerBiddle&Reath

Matthew Topic

May 15, 2015

Page 3

You have a right of review of this response by the Illinois Attorney General's Public Access Counselor, who can be contacted at 500 S. Second St., Springfield, Illinois 62706, or by telephone at (877) 299-3642. You may also seek judicial review of a denial under 5 ILCS 140/11 of FOIA.

Very truly yours,



Jeff Perconte

Enclosures

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 3 of 20

Perconte, Jeff

From: Matt Topic <matt@loevy.com>
Sent: Wednesday, April 22, 2015 2:54 PM
To: FOIA
Cc: Perconte, Jeff; Caroline Hirst
Subject: FOIA Request

My client, Freddy Martinez, requests PDF copies of the following records to be delivered to me by email to this address, or if that is not feasible, by a mutually agreeable alternative mechanism of delivery (please contact me to discuss if needed).

1. All First Amendment Worksheets
2. Records sufficient to show the rank and bureau, department, division, etc. of each officer involved in preparing, reviewing, approving or denying, and implementing each worksheet.

This is not a commercial request. Please do not communicate with me through any means other than by email to this email address.

Thanks,

Matt

Matthew Topic
Loevy & Loevy

May Street, Suite 100
Chicago, IL 60607
312-497-4973 (office)
312-488-8812 (cell)
matt@loevy.com

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 4 OF 20

The sender of this email is an attorney. The information contained in this communication is confidential, may be attorney-client privileged, may be attorney work product, and is intended only for the use of the addressee. It is the property of the sender. Unauthorized use, disclosure or copying of this communication or any part thereof is strictly prohibited and may be unlawful. If you have received this communication in error, please notify me immediately by return e-mail, and destroy this communication and all copies thereof, including all attachments.

FIRST AMENDMENT WORKSHEET

Chicago Police Department

Date and Time of Request

11OCT 02

1100

First Amendment Invest. Tracking
193-2002-01

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer Constantine Andrews

Name and star number

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate

} a First Amendment investigation
relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 13 OCT 02 (Time) 1600 Hours Date Authorization Expires: 30 Day

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify investigation; for termination of an investigation, indicate rationale for that determination (attach continuation sheet, if necessary)

Chicago is hosting the Trans-Atlantic Business Dialogue Conference (TABD) from 5 through 8 NOV 02. Similar events such as the recent IMF meetings in D.C. have led to anti-globalization protests involving damage to property, obstruction of traffic and multiple arrests. The

group has specifically addressed a need to incorporate

"illegal tactics" and "guerilla tactics" during protests against the TABD. This type of protest poses a threat to the safety of all persons involved and assorted properties.

Indicate Investigative Techniques and Minimization Procedures to be used (attach continuation sheet, if necessary)
Collection of hand-out materials and review of pertinent internet web sites.

ELECTRONICALLY FILED

7/2/2015 12:12 PM
2014-CH-15328

PAGE 20 of 20

Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:
Undercover attendance of protest preparation meetings.

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.
[REDACTED]	[REDACTED]	DNA	DNA

Signature of District Commander/ Unit Commanding Officer

Signature of General Counsel

Date

General Counsel's Determination

11Oct 02

Concur

Do Not Concur

FIRST AMENDMENT WORKSHEET

Chicago Police Department

Date and Time of Request

11 NOV 02

1200

First Amendment Invest. Tracking

193-2002-01

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer _____

Name and star number

- Initial Authorization to Conduct }
 Authorization to Continue }
 Order to Terminate }

a First Amendment investigation relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 13 OCT 02(Time) 1600Date Authorization Expires: 30 Da

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify investigation; for termination of an investigation, indicate rationale for that determination (attach continuation sheet, if necessary)

The above-referenced investigation was predicated on the protest against the Trans-Atlantic Business Dialogue Conference (TABD). This event has ended. Subsequently, this related investigation requires termination.

ELECTRONICALLY FILED

7/2/2015 12:12 PM
2014-CH-15338

PAGE 6 of 20

Indicate Investigative Techniques and Minimization Procedures to be used (attach continuation sheet, if necessary)

Signature of District Commander/ Unit Commanding Officer

Signature of General Counsel

Date

General Counsel's Determination

11 Nov 02

Concur

Do Not Concur

FIRST AMENDMENT WORKSHEET

Chicago Police Department

Date and Time of Request

29 JAN 03

160

First Amendment Invest. Tracking

193

To: Superintendent of Police
 Attention: General Counsel

From: District Commander/ Unit Commanding Officer Constantine Andrews #664

Name and star number

 Initial Authorization to Conduct

- Authorization to Continue
 Order to Terminate

} a First Amendment investigation relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 1 FEB 03 (Time) 1100 Date Authorization Expires: 28 I

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to just investigation; for termination of an investigation, indicate rationale for that determination (attach continuation sheet, if necessary)

[REDACTED] is conducting an anti-war "seminar/teach-in" at the UIC Campus. This group states in its own web-site that they wish to "intensify" the pro movement as it referred to the San Francisco protests of 19 JAN 03; wherein 55,000 to 20 protestors demonstrated. These same protests led to multiple arrests and criminal acts property damage. It is the intent of this investigation to determine if local protest efforts entail criminal acts as possibly espoused at the aforementioned seminar.

Indicate Investigative Techniques and Minimization Procedures to be used (attach continuation sheet, if necessary). Unit 193 personnel will have an undercover presence at the aforementioned seminar. Attention will be given to identify attendees who espouse criminal acts during the course of protest actions in order to collect evidence. Hand-out material will likewise be collected.

Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Undercover personnel will be utilized as described in above section.

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	IR No
[REDACTED]	[REDACTED]	Anti-War Movement	

Signature of District Commander/ Unit Commanding Officer

Constantine Andrews

Signature of General Counsel

Karen Rowan 30 Jan 03

Date

General Counsel's Determination

Concur

Do Not Concur



FIRST AMENDMENT WORKSHEET

Chicago Police Department

Date and Time of Request

4 Feb 03

1600

First Amendment Invest. Tracking
193-2003-001

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer Constantine G. Andrews #664
Name and star number

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate

} a First Amendment investigation
relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 1 Feb 2003 (Time) 1100 Date Authorization Expires: 28 Fe

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify investigation; for termination of an investigation, indicate rationale for that determination (attach continuation sheet, if necessary)

This investigation did not result in the discovery of any actual or planned criminal acts. It is therefore requested that this investigation be terminated.

ELECTRONICALLY FILED

7/2/2015 12:12 PM
2014-CH-15338
PAGE 8 of 20

Indicate Investigative Techniques and Minimization Procedures to be used (attach continuation sheet, if necessary)

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.
[REDACTED]	[REDACTED]	Anti-War Movement	
[REDACTED]	[REDACTED]		
[REDACTED]	[REDACTED]		
[REDACTED]	[REDACTED]		

Signature of District Commander/ Unit Commanding Officer

Signature of General Counsel

Date

4 Feb 03

General Counsel's Determination

Concur

Do Not Concur



FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

Date and Time of Request	06 Feb. 2003	1130hr
First Amendment Invest. Tracking		
	193-2003-02	

From: District Commander/ Unit Commanding Officer Constantine Andrews # 664
Name and star number

- Initial Authorization to Conduct }
 Authorization to Continue } a First Amendment investigation
 Order to Terminate } relating to:
 Intellig
 Public Gathering

Investigation Initiated: (Date) 11 Feb. 2003 (Time) 1900 hrs. Date Authorization Expires: 11 Ma

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how t investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justif investigation; for termination of an investigation, indicate rationale for that determination (attach continuation sheet, if necessa

[REDACTED] has posted a meeting for Tuesday - 11 Feb. 2003 at 1900hrs within its headquarters building located at [REDACTED]. The meeting concerns plans for the upcoming May Day demonstrations. The attached internet posting states "Let's get crazy and knock this shit out Chicago." The word "Mayhem" also is cited.

The undersigned requests that based upon concerns for the safety of life and property within the city during the aforementioned demonstration that unit 193 be allow initiate a First Amendment Investigation.

Indicate Investigative Techniques and Minimization Procedures to be used (attach continuation sheet, if necess

The placement of a covert officer at the aforementioned meeting and the collection of handout materials.

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

See Above

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No
[REDACTED]	[REDACTED]		

Signature of District Commander/ Unit Commanding Officer

Signature of General Counsel

Date

General Counsel's Determination

Concur



Do Not Concur



FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

Date and Time of Request
14 Feb 2003 | 1500
First Amendment Invest. Tracking
193-2003-02

From: District Commander/ Unit Commanding Officer Constantine G. Andrews #664
Name and star number

- | | | |
|---|---|---|
| <input type="checkbox"/> Initial Authorization to Conduct
<input type="checkbox"/> Authorization to Continue
<input checked="" type="checkbox"/> Order to Terminate | } a First Amendment investigation relating to: | <input checked="" type="checkbox"/> Intelligence Gathering
<input type="checkbox"/> Public Gathering |
|---|---|---|

Investigation Initiated: (Date) 11 Feb 2003 (Time) 1900 hrs Date Authorization Expires: 11 Ma

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how t
investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify
investigation; for termination of an investigation, indicate rationale for that determination (attach continuation sheet, if necessary)

The investigation did not result in the discovery of any actual or planned criminal acts. It is therefore requested that this investigation be terminated.

ELECTRONICALLY FILED

12:12 PM
H-15338
0 of 20

icate Investigative Techniques and Minimization Procedures to be used (attach continuation sheet, if necessary)

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.
[REDACTED]	[REDACTED]		

Signature of District Commander/ Unit Commanding Officer

Signature of General Counsel

Date

General Counsel's Determination

Concur

Do Not Concur

1

FIRST AMENDMENT WORKSHEET

Chicago Police Department

Date and Time of Request

19 FEB 03

1430

First Amendment Invest. Tracking

193-2003-03

To: Superintendent of Police
Attention: General CounselFrom: District Commander/ Unit Commanding Officer Constantine Andrews #664
Name and star number

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate

} a First Amendment investigation relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 23 FEB 03 (Time) 1330 Date Authorization Expires: 30 Da

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation will serve/ continue to serve a proper law enforcement purpose and source of information investigation; for termination of an investigation, indicate rationale for that determination (attach continuation sheet, if necessary)

Attached document indicates that [REDACTED] at [REDACTED] is hosting a "Civil Disobedience Planning Meeting." The document is a call to action for "a massive campaign of civil disobedience" upon the U.S. attack of Iraq. The document also refers to putting "our bodies on the line to stop this unjustified war." This event and its plan of action [REDACTED] public safety concerns for both the protestors and the general public. If the plan is enacted a multiple arrest situation is likely.

Indicate Investigative Techniques and Minimization Procedures to be used (attach continuation sheet, if necessary)

Collection of printed material made available at the above meeting and the placement of undercover/covert police personnel (Unit 193) inside the meeting.

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

See Above

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.
[REDACTED]	[REDACTED]	DNA	DNA

Signature of District Commander/ Unit Commanding Officer

Signature of General Counsel

Date

20 Feb 03

General Counsel's Determination

Concur

Do Not Concur



FIRST AMENDMENT WORKSHEET

Chicago Police Department

Date and Time of Request

23 MAR 2003

2200

First Amendment Invest. Tracking I

193-2003-03

To: Superintendent of Police
 Attention: General Counsel

From: District Commander/ Unit Commanding Officer Constantine G. Andrews #664
 Name and star number

- Initial Authorization to Conduct }
 Authorization to Continue } a First Amendment investigation
 Order to Terminate } relating to:
 Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 23 Feb 03 (Time) 1330 Date Authorization Expires: 30

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify investigation; for termination of an investigation, indicate rationale for that determination (attach continuation sheet, if necessary)

This investigation was initiated on 23 FEB 2003 relative to gathering intelligence on a massive campaign of civil disobedience upon the attack of Iraq. This investigation has provided critical intelligence relative to the planned activities of members of the various [REDACTED]. This intelligence is vital to the security of the public and officer safety. Based on the intelligence gathered to date, this investigation is still necessary to continue to provide the proper security for protestors and the general public.

Indicate Investigative Techniques and Minimization Procedures to be used (attach continuation sheet, if necessary):
 Continued collection of printed material made available at meeting at the [REDACTED] and placement of undercover police personnel assigned to Unit #193 inside of meetings.

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

See Above

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.
[REDACTED]	[REDACTED]	DNA	DNA

Signature of District Commander/ Unit Commanding Officer

Signature of General Counsel

Date

24 Mar 03

General Counsel's Determination

Concur



Do Not Concur



FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
 Attention: General Counsel

From: District Commander/ Unit Commanding Officer Constantine G. Andrews #664
 Name and star number

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate

} a First Amendment investigation relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 23 FEB 03(Time) 1300Date Authorization Expires: 30

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify investigation; for termination of an investigation, indicate rationale for that determination (attach continuation sheet, if necessary)

This investigation was initiated on 23 FEB 2003 relative to gathering intelligence on a major campaign of civil disobedience upon the attack of Iraq. This investigation has continued to provide critical intelligence relative to the planned activities of members of the various [REDACTED]

[REDACTED] This intelligence is vital to the security of the public and officer safety.

Based on the intelligence gathered to date, this investigation is still necessary to continue to provide the proper security for the protestors and the general public.

Indicate Investigative Techniques and Minimization Procedures to be used (attach continuation sheet, if necessary)

Continued collection of printed material made available at meetings at the [REDACTED] and placement of undercover personnel assigned to Unit #193 inside of the meeting. These meetings were likewise conducted at an assortment of other sporadic locations.

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

See Above

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.
[REDACTED]	[REDACTED]	DNA	DNA
See Above			

Signature of District Commander/ Unit Commanding Officer

Const. G. Andrews

Signature of General Counsel

Karen Louran 6 May 03

Date

General Counsel's Determination

Concur
Do Not Concur

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

Date and Time of Request

22 MAY 2003

1200

First Amendment Invest. Tracking

193-2003-03

From: District Commander/ Unit Commanding Officer

Constantine Andrews #664
Name and star number

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate

} a First Amendment investigation relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 23 FEB 03

(Time) 1330

Date Authorization Expires: _____

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to just investigation; for termination of an investigation, indicate rationale for that determination (attach continuation sheet, if necessary)

This investigation has been terminated due to the end of the Iraq War. The investigation has ceased to provide intelligence relative to the various [REDACTED] demonstrating intentions for planned activities that may involve civil disobedience.

ELECTRONICALLY FILED
7/2/2015 12:12 PM

Indicate Investigative Techniques and Minimization Procedures to be used (attach continuation sheet, if necessary)

[REDACTED]

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

DNA

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.
[REDACTED]	[REDACTED]	DNA	DNA

Name of District Commander/ Unit Commanding Officer

Signature of General Counsel

Date

General Counsel's Determination:
Concur
Do Not Concur

Tony Lomba 700000000000000000

FIRST AMENDMENT WORKSHEET

(Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer Constantine G. Andrews Unit 193
Name and star number

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate

{}

a First Amendment investigation
relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 03 April 2003 (Time) 1200

Date Authorization Expires: 01 August

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation, Indicate rationale for that determination (attach continuation sheet, if necessary)

[REDACTED] have become increasingly prone to commit large scale

These acts, such as Criminal damage to property and arson have become more
throughout this community. See, support documentation attached.

ELECTRONICALLY FILED
7/2/2015 12:12 PM

2014-CH-15338
PAGE 15 of 20

Indicate Investigative Techniques and Minimization Procedures to be used (attach continuation sheet, if necessary):
Collection of group hand outs and Internet postings.

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Utilization of sworn members in an undercover capacity.

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.
[REDACTED]			

Signature of District Commander/Unit Commanding Officer

Signature of General Counsel

Date

General Counsel's Determination

Concur



Do Not Concur



FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer Constantine G. Andrews Unit 193
Name and star number

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate

} a First Amendment investigation
relating to:

Date and Time of Request
01 August 03 1400
First Amendment Invest. Tracking No.
193-2003-04

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 03 April 2003 (Time) 1200 Date Authorization Expires: 31 October

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation, indicate rationale for that determination (attach continuation sheet, if necessary):

have become increasingly prone to commit large scale criminal acts. These acts, such as Criminal damage to property and arson have become more prevalent throughout this community, see support documentation attached.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338

PAGE 16 of 20
Indicate Investigative Techniques and Minimization Procedures to be used (attach continuation sheet, if necessary):
Collection of group hand outs and Internet postings.

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Utilization of sworn members in an undercover capacity.

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.

Signature of District Commander/Unit Commanding officer

Signature of General Counsel

Date

General Counsel's Determination:

Concur

Do Not Concur

FIRST AMENDMENT WORKSHEET

Chicago Police Department

Date and Time of Request
31 Oct. 03 1400First Amendment Invest. Tracking No.
193-03-004To: Superintendent of Police
Attention: General CounselFrom: District Commander/ Unit Commanding Officer Constantine G. Andrews, Unit 19
Name and star number

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate

} a First Amendment investigation relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 03 April. 03 (Time) 1200Date Authorization Expires: 29 Jan

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation, indicate rationale for that determination (attach continuation sheet, if necessary)

[REDACTED] have become increasingly prone to commit large scale criminal acts. These acts have become more prevalent (see support documents attached). Additionally, [REDACTED] leadership representation has come to Chicago to coordinate escalated acts of aggressive protests which historic have led to criminal acts committed by this particular group.

Indicate Investigative Techniques and Minimization Procedures to be used (attach continuation sheet, if necessary)

Collection of group handouts and internet postings.

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Utilization of sworn members in an undercover capacity.

PERSONS OR GROUPS TO BE INVESTIGATED

Name

Address

Affiliation, if Any

I.R. No.

[REDACTED]	[REDACTED]	[REDACTED]

Signature of District Commander/ Unit Commanding Officer

Constantine G. Andrews

Signature of General Counsel

Karen Cowan

Date

31 Oct. 03

General Counsel's Determination

Concur

Do Not Concur

FIRST AMENDMENT WORKSHEET

Chicago Police Department

Date and Time of Request	
29 JAN 04	1200
First Amendment Invest. Tracking N	
193-03-004	

To: Superintendent of Police

Attention: General Counsel

From: District Commander/ Unit Commanding Officer Michael J. Cronin, Unit 193
Name and star number

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate

} a First Amendment investigation relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 3 APR 03 (Time) 1200Date Authorization Expires: 29 JAN

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify investigation; for termination of an investigation, indicate rationale for that determination (attach continuation sheet, if necessary)

The groups outlined in previous worksheets related to this investigation have discernibly diminished their activities during the past ninety (90) day extension period. It is for this reason that the undersigned is terminating this investigation

ELECTRONICALLY FILED

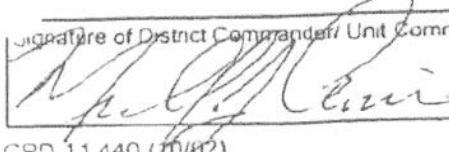
7/2/2015 12:12 PM
2014-CH-13338
PAGE 18 of 20

Indicate Investigative Techniques and Minimization Procedures to be used (attach continuation sheet, if necessary)

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.
Investigation Terminated			

Signature of District Commander/ Unit Commanding Officer

CON 114401M021

Signature of General Counsel

Michael J. Cronin

Date

General Counsel's Determination
Concur
Do Not Concur

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank: Harris G. Byrne

Date and Time of Request	11-Mar-2004	1600
First Amendment Invest. Tracking No.	116 2004 001	

- Initial Authorization to Conduct }
 Authorization to Continue } a First Amendment investigation
 Order to Terminate/Disapproval Of } relating to:
 Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 11-Mar-2004 (Time) 1500 Date Authorization Expires: 10-Apr-2004

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination:

Group organizers have been denied a permit for the area / route in which they are still planning a march and rally for 20-Mar-2004 in the Loop Area of Chicago. I understand that the permit was denied with an alternate route offered due to public safety in the past. We are concerned that without sufficient information for the planning of this event that public safety will be endangered.

See Attach

Indicate Investigative Techniques and Minimization Procedures to be used:

The officers will attend pre planning meetings held by march organizers operating only in the capacity as observers.

See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

In order to avoid causing disruption to the pre planning event and to permit the free flow of information the officers will attend in an undercover capacity.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.

Signature of District Commander/Unit Commanding Officer of Exempt Rank

Harris G. Byrne

Signature of General Counsel

SMechanburg

Date

3/15/03

General Counsel's Determination

Concur

Do Not Concur

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank: Caluris, Steven #520
Name and star number

- Initial Authorization to Conduct }
 Authorization to Continue } a First Amendment investigation
 Order to Terminate/Disapproval Of } relating to:
 Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 11-Mar-2004 (Time) 1500 Date Authorization Expires: 10-Apr-

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination

See Attached Continuation S

Indicate Investigative Techniques and Minimization Procedures to be used :

See Attached Continuation S

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:
-
-
-
-

See Attached Continuation S

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.

Signature of District Commander/Unit Commanding Officer
of Exempt Rank

Signature of General Counsel

Date

General Counsel's Determination

Concur

Do Not Concur

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank: Caluris, Steven 520

- Initial Authorization to Conduct }
 Authorization to Continue } a First Amendment investigation
 Order to Terminate/Disapproval Of } relating to:
 Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 17-Mar-05 (Time) 1800 Date Authorization Expires: 14-Apr

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination

Department Officers received information that groups plan to gather and march on Michigan Ave after having been denied a permit in Federal Court. Participants in similar events have committed crimes that endanger public safety.

See Attached Continuation S

Indicate Investigative Techniques and Minimization Procedures to be used:

Undercover officers will march along with participants functioning strictly as observers.

See Attached Continuation S

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Officers working in this undercover capacity will provide command members with the observations and intelligence in a timely manner to ensure public safety.

See Attached Continuation S

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.

Signature of District Commander/Unit Commanding Officer of Exempt Rank

Signature of General Counsel

Date

General Counsel's Determination

S. Macklenburg

3/13/05

Concur

Do Not Concur

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank:

Date and Time of Request	31-Mar-2005	1600
First Amendment Invest. Tracking N	116-2005-001	

Caluris, Steven #520

Name and star number

- Initial Authorization to Conduct }
 Authorization to Continue } a First Amendment investigation
 Order to Terminate/Disapproval Of } relating to:
 Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 17-Mar-2005 (Time) 1800

Date Authorization Expires: 14-Apr-

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination

See Attached Continuation S

Indicate Investigative Techniques and Minimization Procedures to be used :

See Attached Continuation S

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

See Attached Continuation S

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.

Signature of District Commander/Unit Commanding Officer of Exempt Rank

CPD-11.440 (Rev. 10/03)

Signature of General Counsel

Date

General Counsel's Determination

Concur

Do Not Concur

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

Date and Time of Request	17 January 2006	1500
First Amendment Invest. Tracking No.		116-2005-001

From: District Commander/ Unit Commanding Officer of Exempt Rank:

Steven Caluris

Name and star number

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of

} a First Amendment investigation relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 1/19/06

(Time) 0600

Date Authorization Expires: 5/19/06

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination: Chicago is hosting the 2006 Biotech Conference from 8 April 2006 through 12 April 2006. This conference and its attendees have been targeted by unlawful acts the previous two years, in San Francisco and Philadelphia. These unlawful acts ran the gamut, from disorderly conduct to trespassing and damage to property. These unlawful acts have been verified by Chicago Police Department personnel who have had contact with officers from the San Francisco and Philadelphia police departments. Several groups have also posted photographs of unlawful acts from the previous two years on public web sites. The lawful purpose for which this investigation is being requested, is to determine if groups or individuals are planning or will plan unlawful acts directed at this years conference in Chicago.

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used:

The following investigative techniques will be used during this investigation: monitoring of web sites, collection of pamphlets and hand bills, trash covers, and the use of undercover officers to attend public meetings.

See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Groups and individuals are becoming increasingly hesitant to post information on web sites, due to the fact that they are aware of possible monitoring by law enforcement. For this reason, it is requested that undercover officers be allowed to attend public meetings to determine if any planning of unlawful acts is or will be taking place.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Signature of District Commander/Unit Commanding Officer of Exempt Rank

Signature of General Counsel

Date

Jan. 17, 2006

General Co
Concur
Do Not C

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank:

Date and Time of Request	17 January 2006	1500
First Amendment Invest. Tracking No.		116-2006 J01

Steven Caluris

Name and star number

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of }

a First Amendment investigation relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 1/19/06 (Time) 0600

Date Authorization Expires: 5/19/06

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination :
Chicago is hosting the 2006 Biotech Conference from 8 April 2006 through 12 April 2006. This conference and its attendees have been targeted by unlawful acts the previous two years, in San Francisco and Philadelphia. These unlawful acts ran the gamut, from disorderly conduct to trespassing and damage to property. These unlawful acts have been verified by Chicago Police Department personnel who have had contact with officers from the San Francisco and Philadelphia police departments. Several groups have also posted photographs of unlawful acts from the previous two years on public web sites. The lawful purpose for which this investigation is being requested, is to determine if groups or individuals are planning or will plan unlawful acts directed at this years conference in Chicago.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 4 of 12

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used :

The following investigative techniques will be used during this investigation; monitoring of web sites, collection of pamphlets and hand bills, trash covers, and the use of undercover officers to attend public meetings.

See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Groups and individuals are becoming increasingly hesitant to post information on web sites, due to the fact that they are aware of possible monitoring by law enforcement. For this reason, it is requested that undercover officers be allowed to attend public meetings to determine if any planning of unlawful acts is or will be taking place.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.
[REDACTED]			

Signature of District Commander/Unit Commanding Officer of Exempt Rank

Signature of General Counsel

Date

General Counsel's Determination:

Concur



Do Not Concur



FIRST AMENDMENT WORKSHEET

Chicago Police Department.

To: Superintendent of Police
Attention: General Counsel

Date and Time of Request	13 April 06	09:00
First Amendment Invest. Tracking No.		116-2006-01

From: District Commander/ Unit Commanding Officer of Exempt Rank:

Steven Caluris

Name and star number

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of

} a First Amendment investigation relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 1/17/06 (Time) 0800

Date Authorization Expires: 5/17/06

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination : Reporting Commander requests to terminate First Amendment Investigation #116-2006-01. This Order to Terminate is based on the fact that the focus of the investigation, "BIO 2006" events, have concluded, and the investigation has served it's reasonable law enforcement purpose at this time.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 5 of 12

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used :

See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.

Signature of District Commander/Unit Commanding Officer of Exempt Rank

Signature of General Counsel

Date

4-24-06

General Counsel's Determination:

Concur



Do Not Concur

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank:

Date and Time of Request	24 February 2006	1300
First Amendment Invest. Tracking No.		116-2006-2

Steven Caluris

Name and star number

- Initial Authorization to Conduct }
 Authorization to Continue }
 Order to Terminate/Disapproval Of }
 a First Amendment investigation relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 2/25/06 (Time) 0800

Date Authorization Expires: 6/25/06

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination: Various organizations and individuals are planning an annual anti war march throughout the streets of Chicago on 18 March 2006. In previous years there has been unlawful activity associated with these marches. In 2003, over three hundred individuals were arrested after blocking traffic on Lake Shore Drive and Michigan Avenue and in 2005 five individuals were arrested after gathering unlawfully. [REDACTED] was arrested during both of the aforementioned arrest incidents. [REDACTED] along with [REDACTED] are two identified coordinators of this years events. One of this years web sites which is coordinating events surrounding the march has a listing for "non violence" training which includes, what to expect in an arrest situation, as well as "tactics and strategies." Based upon previous years arrests, the inclusion of [REDACTED] is an organizer of this years events and the above training for march participants in how to handle arrest situations, it would be in the best interest to open an investigation in order to determine whether any group or individual is currently engaged in, or planning, any unlawful activities surrounding the

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used:

Investigative techniques to be used for this investigation include the monitoring of web sites, the use of an undercover officer to attend public meetings and activities and the collection of pamphlets and handbills.

See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

The use of an undercover officer to attend public meetings and events is a necessity. Many organizations and individuals are hesitant to post information, let alone criminal intention on web sites, knowing that law enforcement might be monitoring said sites.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Signature of District Commander/Unit Commanding Officer
Exempt Rank

Signature of General Counsel

Date
2-24-06

General Counsel's Determination:
 Concur
 Do Not Concur

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank:

Date and Time of Request
24 February 2006 1300
First Amendment Invest. Tracking No.
116-2006-2

Initial Authorization to Conduct }
 Authorization to Continue
 Order to Terminate/Disapproval Of }

a First Amendment investigation relating to:

Steven Cahuris

Name and star number:

- Intelligence Gathering
- Public Gathering

Investigation Initiated: (Date) 2/25/06 (Time) 0800

(me) 0800

Date Authorization Expires: 6/25/06

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination : Various organizations and individuals are planning an annual anti war march throughout the streets of Chicago on 18 March 2006. In previous years there has been unlawful activity associated with these marches. In 2003, over three hundred individuals were arrested after blocking traffic on Lake Shore Drive and Michigan Avenue and in 2005 five individuals were arrested after gathering unlawfully.

was arrested during both of the aforementioned arrest incidents. along with
are two identified coordinators of this years events. One of this years web sites which is
coordinating events surrounding the march has a listing for "non violence" training which includes, what to expect in an arrest situation,
as well as "tactics and strategies." Based upon previous years arrests, the inclusion of [REDACTED] as an organizer of this years events and
the above training for march participants in how to handle arrest situations, it would be in the best interest to open an investigation in
order to determine whether any group or individual is currently engaged in, or planning, any unlawful activities surrounding the

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used:

Investigative techniques to be used for this investigation include the monitoring of web sites, the use of an undercover officer to attend public meetings and activities and the collection of pamphlets and handbills.

See Attached Continuation Sheet

Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

The use of an undercover officer to attend public meetings and events is a necessity. Many organizations and individuals are hesitant to post information, let alone criminal intention on web sites, knowing that law enforcement might be monitoring said sites.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Signature of District Commander/Unit Commanding Officer
of Exempt Rank

Signature of General Counsel

Data

General Counsel's Determination:

Concur

四

Do Not Concur

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

Date and Time of Request	
20 March 2006	
First Amendment Invest. Tracking No.	
116-2006-02	

From: District Commander/ Unit Commanding Officer of Exempt Rank:

Steven Caluris
Name and star number

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of

} a First Amendment investigation relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 2/25/06 (Time) 0800

Date Authorization Expires: 6/25/06

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination: Reporting Commander requests to terminate the aforementioned First Amendment Investigation. This order to terminate is based on the fact that the focus of the investigation, [REDACTED] events, have concluded, and the investigation has served its reasonable law enforcement purpose.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 8 of 12

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used:

See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.

Signature of District Commander/Unit Commanding Officer of Exempt Rank

Signature of General Counsel

Date

General Counsel's Determination:

Concur



Do Not Concur



FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank:

Date and Time of Request
02 October 2006
First Amendment Invest. Tracking No.
116-2006-03

David A. Sobczyk

Name and star number

- Initial Authorization to Conduct }
 Authorization to Continue }
 Order to Terminate/Disapproval Of }

a First Amendment investigation
relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 10/2/06 (Time) 1000

Date Authorization Expires: 02 Nov 2006

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination:

[REDACTED] has applied for a permit to protest against President Bush on 05 Oct 2006. [REDACTED] Background: 1) On 15 Oct 05, (114) supporters were arrested at the University of Toledo during a protest action. 2) On 17 Oct 05, (18) self-identified supporters of [REDACTED] were arrested at a NYC protest which targeted a Armed Services Recruiting Station in Times Square. 3) On 19 Oct 05, (5) supporters were arrested at a protest in New York at Hunter College during a protest action. Review of open sources along with [REDACTED] website, [REDACTED] has referred to this event as a "festival of resistance." [REDACTED] are also promoting and referring to wide-spread "student walk-outs" and "campus shut-downs." In direct response and in reference to comments on the aforementioned [REDACTED] website, various persons have e-mailed indymedia.org in order to address the feasibility and purpose of a [REDACTED] participation at the 05 Oct event. References to "breaking windows" and the phrase, "fuck shit up" are present in these e-mails. The lawful purpose for which this investigation is being requested, is to determine if groups or individuals are planning or will plan unlawful acts directed towards Chicago

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used:

The following investigative techniques will be used during this investigation: collection of pamphlets and hand bills, trash covers, and the use of undercover officers to attend public meetings.

See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Groups and individuals are becoming increasingly hesitant to post information on web sites, due to the fact that they are aware of possible monitoring by law enforcement. For this reason, it is requested that undercover officers be allowed to attend public meetings to determine if any planning of unlawful acts is or will be taking place.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Signature of District Commander/Unit Commanding Officer
of Exempt Rank

CPD-11.440 (Rev. 10/03)

Signature of General Counsel

Date

20 Oct. 2006
by LFB

General Counsel's Determination:

Concur

Do Not Concur

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

Date and Time of Request	
30 Oct 2006	
First Amendment Invest. Tracking No.	
116-2006-03	

From: District Commander/ Unit Commanding Officer of Exempt Rank: David A. Schczyk

- Initial Authorization to Conduct
 - Authorization to Continue
 - Order to Terminate/Disapproval Of

a First Amendment investigation relating to:

- Intelligence Gathering
 - Public Gathering

Investigation Initiated: (Date) 02 OCT 06 (Time) 1000 Date Authorization Expires: 02 NOV 06

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination :

This investigation resulted in the generation of one (1) unremarkable report by Sgt. Joel Howard. No indices of criminal activity were observed/documentated. Additionally, the planned protest event on 28 OCT 06 was canceled. Based upon these facts, the undersigned requests that this investigation be closed.

Indicate Investigative Techniques and Minimization Procedures to be used:

See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED			
Name	Address	Affiliation, if Any	I.R. No.

Signature of District Commander/Unit Commanding Officer
of Exempt Rank

Signature of General Counsel

Date _____

| General Covariates Determinants|

SODIUM

Do Not Cease

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank:

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of

} a First Amendment investigation relating to:

Date and Time of Request

17 January 2007

First Amendment Invest. Tracking No

116-2007-00

David Sobczyk

Name and star number

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 1/19/06 (Time) 0700

Date Authorization Expires: 3/31/06

FACTUAL BASIS FOR INVESTIGATION

Investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination: The group [REDACTED] is calling for an eight (8) week protest action targeting the Chicago offices of U.S. Congressional members. During November 2006, this group has participated in protests against the Central Intelligence Agency's involvement in the Iraq Conflict. The protests in Washington D.C. and Smithfield North Carolina resulted in the arrest of fourteen (14) individuals. The arrests included Criminal Trespass. The unlawful acts have been verified by Chicago Police Department personnel who have had contact with law enforcement sources, Central Intelligence Agency and the review of open sources. There are other groups who have also posted photographs and messages relative to unlawful acts on public web sites. The lawful purpose for which this investigation is being requested, is to determine if groups or individuals are planning or will plan unlawful acts directed at elected officials with offices located in Chicago.

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used:

The following investigative techniques will be used during this investigation: collection of pamphlets and hand bills, trash covers, and the use of undercover officers to attend public meetings.

See Attached Continuation Sheet

Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

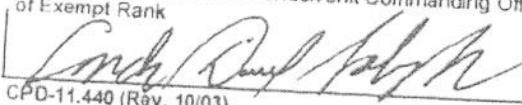
Groups and individuals are becoming increasingly hesitant to post information on web sites, due to the fact that they are aware of possible monitoring by law enforcement. For this reason, it is requested that undercover officers be allowed to attend public meetings to determine if any planning of unlawful acts is or will be taking place.

See Attached Continuation Sheet

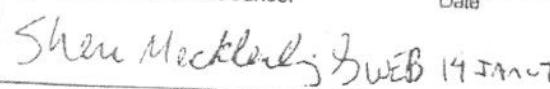
PERSONS OR GROUPS TO BE INVESTIGATED

Name

Signature of District Commander/Unit Commanding Officer of Exempt Rank


CPD-11.440 (Rev. 10/03)

Signature of General Counsel


Shen Mecklenburg 3 WEB 14 JAN 07

Date

General Counsel's Determination:

Concur



Do Not Concur



FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

Date and Time of Request
21 MAR 2007
First Amendment Invest. Tracking No.
116-2007-001

From: District Commander/ Unit Commanding Officer of Exempt Rank:

David A. Sobczyk

Name and star number

- Initial Authorization to Conduct }
 Authorization to Continue }
 Order to Terminate/Disapproval Of } a First Amendment investigation
 relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 1/19/07 (Time) 0600

Date Authorization Expires: 3/31/07

FACTUAL BASIS FOR INVESTIGATION

For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination :
The investigation has been terminated due to the end of the events related to anti-war protests. The investigation has ceased to provide intelligence relative to [REDACTED] demonstrating any intentions for planned activities that may involved civil disobedience

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 12 of 12

Indicate Investigative Techniques and Minimization Procedures to be used :

See Attached Continuation Sheet

See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Signature of District Commander/Unit Commanding Officer of Exempt Rank

CPD-11.440 (Rev. 10/03)

Signature of General Counsel

Date

19 Apr 07

General Counsel's Determination:

Concur



Do Not Concur



FIRST AMENDMENT WORKSHEET

Chicago Police Department

ELECTRONICALLY FILED

7/2/2015 12:12 PM

2014-CH-15338

CALENDAR: 11

23 Ju PAGE 11 of 24

CIRCUIT COURT OF
COOK COUNTY, ILLINOIS
CHANCERY DIVISION
CLERK DOROTHY BROWN

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank:

Commander David Sobczyk

Name and star number

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of }

a First Amendment investigation
relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 7/23/08

(Time) 1330

Date Authorization Expires: 9/22/08

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination :

The lawful purpose for which this investigation is being requested, is to determine if groups or individuals are planning or will plan unlawful acts directed at the City of Chicago and residents of the City of Chicago.

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used :

The following investigative techniques will be used during this investigation: monitoring of web sites, collection of pamphlets, computer discs, hand bills, trash covers, and the use of undercover officers to attend public meetings.

See Attached Continuation Sheet

Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Groups and individuals are becoming increasingly hesitant to post information on web sites, due to the fact that they are aware of possible monitoring by law enforcement. For this reason, it is requested that undercover officers be allowed to attend public meetings to determine if any planning of unlawful acts is or will be taking place.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name

Address

Relationship

I.D. No.

Signature of District Commander/Unit Commanding Officer
of Exempt Rank

CPD-11.440 (Rev. 10/03)

Signature of General Counsel

Date

24 July 2008

General Counsel's Determination:

Concur

Do Not Concur



OFFICE OF THE SUPERINTENDENT
Office of Legal Affairs

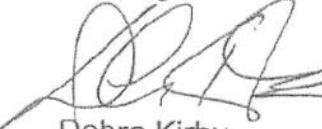
31 March 2009

TO: Jody P. Weis
Superintendent

FROM: Debra Kirby
General Counsel

SUBJECT: Verbal Authorization

On 14 March 2009, I provided verbal authorization to Commander Price to attend a public meeting on 15 March 2009. The purpose is to determine whether any planned activities will be illegal or cause civil disobedience.



Debra Kirby
General Counsel

DK/baj

c:\documents and settings\pc0h804\my documents\first amendment\verbal authorization.doc

Bureau of Investigative Services
Counterterrorism and Intelligence Division
Intelligence Section

16 March 2009

TO: Jody P. Weis
Superintendent of Police

Attn: Debra Kirby
General Counsel

FROM: Ralph M. Price
Commander
Intelligence Section

SUBJECT: First Amendment Intelligence Gathering Investigation

REFERENCE: 191-2009-001

As outlined within General Order 02-10-01B and to ensure that there are no acts of civil disobedience planned during the April visit of the International Olympics Committee (IOC), the Intelligence Section HUMINT Team requested approval for a First Amendment Intelligence Gathering Investigation on the organization [REDACTED]. On 14 March 2009, the undersigned conferred with General Counsel Kirby, who subsequently gave a verbal approval for a provisional First Amendment Investigation.

The investigation will commence on Sunday, 15 March 2009 at 1200 hours. On this date and time, [REDACTED] will host a meeting at [REDACTED]. The purpose of this meeting is to discuss organized opposition to Chicago's bid for the 2016 Olympics during the upcoming 01-08 April visit of the International Olympic Committee.

In the past, the International Olympic Committee and the actual Olympic Games have been the target of unlawful acts such as disorderly conduct, criminal trespass and criminal damage to property. Recently, protests against the upcoming 2010 Olympics in Vancouver British Columbia resulted in several arrests. The purpose of this investigation is to determine if groups or individuals are planning or will plan unlawful acts directed at the International Olympic Committee during their Chicago visit.

Among the investigative techniques that may be utilized are the monitoring of websites, collection of pamphlets, trash covers and the use of undercover officers to attend public meetings. Groups and individuals are becoming increasingly hesitant to post detailed information on websites due to the fact that they may be monitored by law enforcement. It is for this reason that undercover officers will be assigned to attend public meetings to determine if there is any planning of unlawful acts.

The required First Amendment Worksheet was completed and forwarded to the General Counsel. This investigation is not expected to continue beyond thirty (30) days, barring the discovery of intelligence that would warrant an extension request.

Ralph M. Price
Ralph M. Price
Commander
Intelligence Section

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 3 of 24

Bureau of Investigative Services
Counterterrorism and Intelligence Division
Intelligence Section

16 March 2009

Approval Page Only

SUBJECT: First Amendment Intelligence Gathering Investigation

REFERENCE: 191-2009-001

APPROVED:

Patrick Daly for
Brian Murphy
Deputy Chief
Counter Terrorism and Intelligence Division

Patrick Daly
Patrick Daly
Chief
Counter Terrorism and Intelligence Division

Steve Peterson
Steve Peterson
Deputy Superintendent
Bureau of Investigative Services

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 4 of 24

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

Date and Time of Request	
14 March 2009	1600
First Amendment Invest. Tracking No.	
191-2009-001	

From: District Commander/ Unit Commanding Officer of Exempt Rank: Ralph M. Price

- Initial Authorization to Conduct } Name and star number
 Authorization to Continue } a First Amendment investigation Intelligence Gathering
 Order to Terminate/Disapproval Of relating to: Public Gathering

Investigation Initiated: (Date) 3/15/09 (Time) 1200 Date Authorization Expires: 4/13/09

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination : Chicago is hosting the 2016 Olympic Delegation from 02 April 2009 through 08 April 2009. The Olympic Delegation and the Olympic Games have been targeted by unlawful acts such as disorderly conduct and criminal trespass in the past, for example in Vancouver B.C. Canada which resulted in protests and arrests. The lawful purpose to conduct this investigation is to determine if groups or individuals are planning or will plan unlawful acts directed at the 2016 Olympic Delegation in Chicago, Illinois.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 5 of 24

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used :

The following investigative techniques will be used during this investigation: monitoring websites, collection of pamphlets and hand bills, trash covers and the use of undercover officers to attend public meetings.

See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Groups and individuals are becoming increasingly hesitant to post information on websites due to the fact that they are aware of possible monitoring by law enforcement. For this reason, it is requested that undercover officers be allowed to attend public meetings to determine if any planning of unlawful acts are or will be taking place.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Affiliation, if Any	I.R. No.

Signature of District Commander/Unit Commanding Officer of Exempt Rank

CPD-11.440 (Rev. 10/03)

Signature of General Counsel

Date

17 MAR 09

General Counsel's Determination:

Concur

Do Not Concur



Bureau of Investigative Services
Counterterrorism and Intelligence Division
Intelligence Section

15 April 2009

TO: Jody P. Weis
Superintendent of Police

Attn: Debra Kirby
General Counsel

FROM: Ralph M. Price
Commander
Intelligence Section

SUBJECT: First Amendment Intelligence Gathering Investigation -
Order to Terminate

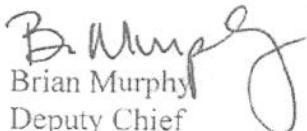
REFERENCE: 191-2009-001

On 08 April 2009 at 0900 hours, the First Amendment Worksheet Order to Terminate was approved by Deputy Chief Brian Murphy on behalf of the undersigned and concurred with by General Counsel Kirby.

This investigation commenced on Sunday, 15 March 2009 at 1200 hours and its termination was based on the fact that the focus of the investigation, [REDACTED] events, has concluded and the investigation has served its reasonable law enforcement purpose at this time.

Ralph M. Price
Commander
Intelligence Section

APPROVED:


Brian Murphy
Deputy Chief
Counter Terrorism and Intelligence Division


Patrick Daly
Chief
Counter Terrorism and Intelligence Division


Steve Peterson
Deputy Superintendent
Bureau of Investigative Services

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 6 of 24

BUREAU OF INVESTIGATIVE SERVICES
Counterterrorism and Intelligence Division
Intelligence Section

26 October 2009

TO: Jody P. Weis
Superintendent of Police

ATTN: Debra Kirby
General Counsel

FROM: Ralph M. Price
Commander
Intelligence Section

SUBJECT: First Amendment Intelligence Gathering Investigation

REFERENCE: 191-2009-002

From 25 through 28 October 2009, the American Banking Association (ABA) is holding their "Annual Meeting, Business Expo and Directors' Forum" at the Sheraton Hotel, 301 East North Water Street in Chicago, Illinois. On 27 October 2009 from 0800 to 1400 hours, the [REDACTED] has a planned march and rally [REDACTED] outside the Sheraton Hotel.

At the recent 24 through 26 September 2009 - "G-20" Economic Summit held in Pittsburgh, PA, hundreds of suspected anarchists conducted organized acts of civil disobedience resulting in 193 arrests. These acts of civil disobedience included throwing rocks at Police Officers and causing extensive property damage through acts of vandalism. Also, past similar type economic or financial events hosted in London, England (April 2009), Washington, DC (October 2007) and Germany (June 2007) resulted in violent demonstration, arrests (London and Germany) and acts of civil disobedience by anarchists. Through open source reporting, it is believed that anarchists will be attending the [REDACTED] event.

As outlined within General Order 02-10-01B and to ensure no acts of civil disobedience occur or escalate at the [REDACTED] 27 October 2009 event, the Intelligence Section FIT Team request approval for a First Amendment Public Gathering Investigation to monitor individuals for suspicious bags/packages or person(s) committing or about to commit acts of civil disobedience or criminal acts.

The required First Amendment Worksheet was completed and forwarded to the General Counsel. This investigation is not expected to continue beyond the conclusion of this one (1) event, barring the discovery of intelligence that would warrant the continuation.

Ralph M. Price
Commander
Intelligence Section

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 7 of 24

BUREAU OF INVESTIGATIVE SERVICES
Counterterrorism and Intelligence Division
Intelligence Section

26 October 2009

Approval Page Only

SUBJECT: First Amendment Intelligence Gathering Investigation
REFERENCE: 191-2009-002

APPROVED:

B Murphy
Brian Murphy
Deputy Chief
Counterterrorism and Intelligence Division

B. Murphy
Patrick Daly
Chief
Counterterrorism and Intelligence Division

B. Murphy
for Steve Peterson
Deputy Superintendent
Bureau of Investigative Services

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 8 of 24

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank: Commander Ralph M. Price (#50)

Date and Time of Request	1500
26 October 2009	
First Amendment Invest Tracking No.	191-2009-002

- Initial Authorization to Conduct }
 Authorization to Continue } a First Amendment investigation
 Order to Terminate/Disapproval Of } relating to:
 Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 10/27/09 (Time) 0830 Date Authorization Expires: 10/28/09

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination:

Chicago is hosting the American Banking Association (ABA) annual meeting, business expo, and directors forum from 25 through 28 October 2009 at the Sheraton Hotel. On 27 October 2009, the [REDACTED] are conducting a planned public gathering. This gathering will include a march from 112 E. Wacker to 400 N. Park (Sheraton Hotel). Outside the Sheraton Hotel, [REDACTED] will host a planned rally of approximately 5,000 to 7,000 people. In past economic type events, acts of civil disobedience and violent protests have occurred. A recent example is Pittsburgh, PA in which the "G-20" economic summit resulted in extensive property damage and 193 arrests. The lawful purpose to conduct this Public Gathering investigation is to monitor individuals for suspicious bags/packages or person(s) committing or about to commit acts of civil disobedience or criminal acts.

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used:

See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Through open source reporting it is believed that anarchists will be attending the [REDACTED] event. For this reason it is requested that undercover officers be allowed to monitor (on the public way) the [REDACTED] march and rally to ensure no unlawful acts are being planned or about to be committed.

See Attached Continuation Sheet

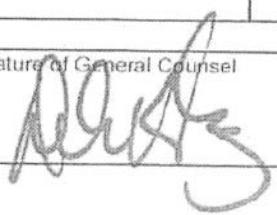
PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.
DNA			

Signature of District Commander/Unit Commanding Officer of Exempt Rank

CPD-11.440 (Rev. 10/03)

Signature of General Counsel



Date

General Counsel's Determination:

Concur



Do Not Concur



FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

Date and Time of Request	
27 October 2009	1230
First Amendment Invest. Tracking No.	
191-2009-002	

From: District Commander/ Unit Commanding Officer of Exempt Rank: Commander Ralph M. Price (#50)

- | | | | |
|--|---|--|---|
| <input type="checkbox"/> Initial Authorization to Conduct
<input type="checkbox"/> Authorization to Continue
<input checked="" type="checkbox"/> Order to Terminate/Disapproval Of | } | a First Amendment investigation relating to: | <input type="checkbox"/> Intelligence Gathering
<input checked="" type="checkbox"/> Public Gathering |
| | | | |

Investigation Initiated: (Date) 10/27/09 (Time) 0830 Date Authorization Expires: 10/28/09

FACTUAL BASIS FOR INVESTIGATION

LEGAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination : Commander Ralph M. Price requests to terminate First Amendment Investigation #191-2009-002. This request to terminate is being made because the "Public Gathering" event has concluded and the investigation has served it's reasonable law enforcement purpose.

ELECTRONICALLY FILED
10/26/2015 10:21 AM

7/2/2015 12:12 PM

Indicate Investigative Techniques and Minimization Procedures to be used:

See Attached Continuation Sheet

תְּהִלָּה

See Attached Continuation Sheet

DNA _____

100

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name _____

Address

Affiliation, if Any

I.R. No.

Name	Address	Affiliation, if Any	I.R. No.
DNA			

Signature of District Commander/Unit Commanding Officer
of Exempt Rank

Signature of General Counsel

Date _____

General Counsel's Determination:

Concur

Do Not Census

BUREAU OF INVESTIGATIVE SERVICES
Counterterrorism and Intelligence Division
Intelligence Section

27 October 2009

TO: Jody P. Weis
Superintendent of Police

ATTN: Debra Kirby
General Counsel

FROM: Ralph M. Price
Commander
Intelligence Section

SUBJECT: First Amendment Intelligence Gathering Investigation Order to Terminate

REFERENCE: 191-2009-002

On 27 October 2009 at 1230 hours, the First Amendment Worksheet Order to Terminate was approved by the Undersigned and concurred with by General Counsel Kirby.

The "Public Gathering" investigation commenced on Tuesday, 27 October 2009 at 0830 and was terminated on 27 October 2009 at 1230 hours. This request to terminate was made because the "Public Gathering" event concluded and the investigation served its reasonable law enforcement purpose.

Ralph. Price
Ralph M. Price
Commander
Intelligence Section

APPROVED:

B. Murphy
Brian Murphy
Deputy Chief
Counterterrorism and Intelligence Division

B. Murphy
For Patrick Daly
Chief
Counterterrorism and Intelligence Division

Steve Peterson
Steve Peterson
Deputy Superintendent
Bureau of Investigative Services

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 11 of 24

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank: Commander Ralph M. Price (#50)

- Initial Authorization to Conduct }
 Authorization to Continue }
 Order to Terminate/Disapproval Of } a First Amendment investigation relating to:
 Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 10/27/09 (Time) 0830

Date Authorization Expires: 10/28/09

FACTUAL BASIS FOR INVESTIGATION

For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination : Commander Ralph M. Price requests to terminate First Amendment Investigation #191-2009-002. This request to terminate is being made because the "Public Gathering" event has concluded and the investigation has served it's reasonable law enforcement purpose.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 12 of 24

Indicate Investigative Techniques and Minimization Procedures to be used : See Attached Continuation Sheet

DNA

See Attached Continuation Sheet

Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

DNA

PERSONS OR GROUPS TO BE INVESTIGATED

See Attached Continuation Sheet

Name	Address	Affiliation, if Any	I.R. No.
DNA			

Signature of District Commander/Unit Commanding Officer of Exempt Rank

Ralph M. Price

CPD-11.440 (Rev. 10/03)

Signature of General Counsel

Date

General Counsel's Determination:

Concur

Do Not Concur

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

Date and Time of Request
20 January 2011 2200
First Amendment Invest. Tracking No.
141-2011-001

From: District Commander/ Unit Commanding Officer of Exempt Rank: ADS Steve E. Georgas

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of }

a First Amendment investigation relating to:

Name and star number

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 1/20/11 (Time) 0800 hrs. Date Authorization Expires: 1/21/11

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination : Chicago Police investigative actions directed towards First Amendment activities were terminated on 20 January 2011 at approximately 2200hrs. Termination ordered due to investigation failing to produce any illegal activities or public safety threats, continued investigation would serve no law enforcement purpose.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 13 of 24

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used :

See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.

Signature of District Commander/Unit Commanding Officer of Exempt Rank

For STEVE E GEORGAS R. Lagan
CPD-11.440 (Rev. 10/03)

Signature of General Counsel

Debra Kirby by
will - F.B.I.
24 JAN 2011

Date

General Counsel's Determination:

Concur

Do Not Concur

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank: ADS Steve E. Georgas

Date and Time of Request

20 January 2011 2200

First Amendment Invest. Tracking No.
141-2011-001

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of

} a First Amendment investigation relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 1/20/11

(Time) 0800 hrs.

Date Authorization Expires: 1/21/11

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination :
Chicago Police investigative actions directed towards First Amendment activities were terminated on 20 January 2011 at approximately 2200hrs. Termination ordered due to investigation failing to produce any illegal activities or public safety threats, continued investigation would serve no law enforcement purpose.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 14 of 24

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used :

See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.

Signature of District Commander/Unit Commanding Officer of Exempt Rank

For Steve E. Georgas R. Lagan

Signature of General Counsel

Debra Kirby by
Wul - F.B.I. 24 JAN 2011

Date

24 JAN 2011

General Counsel's Determination:

Concur

Do Not Concur

BUREAU OF PATROL
Special Functions Group

12 JANUARY 2011

TO: Jody P. Weis
Superintendent of Police

Attention: Debra Kirby
General Counsel

FROM: Steve E. Georgas
Assistant Deputy Superintendent
Special Functions Group

SUBJECT: FIRST AMENDMENT INTELLIGENCE GATHERING INVESTIGATION
Reference: 141-2011-001

On January 19-21, 2011 the President of China will visit the United States of America, with an overnight stay in the City of Chicago on January 20-21, 2011. The President will have two official stops during his stay within the City of Chicago prior to traveling to Woodridge, IL for a final stop before returning to O'Hare International Airport.

There is a history of anti-China demonstrations within the United States and around the world that have resulted in acts of civil disobedience and property damage. The Chinese Consulate is located at 100 W. Erie within the City of Chicago and has been home to regular demonstrations by both [REDACTED] and the [REDACTED]. The City has had experience with acts of civil disobedience and property damage at demonstrations involving [REDACTED] that have included criminal damage to the consulate, criminal trespass to the consulate and acts of reckless conduct. These past behaviors have resulted in the Chicago Police Department to invoke time, place manner restrictions at the consulate for any future demonstrations with [REDACTED]. Similar acts have also occurred in other cities within the United States and around the globe.

As outlined by Department directive this investigation is requested to ensure the public safety, there are no criminal acts and no acts of civil disobedience. This investigation will also provide a reasonable law enforcement purpose that may be useful in assisting command personnel in allocating resources for the interest of public safety. Therefore the Special Functions Group requests approval for a First Amendment Public Gathering Investigation to monitor individuals for suspicious bags/packages or person(s) committing or about to commit acts of civil disobedience or criminal acts.

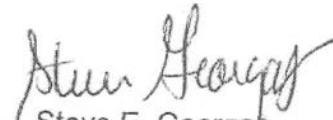
The required First Amendment Worksheet was completed and forwarded to the General Counsel. It is requested that the investigation begin on 20 January 2011 and is not expected to continue beyond the conclusion of this two day visit to the City of Chicago, barring the discovery of intelligence that would warrant the continuation. This investigation will utilize undercover police officers at gatherings on the public way to achieve the mission stated above.

BUREAU OF PATROL
Special Functions Group

12 JANUARY 2011

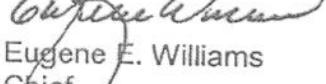
SUBJECT: FIRST AMENDMENT INTELLIGENCE GATHERING INVESTIGATION
Reference: 141-2011-001

Signature Page Only



Steve E. Georgas
Assistant Deputy Superintendent
Special Functions Group

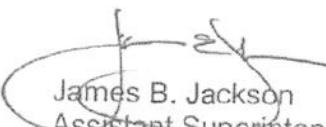
Approval:



Eugene E. Williams
Chief
Bureau of Patrol



Ernest T. Brown
Deputy Superintendent
Bureau of Patrol


James B. Jackson

Assistant Superintendent
Law Enforcement Operations

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

Date and Time of Request	12 January 2011	0800
First Amendment Invest. Tracking No.	141-2011-001	

From: District Commander/ Unit Commanding Officer of Exempt Rank: ADS Steve E. Georgas #300

Name and star number

- Initial Authorization to Conduct }
 Authorization to Continue } a First Amendment investigation
 Order to Terminate/Disapproval Of } relating to:
 Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 1/20/11 (Time) 0800 hours Date Authorization Expires: 1/21/11

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation; indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination :
The President of China will be visiting the City of Chicago on the above dates. The City has a history, along with other major cities of civil disobedience and criminal acts directed at the Chinese, specifically the Chinese Consulate, during previous demonstrations involving groups such as [REDACTED]. This investigation will allow on duty Chicago Police Department personnel to monitor individuals for suspicious bags/packages or person(s) committing or about to commit acts of civil disobedience or criminal acts in interest of public safety and to assist command personnel in decision making for the allocation of resources in interest of public safety.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 17 of 24

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used :

See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

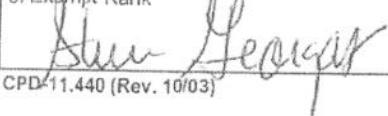
Through past experience there is a likelihood that these groups will again come together and demonstrate against the visit of the President of China. For this reason it is requested that undercover officers be allowed to monitor (on the public way) any gatherings and/or marches that are being planned or spontaneous.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

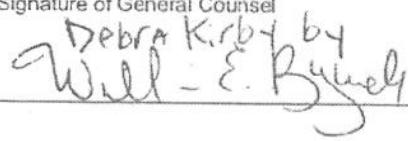
Name	Address	Affiliation, if Any	I.R. No.

Signature of District Commander/Unit Commanding Officer of Exempt Rank


Steve E. Georgas

CPD 11.440 (Rev. 10/03)

Signature of General Counsel


Debra Kirby by
Will E. Bynum

Date

14 JAN 2011

General Counsel's Determination:

Concur

Do Not Concur

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank: ADS Steve E. Georgas #300

Date and Time of Request
12 January 2011 10:00
First Amendment Invest. Tracking No.
141-2011-001

- Initial Authorization to Conduct }
 Authorization to Continue }
 Order to Terminate/Disapproval Of } a First Amendment investigation relating to:
 Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 1/20/11 (Time) 0800 hours Date Authorization Expires: 1/21/11

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination : The President of China will be visiting the City of Chicago on the above dates. The City has a history, along with other major cities of civil disobedience and criminal acts directed at the Chinese, specifically the Chinese Consulate, during previous demonstrations involving groups such as [REDACTED]. This investigation will allow on duty Chicago Police Department personnel to monitor individuals for suspicious bags/packages or person(s) committing or about to commit acts of civil disobedience or criminal acts in interest of public safety and to assist command personnel in decision making for the allocation of resources in interest of public safety.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 18 of 24

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used :

See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Through past experience there is a likelihood that these groups will again come together and demonstrate against the the visit of the President of China. For this reason it is requested that undercover officers be allowed to monitor (on the public way) any gatherings and/or marches that are being planned or spontaneous.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.

Signature of District Commander/Unit Commanding Officer of Exempt Rank

CPD 11.440 (Rev. 10/03)

Signature of General Counsel

Debra Kirby by
Will E. Bynum 19 Jan 2011

Date

General Counsel's Determination:

Concur

Do Not Concur



OFFICE OF THE SUPERINTENDENT
Office of Legal Affairs

19 JANUARY 2012

TO: Garry F. McCarthy
Superintendent of Police

Attn: Constantine Miniatis
Chief
Office of the Superintendent

FROM: Ralph M. Price
General Counsel
Office of the Superintendent

SUBJECT: Non-concurrence with First Amendment Investigation
and Infiltration Request

REFERENCE: First Amendment Investigation Tracking No. 191-2012-01

On 13 January 2012, the undersigned received a request to initiate a First Amendment Investigation of the [REDACTED]

[REDACTED] Additionally, there was a separate request to authorize "infiltration" techniques in conjunction with this First Amendment Investigation.

On 18 January 2012, the undersigned met with Chief Roti, Commander Mealer and Lieutenant DeVries to discuss said request. After thorough review, all parties in attendance agreed there is insufficient factual basis for approval of these requests at this time.


Ralph M. Price
General Counsel
Office of the Superintendent

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

Date and Time of Request
11 January 2012
First Amendment Invest. Tracking No.
191-2012-01

From: District Commander/ Unit Commanding Officer of Exempt Rank: Michael J. Mealer #95

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of

} a First Amendment investigation relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) _____ (Time) _____ Date Authorization Expires: _____

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination :
On 3 January 2012, [REDACTED] submitted an Application for a

Permit-Parade Using the Public Way to the Permit Division of the Office of Emergency Management and Communication to engage in a parade on 19 May 2012 during the G8/NATO conferences. The projected attendance for the event is 5,000 people. The requested activity will require substantial accommodations from the city for traffic control and street closures. The event will require public safety and city service resources to ensure the safety of the participants and prompt and effective response to unforeseen emergency incidents. Protests, marches and parades in other cities during such conferences have resulted in violence, property damage and civil disorder instigated and caused by infiltrators using the cover of lawful protest groups such as [REDACTED]. (See attached continuation sheet)

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338

PAGE 20 of 24

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used :

The following investigative techniques will be used during this investigation: monitoring websites, collection of pamphlets and hand bills, trash covers and the use of undercover officers to attend public meetings and infiltration.

See Attached Continuation Sheet

Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Members of violent anarchist groups who have been attributed with unlawful activity in the past attend meetings to engage others for unlawful conduct. For this reason, it is requested that undercover officers be allowed to attend public meetings to determine if any planning of unlawful acts or recruitment for unlawful activities are, or will be taking place. Infiltration is requested pursuant to the attached request.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name

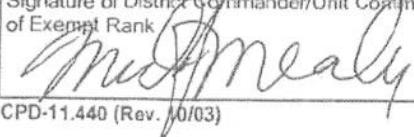
Address

Affiliation, if Any

LR No.

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Signature of District Commander/Unit Commanding Officer of Exempt Rank



CPD-11.440 (Rev. 10/03)

Signature of General Counsel

Ryan Prie

18JAN12

Date

General Counsel's Determination:

Concur



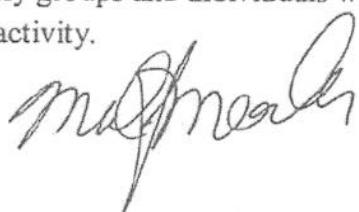
Do Not Concur



Continuation Sheet for First Amendment Worksheet 191-2012-01
Dated 11 January 2012

FACTUAL BASIS FOR INVESTIGATION CONTINUED:

As a recent example the Group of Twenty economic summit held in Pittsburgh, Pennsylvania in March 2009 resulted in civil disturbances that damaged property and resulted in numerous arrests. The Toronto G-20 After Action Report attributes the civil disorder to [REDACTED] and violent anarchist infiltrators to lawful protest groups. The lawful purpose to conduct this investigation is to acquire information to ensure adequate city resources are provided for lawful demonstration activity and to gather information to identify groups and individuals who may utilize lawful activity of [REDACTED] as a cover for criminal activity.



ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 21 of 24

13 JAN 12 15
U.S. DISTRICT COURT
CLERK'S OFFICE
DETROIT, MICHIGAN
63

Bureau of Organized Crime
Intelligence Division

11 January 2012

To:

Garry F. McCarthy
Superintendent of Police

Attention:

Ralph Price
General Counsel to the Superintendent

From:

Michael J. Mealer
Commander
Intelligence Division

Subject:

Request to Initiate a First Amendment Investigation

Reference:

[REDACTED]
First Amendment Investigation Tracking Number: 191-2012-01
Department Special Order 02-01 "Investigations Directed at First
Amendment-Related Intelligence"

Initiation Date & Time:

Effective upon approval

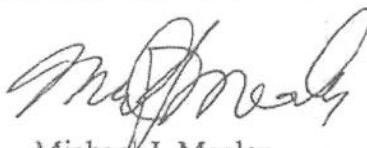
The G8/NATO Conferences are scheduled to be held in Chicago [REDACTED] between 19 May 2012 and 21 May 2012. When held in other cities, demonstrations and protests have occurred. Some demonstrations have resulted in violence, property damage and civil disorder instigated and caused by infiltrators using the cover of lawful protest groups. In order to protect and facilitate the lawful demonstrations that are likely to occur during the events, to protect the citizens and businesses of the city of Chicago, and to adequately plan for security for the events, the Intelligence Division requests approval to initiate a First Amendment Investigation focused on the [REDACTED]

On 3 January 2012, [REDACTED] submitted an *Application for a Permit-Parade Using the Public Way* to the Permit Division of the Office of Emergency Management and Communication. The projected attendance for the event is 5,000 people. The requested activity will require substantial accommodations from the city for traffic control and street closures. The event will require public safety and city service resources to ensure the safety of the participants and prompt and effective response to unforeseen emergency incidents.

The First Amendment investigation of [REDACTED] is necessary to acquire event information from members and participants of [REDACTED] that might not be shared directly with the city by the organization leaders or its members. The anti-war protest conducted by the same organizer on March 20, 2003, resulted in actions that resulted in numerous arrests and stresses on city services due to the event. The information sought through the investigation is to ensure adequate city resources are provided for the event and also to identify groups and individuals who may utilize the lawful purposes of [REDACTED] and the large numbers of peaceful protesters as cover for criminal activity.

The least invasive methods will be utilized to obtain public safety and criminal information and intelligence. The investigation will require covert attendance at organizing, informational, educational and fund raising meetings conducted by [REDACTED] and affiliated organizations. Surveillance of individuals promoting criminal activity or endorsing conduct contrary to the permit will be necessary to identify groups that may disrupt [REDACTED] or the G8/NATO event. Infiltration will be required and is subject to a separate report attached to this request. Review of open source material contained on the internet and public bulletin boards will also be necessary.

The investigation is expected to last until the end of the G8/NATO event and will be reviewed and renewed every thirty days until the conclusion of the G8/NATO. Collection activity will be reviewed weekly.



Michael J. Mealer
Commander
Intelligence Division

13 JAN 12 15
U.S. DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
L3

Approved:



Nicholas J. Roti
Chief
Bureau of Organized Crime

NOT APPROVED a.w.
Alfonza Wysinger
First Deputy Superintendent

cc/Chief Kirby

Bureau of Organized Crime
Intelligence Division

11 January 2012

To: Garry F. McCarthy
Superintendent of Police

Attention: Ralph Price
General Counsel to the Superintendent

From: Michael J. Mealer
Commander
Intelligence Division

Subject: Request for Authorization for Infiltration

Reference: G8/NATO Conferences
First Amendment Investigation Number: 191-2011-01 & 02
First Amendment Investigation Number: 191-2012-01 (Pending)
Department Special Order 02-01 "Investigations Directed at First Amendment-Related Intelligence"

Initiation Date & Time: Effective upon approval

Pursuant to the authorized First Amendment Investigation 191-2011-01 & 02 and to further the investigation requested by First Amendment Investigation 191-2012-01, the undersigned requests authorization to engage in infiltration of the [REDACTED]

During the investigation of [REDACTED] pursuant to FAI 191-2011-02, Police Officer Lynn Bunch became familiar with the participants in the [REDACTED]. Some of the same participants in [REDACTED] are involved in the [REDACTED]. On two separate occasions Officer Bunch attended publicly advertised open public meetings for [REDACTED] without invitation by any of the [REDACTED] individuals or by the [REDACTED] members. She attended the meetings in regard to FAI 191-2011-01, G8/NATO investigation. As of this time Officer Bunch has not engaged in any conduct at organizing events or meetings that would classify her as an infiltrator pursuant to Special Order 02-02-01-II-3. The relevant portion of the order is quoted below:

JAN 12
FBI - LIAISON

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 24 of 24

II-3. Infiltrator

An infiltrator is an officer who affirmatively identifies himself as a member or participant in the group or organization and who does not disclose his function as an agent of the police. An infiltrator becomes a member of the organization under investigation and acts in a manner which participates, influences, or directs the organization.

EXAMPLE: After attending several meetings undercover, the officer becomes friendly with the organizers and is invited to private meetings at organizers' homes. He attends and participates in group debates about how to be effective in the organization's goals. The officer is now an infiltrator.

[REDACTED] Due to the increased organizing, training and informational activity of the organization and the possibility that Officer Bunch will be invited to the meetings as described in the Special Order example quoted above, the undersigned requests authorization to permit Officer Bunch and any officer who may be needed to accompany her, to engage in infiltration of [REDACTED].

The infiltration will be initiated upon approval of the Superintendent and continue for thirty days. Renewals will be sought prior to expiration of the thirty days if continued infiltration is necessary to collect information to achieve the purpose stated in the First Amendment Investigation 191-2012-01.

Michael P. Mealer
Commander
Intelligence Division

Approved:

N. Roti
Nicholas J. Roti
Chief
Bureau of Organized Crime

NOT Approved A.W.
Alfonza Wysinger
First Deputy Superintendent

Garry F. McCarthy
Superintendent of Police

cc/Chief Kirby

13 JAN 12 15
Officer of Legal Services
44

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank:

Michael J. Mealer #95

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of

} a First Amendment investigation relating to:

- Name and star number
 Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 10/14/11 (Time) 0900

Date Authorization Expires: 2/11/12

FACTUAL BASIS FOR INVESTIGATION

- For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination :
As of this time, the [REDACTED] has had a significant lack of participants and further investigation no longer serves the Departments purpose of ensuring that the Chicago Police Department can adequately prepare for large events developing from this movement and to determine whether participants are planning activities that involve violence, property destruction or large scale civil disorder. It is requested that this Investigation be terminated.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 2 of 25

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used :

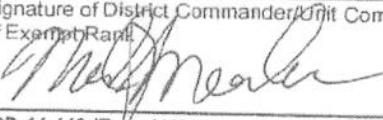
See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Signature of District Commander/Unit Commanding Officer of Exempt Rank 	Signature of General Counsel 	Date <u>19 JAN 12</u>	General Counsel's Determination: Concur <input checked="" type="checkbox"/> Do Not Concur <input type="checkbox"/>
---	---	--------------------------	--

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank: Michael J. Mealer #95

Date and Time of Request	
6 January 2012	0900
First Amendment Invest. Tracking No.	191-2011-002

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of

} a First Amendment investigation relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 10/14/11 (Time) 0900

Date Authorization Expires: 1/12/12 2/11/12 ✓

FACTUAL BASIS FOR INVESTIGATION

For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination:

[REDACTED] has gone national and has manifested itself in Chicago as [REDACTED] engaged in public disorder and violations of the law that resulted in over 700 arrests in New York City on 1 October 2011. On 11 October 2011, 100 [REDACTED] protesters were arrested for trespassing during a demonstration. Other [REDACTED] participants in other cities around the country have been arrested for criminal acts and public disorder. The [REDACTED] movement has occupied the area around LaSalle and Jackson near the Federal Reserve and the Bank of America building since the movement begun. To ensure that the Chicago Police Department can adequately prepare for large events developing from this movement and to determine whether participants are planning activities that involve violence, property destruction or large scale civil disorder, it is necessary to gather intelligence from [REDACTED] participants, meetings and formal and informal events.

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used:

The following investigative techniques will be used during this investigation: monitoring websites, collection of pamphlets and handouts, trash covers and the use of undercover officers to attend public meetings.

See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Members of violent anarchist groups who have been attributed with unlawful activity in the past attend meetings to engage others for unlawful conduct. For this reason, it is requested that undercover officers be allowed to attend public meetings to determine if any planning of unlawful acts or recruitment for unlawful acts are, or will be taking place.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Affiliation, if Any	I.R. No.
[REDACTED]		

Signature of District Commander/Unit Commanding Officer of Exempt Rank

CPD-11.440 (Rev. 10/03)

Signature of General Counsel

R. Mealer

Date

09 JAN 2012

General Counsel's Determination:

Concur



Do Not Concur



Bureau of Organized Crime
Intelligence Division

6 January 2012

To: Nicholas J. Roti
Chief
Bureau of Organized Crime

From: Michael J. Mealer
Commander
Intelligence Division

Subject: 1st Amendment Investigation Extension Request
[REDACTED]
Ref: 191-2011-002
2nd Extension Expiration Date: 12 January 2012
Requested Extension: 11 February 2012

The undersigned request a 30 day extension to the 1st Amendment Investigation to continue to gather information and intelligence to ensure adequate city resources are provided for lawful demonstration activity and to gather information to identify groups and individuals who may utilize lawful demonstrations as a cover for criminal activity.

Level II Investigative techniques will be used as described in the First Amendment Worksheet initiating this investigation. Please note that there are additional [REDACTED]
[REDACTED]



Michael J. Mealer
Commander
Intelligence Division

Approved:



Nicholas J. Roti
Chief
Bureau of Organized Crime

cc/G.C. Price

-9 JAN 12 13
FBI - LOS ANGELES

Bureau of Organized Crime
Intelligence Division

8 December 2011

To: Nicholas J. Roti
Chief
Bureau of Organized Crime

From: Michael J. Mealer
Commander
Intelligence Division

Subject: 1st Amendment Investigation Extension Request

Ref: 191-2011-002
1st Extension Expiration Date: 13 December 2011
Requested Extension: 12 January 2012

The undersigned request a 30 day extension to the 1st Amendment Investigation to continue to gather information and intelligence to ensure adequate city resources are provided for lawful demonstration activity and to gather information to identify groups and individuals who may utilize lawful demonstrations as a cover for criminal activity.

Level II Investigative techniques will be used as described in the First Amendment Worksheet initiating this investigation. Please note that there are additional groups listed on the attached worksheet. These groups are subsidiaries with the overall [REDACTED]

Michael J. Mealer
Commander
Intelligence Division

Approved:

Joseph Patterson
Deputy Chief
Bureau of Organized Crime

Nicholas J. Roti
Chief
Bureau of Organized Crime

U.S. DEPARTMENT OF JUSTICE

DEC 11 14

07

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 5 of 25

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank: Michael J. Mealer #95

Date and Time of Request
8 December 2011
First Amendment Invest. Tracking No.
191-2011-002

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of

} a First Amendment investigation relating to:

Name and star number

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 10/14/11

(Time) 0900

Date Authorization Expires: 12/31/11

1/12/12

FACTUAL BASIS FOR INVESTIGATION

For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination:

[REDACTED] has gone national and has manifested itself in Chicago as the [REDACTED]
[REDACTED] engaged in public disorder and violations of the law that resulted in over 700 arrests in New York City on 1 October 2011. On 11 October 2011, 100 [REDACTED] protesters were arrested for trespassing during a demonstration. Other [REDACTED] participants in other cities around the country have been arrested for criminal acts and public disorder. The [REDACTED] has occupied the area around LaSalle and Jackson near the Federal Reserve and the Bank of America building since the movement begun. To ensure that the Chicago Police Department can adequately prepare for large events developing from this movement and to determine whether participants are planning activities that involve violence, property destruction or large scale civil disorder, it is necessary to gather intelligence from [REDACTED] participants, meetings and formal and informal events.

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used:

The following investigative techniques will be used during this investigation: monitoring websites, collection of pamphlets and handouts, trash covers and the use of undercover officers to attend public meetings.

See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Members of violent anarchist groups who have been attributed with unlawful activity in the past attend meetings to engage others for unlawful conduct. For this reason, it is requested that undercover officers be allowed to attend public meetings to determine if any planning of unlawful acts or recruitment for unlawful acts are, or will be taking place.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Signature of District Commander/Unit Commanding Officer of Exempt Rank

CPD-11.440 (Rev. 10/03)

Signature of General Counsel

Ron J. Mealer 08 Dec 2011

Date

General Counsel's Determination:

Concur



Do Not Concur



Bureau of Organized Crime
Intelligence Division

7 November 2011

To: Nicholas J. Roti
Chief
Bureau of Organized Crime

From: Michael J. Mealer
Commander
Intelligence Division

Subject: 1st Amendment Investigation Extension Request
[REDACTED]
Ref: 191-2011-002
Original Expiration Date: 13 November 2011
Requested Extension: 13 December 2011

The undersigned request a 30 day extension to the 1st Amendment Investigation to continue to gather information and intelligence to ensure adequate city resources are provided for lawful demonstration activity and to gather information to identify groups and individuals who may utilize lawful demonstrations as a cover for criminal activity.

Level II Investigative techniques will be used as described in the First Amendment Worksheet initiating this investigation.

Michael J. Mealer
Commander
Intelligence Division

Approved:

Joseph Patterson
Deputy Chief
Bureau of Organized Crime

Nicholas J. Roti
Chief
Bureau of Organized Crime

cc/G.C. Price

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 7 of 25

RECEIVED
FBI - NEW YORK

JUL 11 2011 8-

FIRST AMENDMENT WORKSHEET

Chicago Police Department

Date and Time of Request
10 November 2011
First Amendment Invest. Tracking No.
191-2011-002

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank: Michael J. Mealer #95

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of

} a First Amendment investigation relating to:

Name and star number

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 10/14/11 (Time) 0900

Date Authorization Expires: 11/14/11 12/13/11 RP

FACTUAL BASIS FOR INVESTIGATION

For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination:

The [REDACTED] has gone national and manifested itself in Chicago as the [REDACTED] New York City on 01 October 2011. On 11 October 2011, 100 [REDACTED] protesters were arrested for trespassing during a demonstration. Other [REDACTED] participants in other cities around the country have been arrested for criminal acts and public disorder. The [REDACTED] has occupied the area around LaSalle and Jackson near the Federal Reserve and Bank of America building since the movement begun. To ensure that the Chicago Police Department can adequately prepare for large events developing from this movement and to determine whether participants are planning activities that involve violence, property destruction or large scale civil disorder, it is necessary to gather intelligence from [REDACTED] participants, meetings and formal and informal events.

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used:

The following investigative techniques will be used during this investigation: monitoring websites, collection of pamphlets and hand bills, trash covers and the use of undercover officers to attend public meetings.

See Attached Continuation Sheet

Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Members of violent anarchist groups who have been attributed with unlawful activity in the past attend meetings to engage others for unlawful conduct. For this reason, it is requested that undercover officers be allowed to attend public meetings to determine if any planning of unlawful acts or recruitment for unlawful acts are, or will be taking place.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Affiliation, if Any	I.R. No.
[REDACTED]	[REDACTED]	[REDACTED]

Signature of District Commander/Unit Commanding Officer of Exempt Rank <i>Michael J. Mealer</i>	Signature of General Counsel <i>Ryan L. R.</i>	Date 08 Nov 11	General Counsel's Determination: Concur <input checked="" type="checkbox"/> Do Not Concur <input type="checkbox"/>
CPD-11.440 (Rev. 10/03)			

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

Date and Time of Request
14 October 2011
First Amendment Invest. Tracking No.
191-2011-002

From: District Commander/ Unit Commanding Officer of Exempt Rank: Michael J. Mealer #95

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of }

a First Amendment investigation relating to:

Name and star number

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 10/14/11

(Time) 0900

Date Authorization Expires: 11/13/11

FACTUAL BASIS FOR INVESTIGATION

For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination:

[REDACTED] has gone national and has manifested itself in Chicago as the [REDACTED]
[REDACTED] engaged in public disorder and violations of the law that resulted in over 700 arrests in New York City on 1 October 2011. On 11 October 2011, 100 [REDACTED] protesters were arrested for trespassing during a demonstration. Other [REDACTED] participants in other cities around the country have been arrested for criminal acts and public disorder. The [REDACTED] has occupied the area around LaSalle and Jackson near the Federal Reserve and the Bank of America building since the movement begun. To ensure that the Chicago Police Department can adequately prepare for large events developing from this movement and to determine whether participants are planning activities that involve violence, property destruction or large scale civil disorder, it is necessary to gather intelligence from [REDACTED] participants, meetings and formal and informal events.

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used:

The following investigative techniques will be used during this investigation: monitoring websites, collection of pamphlets and hand bills, trash covers and the use of undercover officers to attend public meetings.

See Attached Continuation Sheet

Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Members of violent anarchist groups who have been attributed with unlawful activity in the past attend meetings to engage others for unlawful conduct. For this reason, it is requested that undercover officers be allowed to attend public meetings to determine if any planning of unlawful acts or recruitment for unlawful acts are, or will be taking place.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Signature of District Commander/Unit Commanding Officer of Exempt Rank

CPD-11.440 (Rev. 10/03)

Signature of General Counsel

Date

19 Oct 11

General Counsel's Determination:

Concur



Do Not Concur



14 October 2011

To: Garry F. McCarthy
Superintendent of Police

Attention: Ralph Price
General Counsel to the Superintendent

From: Michael J. Mealer
Commander
Intelligence Division

Subject: Request to Initiate a First Amendment Investigation

Reference: [REDACTED]
First Amendment Investigation Tracking Number: 191-2011-02
Department Special Order 02-01 "Investigations Directed at First
Amendment-Related Intelligence"

Initiation Date & Time: 14 October 2011 0900 hours

[REDACTED] has gone [REDACTED]. To ensure that national and has manifested itself in Chicago as [REDACTED] the Chicago Police Department can adequately prepare for large events developing from this movement and to determine whether participants are planning activities that involve violence, property destruction or large scale civil disorder, it is necessary to gather intelligence from [REDACTED] participants, meetings and formal and informal events.

The methods for gathering information for the public safety goals and to identify criminal activity will include undercover surveillance and undercover attendance at open and public meeting of groups planning demonstrations for the events. Review of open source material contained on the internet and public bulletin boards will also be necessary. If infiltration is required, a separate report will be generated requesting authorization. In all cases, the least invasive methods will be utilized.

The investigation is not expected to continue beyond thirty days, barring the discovery of intelligence that would warrant an extension request. Collection activity will be reviewed weekly.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 10 of 25

14 October 2011

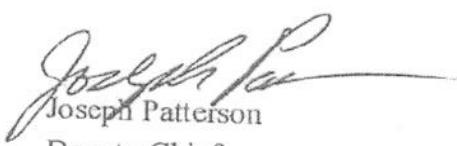
Page 2 of 2

FOR SIGNATURES ONLY



Michael J. Mealer
Commander
Intelligence Division

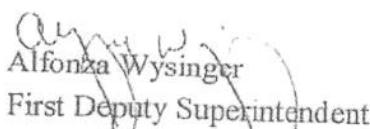
Approved:



Joseph Patterson
Deputy Chief
Bureau of Organized Crime



Nicholas J. Roti
Chief
Bureau of Organized Crime



Alfonza Wysinger
First Deputy Superintendent

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 11 of 25

19 OCT 11
12 51
FBI - NEW YORK

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

23 MAY 12 12 13

From: District Commander/ Unit Commanding Officer of Exempt Rank: Michael J. Mealer #95

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of

a First Amendment investigation relating to:

Investigation Initiated: (Date) 9/27/11

(Time) 1500

Name and star number

- Intelligence Gathering
 Public Gathering

Date Authorization Expires:

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation: for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination : The investigation is terminated due to the NATO event being completed and current extension expiring.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 12 of 25

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used :

See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.

Signature of District Commander/Unit Commanding Officer of Exempt Rank

CPD-11.440 (Rev. 10/03)

Signature of General Counsel

23 May 12

Date

General Counsel's Determination:

Concur



Do Not Concur



OFFICE OF THE SUPERINTENDENT
Office of Legal Affairs

22 May 2012

TO: Garry F. McCarthy
Superintendent of Police

ATTN: Nicholas J. Roti
Chief
Bureau of Organized Crime

Michael J. Mealer
Commander
Intelligence Division

FROM: Ralph M. Price
General Counsel
Office of the Superintendent

SUBJECT: First Amendment Extension Request
NATO Conference

REFERENCE: 191-2011-001

After consulting with Commander Michael Mealer of the Intelligence Division, First Amendment Investigation 191-2011-001 will terminate as scheduled on 22 May 2012.

Ralph M. Price
Ralph M. Price
General Counsel
Office of the Superintendent

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 13 of 25

22 MAY 12 17 33

U.S. GOVERNMENT PRINTING OFFICE: 2012 O-124-1

Bureau of Organized Crime
Intelligence Section

23 May 2012

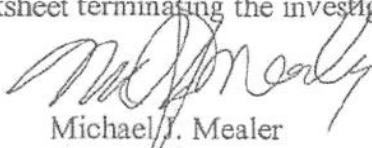
To: Nicholas J. Roti
Chief
Bureau of Organized Crime

From: Michael J. Mealer
Commander
Intelligence Division

Subject: 1st Amendment Investigation Termination
NATO Summit
Ref. 191-2011-001

The undersigned requests that the referenced First Amendment investigation is terminate due to the NATO event being completed.

A First Amendment Worksheet terminating the investigation is attached.



Michael J. Mealer
Commander
Intelligence Section

Approved:



Keith Calloway
Deputy Chief
Bureau of Organized Crime



Nicholas J. Roti
Chief
Bureau of Organized Crime

cc/G.C. Price

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 14 of 25

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

22 MAY 12 13 10

OFFICE OF LEGAL AFFAIRS

Date and Time of Request

21 May 2012

First Amendment Invest. Tracking No.

191-2011-001

From: District Commander/ Unit Commanding Officer of Exempt Rank: Michael J. McAlor #95

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of

} a First Amendment investigation relating to:

Name and star number

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 9/27/11 (Time) 1500

Date Authorization Expires:

FACTUAL BASIS FOR INVESTIGATION

- For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination:

Chicago is hosting the NATO conference between 19 May and 21 May 2012. When such conferences are held in other cities, demonstrations and protests have occurred that resulted in violence, property damage and civil disorder instigated and caused by infiltrators using the cover of lawful protest groups. As a recent example the Group of Twenty economic summit held in Pittsburgh, Pennsylvania in March 2009 resulted in civil disturbances that damaged property and resulted in numerous arrests. The Toronto G-20 After Action Report attributes the civil disorder to [REDACTED] and violent anarchist infiltrators to lawful protest groups. The lawful purpose to conduct this investigation is to acquire information to ensure adequate city resources are provided for lawful demonstration activity and to gather information to identify groups and individuals who may utilize lawful demonstrations as a cover for criminal activity. *This extension is requested pursuant to the attached memo.*

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used:

The following investigative techniques will be used during this investigation: monitoring websites, collection of pamphlets and hand bills, trash covers and the use of undercover officers to attend public meetings.

See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Members of violent anarchist groups who have been attributed with unlawful activity in the past attend meetings to engage others for unlawful conduct. For this reason, it is requested that undercover officers be allowed to attend public meetings to determine if any planning of unlawful acts or recruitment for unlawful activities are, or will be taking place.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Signature of District Commander/Unit Commanding Officer of Exempt Rank

CPD-11.440 (Rev. 10/03)

Signature of General Counsel

Ryan. Mc

Date

22 May 12

General Counsel's Determination:

Concur



Do Not Concur



Bureau of Organized Crime
Intelligence Division

21 May 2012

22 MAY 12 13 69

OFFICE OF LEGAL ATTACHE

To: Nicholas J. Roti
Chief
Bureau of Organized Crime

From: Michael J. Mealer
Commander
Intelligence Division

Subject: 1st Amendment Investigation Extension Request
G8/NATO Conference
Ref: 191-2011-001

The undersigned request a thirty day extension to the 1st Amendment Investigation due to NATO associated event occurring on 22 May 2012 at the Chicago Hilton Hotel, 720 S. Michigan. NATO participants will appear at the Hilton Hotel and current intelligence has disclosed that groups intend to protest the events. Current events have been infiltrated by [REDACTED] anarchists and continued investigation is necessary to ensure that the [REDACTED] cannot use violence and property damage to disrupt the protesters or the event.

Level II Investigative techniques will be used as described in the First Amendment Worksheet initiating this investigation.

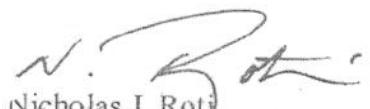


Michael J. Mealer
Commander
Intelligence Division

Approved:



Keith Calloway
Deputy Chief
Bureau of Organized Crime



Nicholas J. Roti
Chief
Bureau of Organized Crime

cc/G.C. Price

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 16 of 25

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank:

Michael J. Mealer #95

Date and Time of Request

18 April 2012

0900

First Amendment Invest. Tracking No.

191-2011-001

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of

} a First Amendment investigation relating to:

- Intelligence Gathering
 Public Gathering

Name and star number

Investigation Initiated: (Date) 9/27/11

(Time) 1500

Date Authorization Expires: 22 May 2012

FACTUAL BASIS FOR INVESTIGATION

- For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination : Chicago is hosting the NATO Conference between 19 May and 21 May 2012. When such conferences are held in other cities, demonstrations and protests have occurred that resulted in violence, property damage and civil disorder instigated and caused by infiltrators using the cover of lawful protest groups. As a recent example the Group of Twenty economic summit held in Pittsburgh, Pennsylvania in March of 2009 resulted in civil disturbances and damaged property and resulted in numerous arrests. The Toronto G-20 After Action report attributes the civil disorder to [REDACTED] and violent anarchist infiltrators to lawful protest groups. The lawful purpose to conduct this investigation is to acquire information to ensure adequate city resources are provided for lawful demonstration activity and to gather information to identify groups and individuals who may utilize lawful demonstrations as a cover for criminal activity.

ELECTRONICALLY FILED

7/2/2015 12:12 PM
2014-CH-15338

PAGE 17 of 25

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used :
 The following investigative techniques will be used during this investigation: monitoring websites, collection of pamphlets and hand bills, trash covers and the use of undercover officers to attend public meetings.

See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Members of violent anarchist groups who have been attributed with unlawful activity in the past attend meetings to engage others for unlawful conduct. For this reason, it is requested that undercover officers be allowed to attend public meetings to determine if any planning of unlawful acts or recruitment for unlawful acts are, or will be taking place.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.

Signature of District Commander/Unit Commanding Officer of Exempt Rank

CPD-11.440 (Rev. 10/03)

Signature of General Counsel

Ronnie Rice 20 Nov 13

Date

General Counsel's Determination:

Concur



Do Not Concur



Bureau of Organized Crime
Intelligence Section

18 April 2012

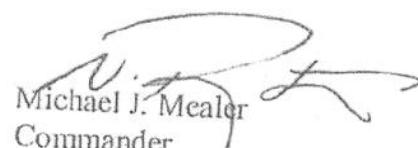
To: Nicholas J. Roti
Chief
Bureau of Organized Crime

From: Michael J. Mealer
Commander
Intelligence Section

Subject: 1st Amendment Investigation Extension Request
NATO Conference
Ref: 191-2011-001
6th Extension Expiration Date: 22 April 2012

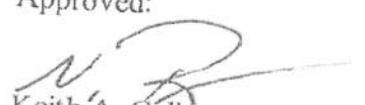
The undersigned request a 30 day extension to the 1st Amendment Investigation to continue to gather information and intelligence to ensure adequate city resources are provided for lawful demonstration activity and to gather information to identify groups and individuals who may utilize lawful demonstrations as a cover for criminal activity.

Level II Investigative techniques will be used as described in the First Amendment Worksheet initiating this investigation.

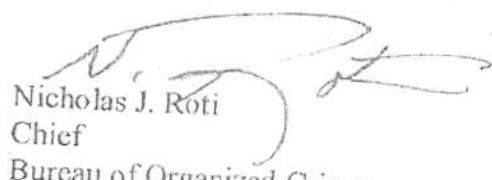


Michael J. Mealer
Commander
Intelligence Section

Approved:



Keith A. Calloway
Deputy Chief
Bureau of Organized Crime



Nicholas J. Roti
Chief
Bureau of Organized Crime

cc/G.C. Price

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 18 of 25

20 APR 12 12 2012

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank:

Michael J. Mealer #95

Date and Time of Request	20 March 2012	0905
First Amendment Invest. Tracking No.	191-2011-001	

Initial Authorization to Conduct

Name and star number

Authorization to Continue

Intelligence Gathering

Order to Terminate/Disapproval Of

Public Gathering

} a First Amendment investigation relating to:

Investigation Initiated: (Date) 9/27/11

(Time) 1500

Date Authorization Expires: 4/22/12

FACTUAL BASIS FOR INVESTIGATION

For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination : Chicago is hosting the NATO Conference between 19 May and 21 May 2012. When such conferences are held in other cities, demonstrations and protests have occurred that resulted in violence, property damage and civil disorder instigated and caused by infiltrators using the cover of lawful protest groups. As a recent example the Group of Twenty economic summit held in Pittsburgh, Pennsylvania in March 2009 resulted in civil disturbances and damaged property and resulted in numerous arrests. The Toronto G-20 After Action report attributes the civil disorder to [REDACTED] and violent anarchist infiltrators to lawful protest groups. The lawful purpose to conduct this investigation is to acquire information to ensure adequate city resources are provided for lawful demonstration activity and to gather information to identify groups and individuals who may utilize lawful demonstrations as a cover for criminal activity.

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used :

The following investigative techniques will be used during this investigation: monitoring websites, collection of pamphlets and handouts, trash covers and the use of undercover officers to attend public meetings.

See Attached Continuation Sheet

Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Members of violent anarchist groups who have been attributed with unlawful activity in the past attend meetings to engage others for unlawful conduct. For this reason, it is requested that undercover officers be allowed to attend public meetings to determine if any planning of unlawful acts or recruitment for unlawful acts are, or will be taking place.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	ER# No.
			53
			72
			13

Signature of District Commander/Unit Commanding Officer of Exempt Rank

Signature of General Counsel

Micheal J. Mealer 23 March 12

Date

General Counsel's Determination:

Concur



Do Not Concur



Bureau of Organized Crime
Intelligence Division

20 March 2012

To: Nicholas J. Roti
Chief
Bureau of Organized Crime

From: Michael J. Mealer
Commander
Intelligence Division

Subject: 1st Amendment Investigation Extension Request
NATO Conference
Ref: 191-2011-001
5th Extension Expiration Date: 23 March 2012

The undersigned request a 30 day extension to the 1st Amendment Investigation to continue to gather information and intelligence to ensure adequate city resources are provided for lawful demonstration activity and to gather information to identify groups and individuals who may utilize lawful demonstrations as a cover for criminal activity.

Level II Investigative techniques will be used as described in the First Amendment Worksheet initiating this investigation.



Michael J. Mealer
Commander
Intelligence Division

Approved:



Keith A. Calloway
Executive Officer
Bureau of Organized Crime



Nicholas J. Roti
Chief
Bureau of Organized Crime

cc/G.C. Price

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15328
PAGE 20 of 25

23 MAR 12 13 46

Office of Legal Affairs

BUREAU OF ORGANIZED CRIME

26 March 2012

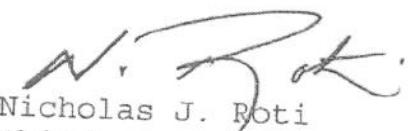
BOC# 12-0154

To: Ralph M. Price
General Counsel
Office of the Superintendent

From: Nicholas J. Roti
Chief
Bureau of Organized Crime

Subject: 1st Amendment Investigation Extension Request

Please see attached regarding 1st Amendment
Investigation Extension Request.



Nicholas J. Roti
Chief
Bureau of Organized Crime

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 21 of 25

23 MAR 12 13 16
U.S. DEPT. OF JUSTICE, WASH., D.C.

NR/sb
Attachments:

FIRST AMENDMENT WORKSHEET

Chicago Police Department

Date and Time of Request
17 February 2012
First Amendment Invest. Tracking No.
191-2011-001

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank: Michael J. Mealer #95

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of }

a First Amendment investigation relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 9/27/11 (Time) 1500

Date Authorization Expires: 3/23/12

FACTUAL BASIS FOR INVESTIGATION

For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination: Chicago is hosting the Group of Eight Summit and NATO conference between 19 May and 21 May 2012. When such conferences are held in other cities, demonstrations and protests have occurred that resulted in violence, property damage and civil disorder instigated and caused by infiltrators using the cover of lawful protest groups. As a recent example the Group of Twenty economic summit held in Pittsburgh, Pennsylvania in March 2009 resulted in civil disturbances and damaged property and resulted in numerous arrests. The Toronto G-20 After Action report attributes the civil disorder to [REDACTED] and violent anarchist infiltrators to lawful protest groups. The lawful purpose to conduct this investigation is to acquire information to ensure adequate city resources are provided for lawful demonstration activity and to gather information to identify groups and individuals who may utilize lawful demonstrations as a cover for criminal activity.

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used:

The following investigative techniques will be used during this investigation: monitoring websites, collection of pamphlets and hand bills, trash covers and the use of undercover officers to attend public meetings.

See Attached Continuation Sheet

Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Members of violent anarchist groups who have been attributed with unlawful activity in the past attend meetings to engage others for unlawful conduct. For this reason, it is requested that undercover officers be allowed to attend public meetings to determine if any planning of unlawful acts or recruitment for unlawful acts are, or will be taking place.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.

Signature of District Commander/Unit Commanding Officer of Exempt Rank

CPD-11.440 (Rev. 10/03)

Signature of General Counsel

Date

21 Feb 12

General Counsel's Determination:

- Concur
 Do Not Concur

Bureau of Organized Crime
Intelligence Division

17 February 2012

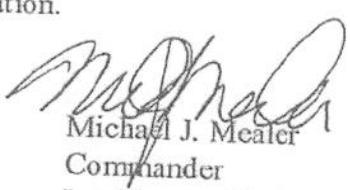
To: Nicholas J. Roti
Chief
Bureau of Organized Crime

From: Michael J. Mealer
Commander
Intelligence Division

Subject: 1st Amendment Investigation Extension Request
G8/NATO Conference
Ref: 191-2011-001
4th Extension Expiration Date: 22 February 2012
Requested Extension: 23 March 2012

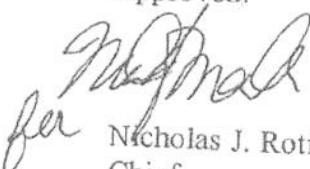
The undersigned request a 30 day extension to the 1st Amendment Investigation to continue to gather information and intelligence to ensure adequate city resources are provided for lawful demonstration activity and to gather information to identify groups and individuals who may utilize lawful demonstrations as a cover for criminal activity.

Level II Investigative techniques will be used as described in the First Amendment Worksheet initiating this investigation.



Michael J. Mealer
Commander
Intelligence Division

Approved:



Nicholas J. Roti
Chief
Bureau of Organized Crime

cc/G.C. Price

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 23 of 25

17 FEB 12
FBI - NEW YORK

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank: Michael J. Mealer #95

Date and Time of Request	19 January 2012	140
First Amendment Invest. Tracking No.	191-2011-001	

Initial Authorization to Conduct }
 Authorization to Continue }
 Order to Terminate/Disapproval Of } a First Amendment investigation
 relating to:

Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 9/27/11 (Time) 1500 Date Authorization Expires: 2/22/12

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination : Chicago is hosting the Group of Eight Summit and NATO conference between 19 May and 21 May 2012. When such conferences are held in other cities, demonstrations and protests have occurred that resulted in violence, property damage and civil disorder instigated and caused by infiltrators using the cover of lawful protest groups. As a recent example the Group of Twenty economic summit held in Pittsburgh, Pennsylvania in March 2009 resulted in civil disturbances that damaged property and resulted in numerous arrests. The Toronto G-20 After Action Report attributes the civil disorder to [REDACTED] and violent anarchist infiltrators to lawful protest groups. The lawful purpose to conduct this investigation is to acquire information to ensure adequate city resources are provided for lawful demonstration activity and to gather information to identify groups and individuals who may utilize lawful demonstrations as a cover for criminal activity.

ELECTRONICALLY FILED

7/2/2015 12:12 PM
2014-CH-15338
PAGE 24 of 25

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used :

The following investigative techniques will be used during this investigation: monitoring websites, collection of pamphlets and hand bills, trash covers and the use of undercover officers to attend public meetings.

See Attached Continuation Sheet

Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Members of violent anarchist groups who have been attributed with unlawful activity in the past attend meetings to engage others for unlawful conduct. For this reason, it is requested that undercover officers be allowed to attend public meetings to determine if any planning of unlawful acts or recruitment for unlawful activities are, or will be taking place.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	T.R. No.
[REDACTED]	[REDACTED]	[REDACTED]	123
[REDACTED]	[REDACTED]	[REDACTED]	123
[REDACTED]	[REDACTED]	[REDACTED]	123
[REDACTED]	[REDACTED]	[REDACTED]	123
[REDACTED]	[REDACTED]	[REDACTED]	123
[REDACTED]	[REDACTED]	[REDACTED]	123
[REDACTED]	[REDACTED]	[REDACTED]	123
[REDACTED]	[REDACTED]	[REDACTED]	123

Signature of District Commander/Unit Commanding Officer of Exempt Rank:

CPD-11.440 (Rev. 10/03)

Signature of General Counsel:

Ryan P. [REDACTED]

Date

19 Jan 12

General Counsel's Determination:

Concur



Do Not Concur



FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

21 DEC 11 12:00

Date and Time of Request

19 December 2011

1/300

First Amendment Invest. Tracking No.

191-2011-001

From: District Commander/ Unit Commanding Officer of Exempt Rank:

Michael J. Mealer #95

Name and star number

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of }

a First Amendment investigation
relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 9/27/11

(Time) 1500

Date Authorization Expires: 1/23/12

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination : Chicago is hosting the Group of Eight Summit and NATO conference between 19 May and 21 May 2012. When such conferences are held in other cities, demonstrations and protests have occurred that resulted in violence, property damage and civil disorder instigated and caused by infiltrators using the cover of lawful protest groups. As a recent example the Group of Twenty economic summit held in Pittsburgh, Pennsylvania in March 2009 resulted in civil disturbances that damaged property and resulted in numerous arrests. The Toronto G-20 After Action Report attributes the civil disorder to [REDACTED] and violent anarchist infiltrators to lawful protest groups. The lawful purpose to conduct this investigation is to acquire information to ensure adequate city resources are provided for lawful demonstration activity and to gather information to identify groups and individuals who may utilize lawful demonstrations as a cover for criminal activity.

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used :

The following investigative techniques will be used during this investigation: monitoring websites, collection of pamphlets and hand bills, trash covers and the use of undercover officers to attend public meetings.

See Attached Continuation Sheet

Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Members of violent anarchist groups who have been attributed with unlawful activity in the past attend meetings to engage others for unlawful conduct. For this reason, it is requested that undercover officers be allowed to attend public meetings to determine if any planning of unlawful acts or recruitment for unlawful activities are, or will be taking place.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, If Any	I.R. No.

Signature of District Commander/Unit Commanding Officer of Exempt Rank

Signature of General Counsel

Date

21 Dec 11

General Counsel's Determination:

Concur



Do Not Concur



ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
CALENDAR: 11
PAGE 1 of 20
CIRCUIT COURT OF
COOK COUNTY, ILLINOIS
CHANCERY DIVISION
CLERK DOROTHY BROWN

Bureau of Organized Crime
Intelligence Division

19 December 2011

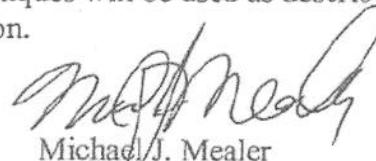
To: Nicholas J. Roti
Chief
Bureau of Organized Crime

From: Michael J. Mealer
Commander
Intelligence Division

Subject: 1st Amendment Investigation Extension Request
G8/NATO Conference
Ref. 191-2011-001
2nd Extension Expiration Date: 24 December 2011
Requested Extension: 23 January 2012

The undersigned request a 30 day extension to the 1st Amendment Investigation to continue to gather information and intelligence to ensure adequate city resources are provided for lawful demonstration activity and to gather information to identify groups and individuals who may utilize lawful demonstrations as a cover for criminal activity.

Level II Investigative techniques will be used as described in the First Amendment Worksheet initiating this investigation.



Michael J. Mealer
Commander
Intelligence Division

Approved:



Joseph Patterson
Deputy Chief
Bureau of Organized Crime



Nicholas J. Roti
Chief
Bureau of Organized Crime

cc/G.C. Price

21 DEC 11 12 28

FIRST AMENDMENT WORKSHEET

Chicago Police Department

Date and Time of Request
14 November 2011
First Amendment Invest. Tracking No.
191-2011-001

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank: Michael J. Mealer #95

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of }

a First Amendment investigation relating to:

Name and star number

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 9/27/11 (Time) 1500

Date Authorization Expires: 11/24/11

13/24/11
M

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination : Chicago is hosting the Group of Eight Summit and the NATO conference between 19 May 2012 and 21 May 2012. When such conferences are held in other cities, demonstrations and protests have occurred that resulted in violence, property damage and civil disorder instigated and caused by infiltrators using the cover of lawful protest groups. As a recent example, the Group of Twenty economic summit held in Pittsburgh, Pennsylvania in March 2009 resulted in civil disturbances that damaged property and resulted in numerous arrests. The Toronto G-20 After Action Report attributes the civil disorder to [REDACTED] and violent anarchist infiltrators to lawful protest groups. The lawful purpose to conduct this investigation is to acquire information to ensure adequate city resources are provided for lawful demonstration activity and to gather information to identify groups and individuals who may utilize lawful demonstrations as a cover for criminal activity.

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used :

The following investigative techniques will be used during this investigation: monitoring websites, collection of pamphlets and hand bills, trash covers and the use of undercover officers to attend public meetings.

See Attached Continuation Sheet

Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Members of violent anarchist groups who have been attributed with unlawful activity in the past attend meetings to engage others for unlawful conduct. For this reason, it is requested that undercover officers be allowed to attend public meetings to determine if any planning of unlawful acts or recruitment for unlawful activities are, or will be taking place.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.

Signature of District Commander/Unit Commanding Officer of Exempt Rank

Signature of General Counsel

Ryan P. Ri

Date

15 Nov 11

General Counsel's Determination:

- Concur
 Do Not Concur

Bureau of Organized Crime
Intelligence Division

14 November 2011

02/02/2011 12:12 PM

15 NOV 11 12 17

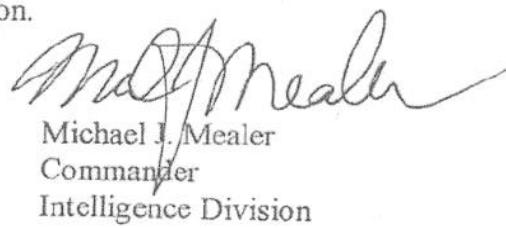
To: Nicholas J. Roti
Chief
Bureau of Organized Crime

From: Michael J. Mealer
Commander
Intelligence Division

Subject: 1st Amendment Investigation Extension Request
G8/NATO Conference
Ref: 191-2011-001
1st Extension Expiration Date: 24 November 2011
Requested Extension: 24 December 2011

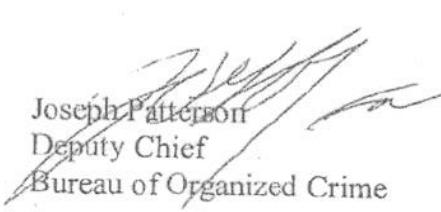
The undersigned request a 30 day extension to the 1st Amendment Investigation to continue to gather information and intelligence to ensure adequate city resources are provided for lawful demonstration activity and to gather information to identify groups and individuals who may utilize lawful demonstrations as a cover for criminal activity.

Level II Investigative techniques will be used as described in the First Amendment Worksheet initiating this investigation.

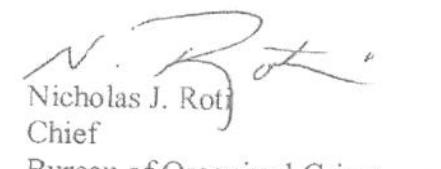


Michael J. Mealer
Commander
Intelligence Division

Approved:



Joseph Patterson
Deputy Chief
Bureau of Organized Crime



Nicholas J. Roti
Chief
Bureau of Organized Crime

cc/G.C. Price

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 3 of 20

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank: Michael J. Mealer #95

Date and Time of Request
24 October 2011
First Amendment Invest. Tracking No.
191-2011-001

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of }

a First Amendment investigation relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 9/27/11

(Time) 1500

Date Authorization Expires: 11/24/11

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination : Chicago is hosting the Group eight Summit and NATO conference between 19 May 2012 and 21 May 2012. When such conferences are held in other cities, demonstrations and protests have occurred that resulted in violence, property damage and civil disorder instigated and caused by infiltrators using the cover of lawful protest groups. As a recent example the Group of twenty economic summit held in Pittsburgh, Pennsylvania in March 2009, resulted in extensive property damage and numerous arrests. The Group of Twenty summit held in June 2010 in Toronto, Ontario, Canada also resulted in civil disturbances that damaged property and resulted in numerous arrests. The Toronto G-20 After Action Report attributes the civil disorder to violent anarchist infiltrators to lawful protest groups. The lawful purpose to conduct this investigation is to acquire information to ensure adequate city resources are provided for lawful demonstration activity and to gather information to identify groups and individuals who may utilize lawful demonstrations as a cover for criminal activity.

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used :

The following investigative techniques will be used during this investigation: monitoring websites, collection of pamphlets and hand bills, trash covers and the use of undercover officers to attend public meetings.

See Attached Continuation Sheet

Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Members of violent anarchist groups who have been attributed with unlawful activity in the past attend meetings to engage others for unlawful conduct. For this reason, it is requested that undercover officers be allowed to attend public meetings to determine if any planning of unlawful acts or recruitment for unlawful activities are, or will be taking place.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.

Signature of District Commander/Unit Commanding Officer of Exempt Rank

CPD-11.440 (Rev. 10/03)

Signature of General Counsel

R. M. Pi

Date

01 NOV 11

General Counsel's Determination:

Concur

Do Not Concur

BUREAU OF ORGANIZED CRIME

27 October 2011
BOC# 11-0335

To: Ralph M. Price
General Counsel
Office of the Superintendent

From: Nicholas J. Roti
Chief
Bureau of Organized Crime

Subject: First Amendment Investigation Extension Request

Please see attached regarding First Amendment
Investigation Extension for the Intelligence Division, Unit 191.



Nicholas J. Roti
Chief
Bureau of Organized Crime

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 5 of 20

27 OCT 11 10 13

NR/sb
Attachments:

Bureau of Organized Crime
Intelligence Division

21 October 2011

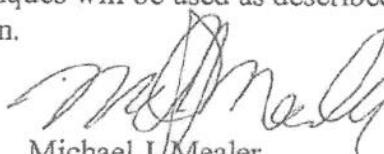
To: Nicholas J. Roti
Chief
Bureau of Organized Crime

From: Michael J. Mealer
Commander
Intelligence Division

Subject: 1st Amendment Investigation Extension Request
G8/NATO Conference
Ref: 191-2011-001
Original Expiration Date: 26 October 2011
Requested Extension: 24 November 2011

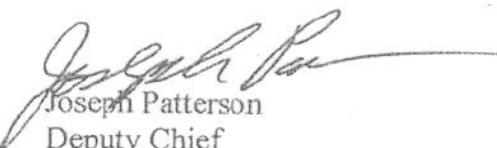
The undersigned request a 30 day extension to the 1st Amendment Investigation to continue to gather information and intelligence to ensure adequate city resources are provided for lawful demonstration activity and to gather information to identify groups and individuals who may utilize lawful demonstrations as a cover for criminal activity.

Level II Investigative techniques will be used as described in the First Amendment Worksheet initiating this investigation.



Michael J. Mealer
Commander
Intelligence Division

Approved:



Joseph Patterson
Deputy Chief
Bureau of Organized Crime



Nicholas J. Roti
Chief
Bureau of Organized Crime

cc/G.C. Price

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 6 of 20

27 OCT 11 10 11 2011

2014-CH-15338

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

From: District Commander/ Unit Commanding Officer of Exempt Rank: Michael J. Mealer #95

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of

} a First Amendment investigation relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 9/27/11 (Time) 1500

Date Authorization Expires: 10/26/11

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination : Chicago is hosting the Group of Eight Summit and NATO conference between 19 May 2012 and 21 May 2012. When such conferences are held in other cities, demonstrations and protests have occurred that resulted in violence, property damage and civil disorder instigated and caused by infiltrators using the cover of lawful protest groups. As a recent example the Group of Twenty economic summit held in Pittsburgh, Pennsylvania in March 2009, resulted in extensive property damage and numerous arrests. The Group of Twenty summit held in June 2010 in Toronto, Ontario, Canada also resulted in civil disturbances that damaged property and resulted in numerous arrests. The Toronto G-20 After Action Report attributes the civil disorder to [REDACTED] and violent anarchist infiltrators to lawful protest groups. The lawful purpose to conduct this investigation is to acquire information to ensure adequate city resources are provided for lawful demonstration activity and to gather information to identify groups and individuals who may utilize lawful demonstrations as a cover for criminal activity.

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used :
The following investigative techniques will be used during this investigation: monitoring websites, collection of pamphlets and hand bills, trash covers and the use of undercover officers to attend public meetings.

See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

Members of violent anarchist groups who have been attributed with unlawful activity in the past attend meetings to engage others for unlawful conduct. For this reason it is requested that undercover officers be allowed to attend public meetings to determine if any planning of unlawful acts or recruitment for unlawful activities are, or will be taking place.

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, If Any	I.R. No.

Signature of District Commander/Unit Commanding Officer of Exempt Rank

Michael J. Mealer

9/27/11

Signature of General Counsel

Ryan Rie

Date

28 Sept 11

General Counsel's Determination:

Concur



Do Not Concur



ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 8 of 20

28 SEP 11 11 10

Bureau of Organized Crime
Intelligence Division

15 September 2011

To: Garry F. McCarthy
Superintendent of Police

Attention: Ralph Price
General Counsel to the Superintendent

From: Michael J. Mealer
Commander
Intelligence Division

Subject: Request to Initiate a First Amendment Investigation

Reference: G8/NATO Conferences
First Amendment Investigation Tracking Number: 191-2011-01
Department Special Order 02-01 "Investigations Directed at First
Amendment-Related Intelligence"

Initiation Date & Time: Effective upon approval

The G8/NATO Conferences are scheduled to be held in Chicago between 19 May 2012 and 21 May 2012. When held in other cities, demonstrations and protests have occurred. Some demonstrations have resulted in violence, property damage and civil disorder instigated and caused by infiltrators using the cover of lawful protest groups. In order to protect and facilitate the lawful demonstrations that are likely to occur during the events, to protect the citizens and businesses of the city of Chicago, and to adequately plan for security for the events, the Intelligence Division requests approval to initiate a First Amendment Investigation. The investigation is necessary to acquire information to ensure adequate city resources are provided for demonstration activity. Information gathering must also identify groups and individuals who may utilize lawful demonstrations as cover for criminal activity.

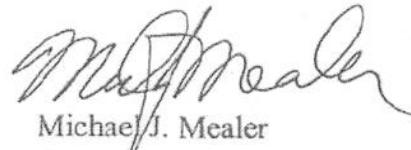
The methods for gathering information for the public safety goals and to identify criminal activity will include undercover surveillance and undercover attendance at open and public meeting of groups planning demonstrations for the events. Review of open source material contained on the internet and public bulletin boards will also be necessary. If infiltration is required, a separate report will be generated requesting authorization. In all cases, the least invasive methods will be utilized.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 9 of 20

15 September 2011

Page 2 of 2

The investigation is expected to last until the end of the G8/NATO event. Pursuant to department directives, the initial authorization can be no longer than 120 days from date of approval. A report requesting continued authorization will be submitted prior to the 120 days unless instructed otherwise. Collection activity will be reviewed biweekly.



Michael J. Mealer

Commander

Intelligence Division

Approved:



Joseph Patterson

Deputy Chief

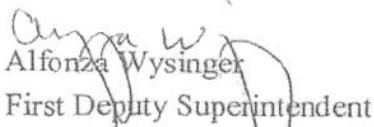
Bureau of Organized Crime



Nicholas J. Roti

Chief

Bureau of Organized Crime



Alfonza Wysinger

First Deputy Superintendent

Cc/ Chief Debra Kirby

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 10 of 20

FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

12 NOV 16 15 02

OFFICIAL USE ONLY

Date and Time of Request

07 Nov 2014

10/12

First Amendment Invest. Tracking No

001-116-2014

From: District Commander/ Unit Commanding Officer of Exempt Rank:

Steven Culuris #520

Name and star number

Initial Authorization to Conduct

Authorization to Continue

Order to Terminate/Disapproval Of

} a First Amendment investigation
relating to:

Intelligence Gathering

Public Gathering

Investigation Initiated: (Date) 11/7/14

(Time) 1600

Date Authorization Expires: 12/7/14

FACTUAL BASIS FOR INVESTIGATION

- For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination :

There has been a "call to action" on many open source websites and social media posts concerning the police related shooting of Mike Brown and the pending Grand Jury decision surrounding the involved officer. Missouri has been experiencing multiple large crowd gatherings along with violent criminal incidents surrounding public response. A number of individuals and organizations involved in the activity in Ferguson, Mo are from Chicago. Locally we've seen multiple social media posts by these same organizations calling for protests here and associating calls for civil disobedience once the Grand Jury decision is rendered. The undersigned seeks authorization to monitor open source communications involving these specific groups to both determine gathering locations, levels of interest, as well as to identify criminal concerns to ensure public safety. Attached are social media posts and information reports as examples of interest.

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used :

Officers will utilize social media searches only on an open source basis

See Attached Continuation Sheet

Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.
[REDACTED]			

Signature of District Commander/Unit Commanding Officer of Exempt Rank

Signature of General Counsel

Reported 10/12/2014

Date

General Counsel's Determination:

Concur



Do Not Concur



FIRST AMENDMENT WORKSHEET

Chicago Police Department

To: Superintendent of Police
Attention: General Counsel

-5 DEC 14 16 32

Date and Time of Request
5 Dec 2014 1330 hour
First Amendment Invest. Tracking No.
001-116-2014

From: District Commander/ Unit Commanding Officer of Exempt Rank:

STEVEN CALURIS #500

Name and star number

- Initial Authorization to Conduct
- Authorization to Continue
- Order to Terminate/Disapproval Of } a First Amendment investigation relating to:

- Intelligence Gathering
- Public Gathering

Investigation Initiated: (Date) 12/5/14

(Time) 1330 hours

Date Authorization Expires: 1/5/15

FACTUAL BASIS FOR INVESTIGATION

For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination : A request to extend the First Amendment initiated on 11/7/14 is being made. The investigation conducted during the time frame has found posts on social media sites that note to "shut down the Ryan" and "shut down the Ryan again." On 3Dec 14, the decision of a Grand Jury in New York City to not indict a New York Police Department Officer was announced. That decision and continuation of the Ferguson related event precipitated large scale protests around the country, to include Chicago on 4 Dec 14. At 1700 hours on 4 Dec 14, protesters walked through the Central Business District and ended up in the northbound lanes of Lake Shore Drive at approximately North Avenue. As a result, traffic had to be shut down. Prior to this, some protesters entered the southbound lanes of I-94 at Roosevelt Road, thereby stopping traffic. Protesters laid down in some intersections during the course of the protest thereby disrupting traffic and impeding the movement of emergency vehicles and pedestrians. This protest resulted in four arrests and injuries to three officers. A protest/march is scheduled for 8 Dec 14 on the UIC Campus in the Medical District. Social media posts with regards to "shut down

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used : Officers will utilize social media searches only on an open source basis

See Attached Continuation Sheet

- Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

PERSONS OR GROUPS TO BE INVESTIGATED

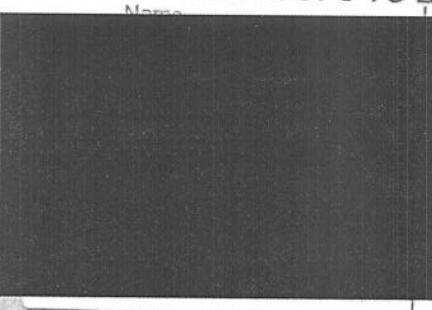
Name

Address

Affiliation, if Any

I.R. No.

See Attached Continuation Sheet



Signature of District Commander/Unit Commanding Officer of Exempt Rank

Signature of General Counsel

Date

General Counsel's Determination:

Concur



Do Not Concur



FIRST AMENDMENT INVESTIGATION TRACKING #
001-116-2014

-5 DEC 14 16 32

OFFICE OF LEGAL AFFAIRS

FIRST AMENDMENT WORKSHEET

CONTINUATION PAGE

FACTUAL BASIS FOR INVESTIGATION (continued)

"Chicago" have been noted in regards to this event in the Medical District. This location is in very close proximity to the Expressway System. As a result of the aforementioned, it is requested to add the noted persons or groups to the "persons or groups to be investigated" section.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 13 of 20

FIRST AMENDMENT WORKSHEET

Chicago Police Department

Date and Time of Request
5 Jan 15 1000 hours
First Amendment Invest. Tracking No.
001-116-2014

To: Superintendent of Police
Attention: General Counsel

-5 JAN 15 11 32

From: District Commander/ Unit Commanding Officer of Exempt Rank: Commander Steven Caluris #520

Name and star number

- Initial Authorization to Conduct
 Authorization to Continue
 Order to Terminate/Disapproval Of }

a First Amendment investigation relating to:

- Intelligence Gathering
 Public Gathering

Investigation Initiated: (Date) 11/7/14

(Time) 1600 hours

Date Authorization Expires: 1/5/15

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination :
The undersigned requests to terminate this First Amendment Investigation. The investigation conducted during the aforementioned time frame found posts on social media to indicate plans to disrupt traffic, thereby hindering the movement of emergency vehicles. Those posts included the following: "to shut the chicago Dan Ryan Down!" #shutdownchicago, "take over the Dan Ryan." The following posts were also found, "#emptythemalls" and "SIGNS DOWN GUNS UP LETS KILL A COP," "And pick up your guns. Let's start killing cops." During the course of this First Amendment investigation, approximately forty three demonstrations/protests were held. Some of those demonstrations/protests involved subjects entering an expressway and laying down in intersections which hindered the movement of emergency vehicles. The information found via open source searching of the Internet was communicated to Department command staff charged with ensuring the safety of the protesters/demonstrators and the public so that the demonstration/protest could take place. This First Amendment investigation was limited to open source searching of the Internet. It was begun on 7 Nov 14 at 1600

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 14 of 20

See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used :

See Attached Continuation Sheet

Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.

Signature of District Commander/Unit Commanding Officer of Exempt Rank

Signature of General Counsel

Date

General Counsel's Determination:

Concur



Do Not Concur





INVESTIGATIONS DIRECTED AT FIRST AMENDMENT-RELATED INFORMATION

ISSUE DATE:	01 May 2015	EFFECTIVE DATE:	01 May 2015
RESCINDS:	19 April 2012 Version		
INDEX CATEGORY:	Human Rights and Community Partnerships		

I. PURPOSE

This directive establishes the responsibilities and procedures for:

- A. the special approval and authorization required for permissible First Amendment information gathering investigations.
- B. documenting investigations of public gatherings.
- C. the retention of documents related to First Amendment information gathering.

NOTE: Department members will refer to the General Order titled "Investigations Directed at First Amendment-Related Information" for examples of permissible and impermissible First Amendment-related investigations.

SPECIAL AUTHORIZATIONS REQUIRED FOR PERMISSIBLE FIRST AMENDMENT INFORMATION GATHERING INVESTIGATIONS**A. Approvals and Authorization****1. First Amendment-Related Investigation Initiation Report**

A member who seeks to conduct a First Amendment-related information gathering investigation will submit to his or her exempt commanding officer a To-From-Subject report, addressed to the Superintendent of Police, Attention: General Counsel, and containing an approval line for the member's exempt commanding officer and the chief of the member's bureau. The report will contain the following information:

- a. Date and time the investigation will be initiated;
- b. Basis of initiating the investigation and the reasonable law enforcement purpose of the investigation;
- c. Methods of investigation sought to be employed and why these methods are likely to be more effective than less invasive investigative methods;
- d. Amount of time the investigation is expected to last.

2. Exempt Commanding Officer Approval and the First Amendment Worksheet (CPD-11.440)

- a. The exempt commanding officer who receives a To-From-Subject report initiating a First Amendment-related information gathering investigation will approve the request only if he or she determines that the investigation is in accordance with the Department policy expressed in the General Orders titled "The First Amendment

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 15 of 20

and Police Actions" and "Investigations Directed at First Amendment-Related Information."

NOTE: In the absence of an exempt commanding officer, the exempt commanding officer of the next higher rank will assume this responsibility.

b. If the exempt commanding officer approves the investigation, he or she will:

(1) complete a First Amendment Worksheet, assigning a proper First Amendment Investigation tracking number to the worksheet using the following formula:

- (a) the requesting unit number will appear first, followed by a dash;
- (b) the calendar year will appear second, followed by a dash;
- (c) the last number in the series will be the sequential number of the First Amendment-related investigation for that unit, as evidenced by that unit's First Amendment Investigation Unit Log.

EXAMPLE: A number of 188-2012-03 will designate the third First Amendment-related investigation for Unit 188 in the year 2012. This number will be recorded on the First Amendment Worksheet in the upper right-hand corner.

- (2) provide written authorization for the investigation to the initiating member in the form of a copy of the completed First Amendment Worksheet containing the date on which the authorization will expire and any limits on the use of investigative methods.
- (3) submit the approved To-From-Subject initiation report and the completed First Amendment Worksheet to the chief of his or her bureau.

3. Chief Approval

A chief who receives an approved To-From-Subject report initiating a First Amendment-related information gathering investigation will approve the request only if he or she determines that the investigation is in accordance with the policy expressed in the General Orders titled "The First Amendment and Police Actions" and "Investigations Directed at First Amendment-Related Information." If approved, the chief will submit the To-From-Subject initiation report, the First Amendment Worksheet, and any other pertinent materials to the General Counsel to the Superintendent.

4. General Counsel Concurrence

The General Counsel will determine if the investigation is permitted by the First Amendment and Department policy and ensure that the investigation does not duplicate another ongoing, approved First Amendment-related investigation. The General Counsel will review the submitted materials and either:

- a. sign a concurrence on the First Amendment Worksheet where indicated, based upon the information provided, and return the original To-From-Subject initiation report and First Amendment Worksheet to the submitting chief.
- b. if not in concurrence with an authorization, contact the affected chief in an attempt to resolve any concerns. If such concerns cannot be resolved, the matter will be submitted to the First Deputy Superintendent for a decision. If the First Deputy Superintendent determines that the investigation shall be initiated, the First Deputy Superintendent will sign the concurrence in place of the General Counsel.

5. Notwithstanding the requirement of special authorization, a member may initiate and conduct a First Amendment-related information gathering investigation without prior special authorization, provided:

- a. it is impractical to submit the required paperwork prior to initiating the investigation;
- b. an exempt commanding officer has verbally approved the investigation, however, the use of an infiltrator may be approved verbally **only** by the Superintendent; and,
- c. all required paperwork is submitted as soon as practicable but in no event later than twenty-four (24) hours after the initiation of the investigation.

B. Additional Authorization Necessary For Use of Infiltrator

Any use of an infiltrator requires the prior approval of the Superintendent. A request to use an infiltrator will be submitted in a separate To-From-Subject report in the form of a First Amendment-related investigation initiation report, in accordance with the requirements of such a report as indicated in Item II-A-1 of this directive, with an additional approval line for the Superintendent.

C. Continued Monitoring

Members will continually assess the authorized use of undercover methods and determine whether the use of these methods remain warranted in light of the information generated by these methods. Members conducting the investigation will submit to their exempt commanding officer To-From-Subject reports detailing the progress of the investigation at thirty-day (30) intervals or at shorter intervals as directed by the exempt commanding officer. The exempt commanding officer may revoke his or her approval at any time for good reason and will, upon such revocation, notify his or her chief. A chief may revoke his or her approval at any time for good reason. Upon the revocation of either approval, the investigation will be terminated.

D. Time Limits on Authorizations of Investigations

1. Authorization to conduct First Amendment-related information gathering will be in effect for a period not to exceed one hundred twenty (120) days and may be approved in increments not to exceed one hundred twenty (120) days in order to ensure that the investigation remains in accordance with the First Amendment and Department policy and procedure. Prior to the expiration of the initial or succeeding authorized periods, application may be made for an additional period of up to one hundred twenty (120) days, beginning upon the expiration of the preceding period, in a To-From-Subject report to the chief of the bureau containing the investigative unit. If the authorized period expires without proper approval of an extension, the investigation is automatically terminated.
2. Authorization to employ undercover methods will be in effect for a period not to exceed thirty (30) days and may be approved in shorter increments in order to ensure that the investigation remains in accordance with the First Amendment and Department policy and procedure. Prior to the expiration of the initial or succeeding authorized periods, application may be made for an additional period of up to thirty (30) days, beginning upon the expiration of the preceding period, in a To-From-Subject report to the chief of the bureau containing the investigative unit. If the authorized period expires without proper approval of an extension, the investigation is automatically terminated.
3. Continued use of an infiltrator after the expiration of the initial authorized period also requires application for an extension for up to thirty (30) days, in the form of a separate To-From-Subject report to the chief, with an additional approval line for the Superintendent.

E. Terminations

Upon termination of the investigation, by expiration or otherwise, the exempt commanding officer of the investigating unit will complete a First Amendment Worksheet detailing the basis for and the date of the termination of the investigation and submit that Worksheet to his or her chief for forwarding to the General Counsel. All members involved in the investigation will be notified of the termination, and all documents will be retained and/or forwarded as indicated in Item IV of this directive.

III. PUBLIC GATHERINGS AND FIRST AMENDMENT CONDUCT

A. Documenting Investigations of Public Gatherings

Information obtained during the course of such a preliminary investigation will be made the subject of an Automated Information Report, in order to facilitate future assessments of resources and public safety. That report, along with pertinent attachments, will be forwarded through the chain of command to the chief of the bureau of the member and to the First Deputy Superintendent. The Automated Information Report will be treated, maintained, and retained in accordance with Department policy for non-First Amendment-related investigations.

B. Video Recording, Audio Recording, and Photographing Public Gatherings

Video recording and photographing of events on the public way are generally appropriate and may be conducted for any proper law enforcement purpose, including documenting violations of law, monitoring police conduct, defending against allegations of police misconduct, aiding in the future coordination and deployment of police resources, and training. Furthermore, audio recording may be authorized at the discretion of an exempt commanding officer as circumstances warrant, including documenting the issuance of police orders, warnings, or notices.

1. If done for any of the above reasons, video recording, audio recording, or photographing a public gathering is not an investigation directed toward First Amendment-related information within the meaning of this directive, and the retention and disposal of such video recording, audio recording, or photographs will follow the restrictions outlined in Item III-B-4 of this directive.
2. If video recording, audio recording, or photographing is done as part of an First Amendment-related information gathering investigation, the retention and disposal of such video recordings, audio recording, or photographs will follow the restrictions outlined in Item IV of this directive. Each video recording, audio recording, or photograph will be identified by its own unique tracking number.
3. Video recording, audio recording, and photographing public gatherings must be approved by an exempt commanding officer. The exempt commanding officer will determine, based upon operational needs, who or which unit will conduct the video recording, audio recording, or photographing. The officer in charge of the event will ensure that the video recording, audio recording, or photographing equipment is available and used appropriately.
4. Retention of Video Recordings, Audio Recordings, or Photographs Taken at Public Gatherings
 - a. As soon as practicable, the unit which conducted the video recording, audio recording, or photographing will send a To-From-Subject report to the persons listed below, indicating the nature of the video recording, audio recording, or photographs, the fact that they will be held within the unit for ninety (90) days, and requesting a written signature acknowledging that there is no known reason to retain them past the ninety-day time period. Reasons for retention of the video recording, audio recording, or photographs include future training or planning purposes or allegations of criminal conduct or officer misconduct arising out of the event for which the video recording, audio recording, or photographs may be useful.
 - (1) Office of the General Counsel;
 - (2) Chief, Bureau of Detectives;
 - (3) Deputy Chief, Education and Training Division;
 - (4) Chief, Bureau of Support Services;
 - (5) Commander, Special Events Unit
 - (6) Chief Administrator, Independent Police Review Authority.
 - b. If the persons listed above all sign an acknowledgment that there is no known reason to retain the video recording, audio recording, or photographs, then the unit retaining

the video recording, audio recording, or photographs will dispose of them but retain the signed acknowledgments in unit files. If any person listed in Item III-B-4-a-(1) through (6) requests that the video recording, audio recording, or photographs be retained due to future training or planning purposes or due to allegations of criminal conduct or officer misconduct arising out of the event, then the person requesting retention will direct the unit where to send the video recording, audio recording, or photographs. The sending unit will document the transfer of the video recording, audio recording, or photographs in a To-From-Subject report, which will be signed by a member at the accepting unit to indicate receipt of the video recording, audio recording, or photographs. The To-From-Subject report will be retained in original unit files.

IV. RETENTION OF DOCUMENTS RELATING TO FIRST AMENDMENT-RELATED INFORMATION INVESTIGATIONS

- A. The exempt commanding officer of the investigating unit will retain the documents, video recordings, audio recordings, or photographs related to a First Amendment-related information gathering investigation until the latter of:
 1. the time that the documents, video recordings, audio recordings, or photographs cease to serve a proper law enforcement purpose (for instance, the information becomes stale); OR
 2. the investigation is closed.
- B. Upon the later expiration of the two preceding events, the exempt commanding officer will forward all documents, video recordings, audio recordings, or photographs related to this investigation, including all copies, to the Chief, Bureau of Support Services, with a To-From-Subject report indicating the action taken and the reason for the action (i.e., that the information is no longer relevant or that the investigation closed on a date indicated in the report). A copy of this report will also be directed to the Commander, Inspections Division.
- C. Upon receipt of documents, video recordings, audio recordings, or photographs from the exempt commanding officer, the Chief, Bureau of Support Services will retain them until the next internal First Amendment audit, at which time the Chief, Bureau of Support Services, will turn over the materials to the Inspections Division. The Chief, Bureau of Support Services will address a To-From-Subject report to the Commander, Inspections Division, indicating the date that the documents, video recordings, audio recordings, or photographs are turned over. The report and the related materials will be hand-carried to the Inspections Division, where a member of that division will sign a copy of the To-From-Subject report to indicate receipt of the materials. The Chief, Bureau of Support Services will retain that signed received copy of the To-From-Subject report for a period of three (3) years.
- D. The Inspections Division will maintain and preserve the documents, video recordings, audio recordings, or photographs from First Amendment-related investigations received from the Chief, Bureau of Support Services, for a period of three (3) years from the close of the investigation.

NOTE: This retention schedule will ensure that the documents will be available to defend any First Amendment-related lawsuit (such lawsuit being required to be filed within two years of the incident). Upon learning of the filing of any such lawsuit, the Inspection Division will suspend any destruction of relevant documents without regard to the retention schedule described above.

- E. The General Counsel will maintain a copy of all First Amendment Worksheets for a period of three years from the close of the investigation.
- F. Notwithstanding anything in this directive, the exempt commanding officer of the investigating unit or the respective chief may forward a copy of a report detailing information gathered in an investigation governed by this directive to the Deployment Operations Section, if appropriate, to serve a reasonable law enforcement purpose. The exempt commanding officer of the investigative unit will document the forwarding of the copy of such information to the Deployment Operations Section in a To-From-Subject report containing the action taken, the date of such action, and the reason for the action.

- G. Notwithstanding anything in this directive, the exempt commanding officer of the investigative unit or the respective chief may forward to the appropriate unit(s), copies of any information gathered in an investigation governed by this directive which relate to a threat to the physical safety of a dignitary or to a public gathering.

Authenticated by: KC

Garry F. McCarthy
Superintendent of Police

15-004 TSS

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 20 of 20

Chicago police are spying on citizens

Authorities have conducted surveillance on activists in recent years but won't say why.

By Mick Dumke

@mickeyd1971 and Ben Joravsky

@joravben

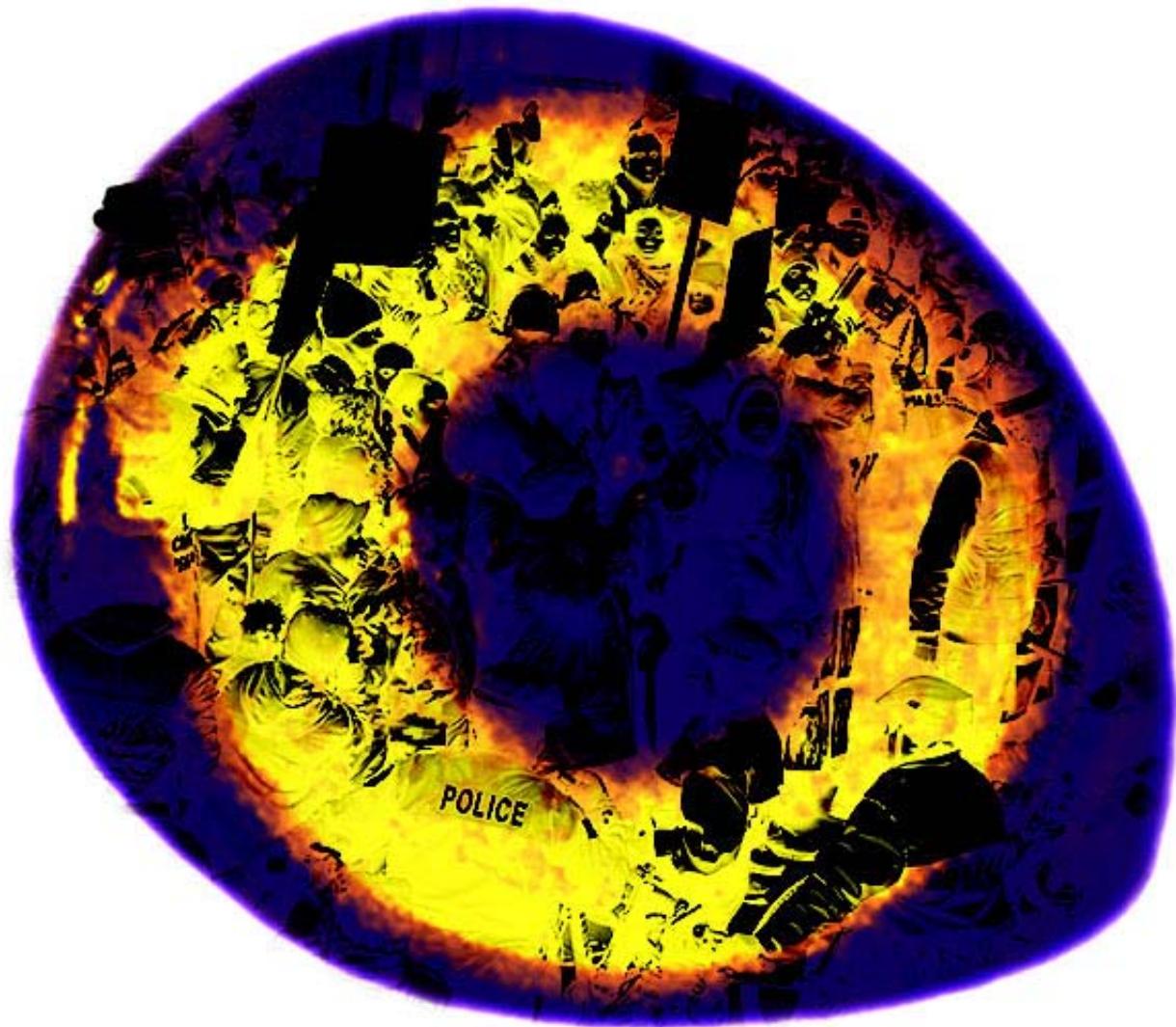


PHOTO ILLUSTRATION: SUE KWONG; PHOTOS: SCOTT OLSON, MOHAMMED ALNASER

At least one thing became clear last year during the trial of the so-called NATO Three: the Chicago Police Department spied on citizens exercising their First Amendment right to free speech.

Exhibit 1-B

The three defendants were acquitted of terrorism but convicted of mob action and arson charges, an outcome that largely hinged on the testimony of two undercover Chicago police officers nicknamed "Mo" and "Gloves," who had [posed as radicals to infiltrate local activist groups](#). As prosecutors continued to defend the case in the aftermath of the trial, we wondered: Have the police been conducting surveillance on other protesters and activist organizations around town?

The answer is yes.

Since 2009 the Chicago Police Department has opened at least six investigations that involved spying on citizens, internal police records show. Four of the investigations were launched during the first term of Mayor Rahm Emanuel.

We acquired the records from the department through a Freedom of Information Act request made last November. Specifically, we asked for copies of the paperwork required when police open what they call "First Amendment-related investigations," which are prompted by or based upon a person's speech or other expression," according to department rules. These investigations could include undercover officers, infiltration of protest groups, or electronic surveillance such as wiretaps or StingRay cell-phone tracking devices that can intercept calls, texts, and e-mails.

In response, the police department sent 26 pages of records in which most of the essential information was blacked out—including sections showing who was being investigated, what the justification was, and which methods police used.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE of

[Chicago Police Department's "First Amendment Worksheets," acquired through a FOIA request](#)



Nonetheless, the heavily redacted records do offer a glimpse of what the police have been up to.

For instance, on March 14, 2009, when former mayor Richard M. Daley was in office, the police launched an "intelligence gathering" operation that was authorized through April 13 of that year.

As with all of these investigations, it was approved by some of the highest-ranking officials in the department, including the general counsel for the police superintendent, who was then Jody Weis.

The names of the people being investigated are blacked out in the records we received, but it was authorized just two weeks before Chicago hosted a delegation from the International Olympic Committee, which ultimately decided which city would get the games in 2016. [Daley's Olympics proposal](#) had stirred up opposition from a number of quarters, including police officers upset about delays in getting a new contract. When the IOC delegation arrived on April 3, 2009, roughly 1,000 off-duty officers formed a ring around City Hall chanting, "No contract, no Olympics!" Were the police actually spying on police? Only the police know.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 7 OF 7

The next known investigation was requested on October 26, 2009, and lasted for just one day. That happened to coincide with a convention of the American Bankers Association in the Gold Coast. While the bankers were in town, protests were held throughout the city.

One demonstration against mortgage policies tied to thousands of foreclosures featured Reverend Jesse Jackson and Senator Richard Durbin.

The police requested another one-day investigation on January 20, 2011. Again, the subjects and rationale were redacted from our copies of the records. But it's possibly related to a January 21 visit by Chinese president Hu Jintao, who was being ushered around town by Mayor Daley. Hu's visit brought out protesters who objected to China's occupation of Tibet. The police investigation was officially terminated at 10 PM on January 21, a few hours after the protesters disbanded.

Police spying really picked up later in 2011, according to the records, after newly elected Mayor Emanuel and his old boss President Obama announced that NATO would hold a summit in Chicago the following spring. Within weeks, anti-NATO protesters around the country were vowing to hold demonstrations in Chicago during the summit.

On September 27, 2011, the general counsel for police superintendent Garry McCarthy authorized an undercover operation into NATO protesters, though the summit was months away. The section of the records listing the specific people or groups targeted by the investigation was left blank.

Then, on October 14, a simultaneous undercover operation was launched into the small but vociferous Occupy Chicago movement that had camped out in the city's financial district and in Grant Park. In their authorization forms, the police said they needed to "determine whether participants are planning activities that involve violence, property destruction or large scale civil disorder."

Two days later, Chicago police moved into Grant Park and arrested about 200 Occupy activists who were camped there. A Cook County judge later vacated the arrests on the grounds that they were unconstitutional.

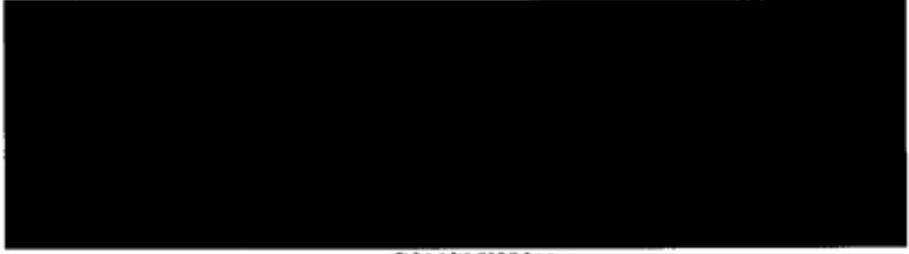
Even as the Occupy and NATO investigations were under way, police officials proposed a third surveillance operation. That request was made on January 12, 2012, and would have focused on three people or groups—but we don't know who they were, because the names were again blacked out in our copies. McCarthy's general counsel turned down the request for the investigation. We have no evidence that it went forward.

The police department officially closed its Occupy investigation on January 19, 2012. "As of this time, the Occupy Movement has had a significant lack of participants," the termination notice says in one of the few sentences that was not redacted in the 26 pages of records we received.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15328
PAGE 2 of 2

Information Exempt Under Section 7(1)(d)(vi)

It is also the position of the Department that redacted information in the records provided to the requester are exempt from disclosure pursuant to sections 7(1)(d)(vi) of FOIA (5 ILCS 140/7(1)(d)(vi)). The below italicized information is confidential and shall not be disclosed to the requester:

CONCLUSION

For the reasons stated above, the Department requests that your office find that the Department is in conformance with FOIA and deny the instant request for review. Should you have any questions or concerns, please contact me at your convenience.

Sincerely,

Terrence Collins

Terrence Collins
Office of Legal Affairs
Chicago Police Department

In a letter to the Illinois attorney general's office, a lawyer for the Chicago Police Department blacked out even his explanation of why the department won't release key information about police surveillance.

By the time police wrapped up the Occupy investigation, the surveillance of potential NATO protesters was in full effect. Undercover police Mo and Gloves—whose real names are Mehmet Uygun and Nadia Chikko—"gathered intelligence and information in various locations, including coffee shops, meetings, protests, rallies and concerts in an effort to root out any plans for criminal activity before, during or after the NATO summit," according to documents later filed in court by prosecutors.

For a while, Mo and Gloves infiltrated the movement against Mayor Emanuel's [closure of six mental health clinics](#). Mo was even arrested at a rally outside the shuttered Woodlawn clinic and hauled to a jail cell. There he was handcuffed to Matthew Ginsberg-Jaeckle, a leading mental health activist.

"He was trying to get me to say something incendiary," Ginsberg-Jaeckle told

the *Reader* last summer. "He kept saying, 'We need to take it to the next level.' I said, 'I don't know what you mean. But whatever it is—this is not a place to discuss it.' I mean, we're in a jail cell."

On May 16, 2012, police accompanied by agents from the FBI arrested three out-of-town protesters—Brent Betterly, Brian Church, and Jared Chase—who became known as the NATO Three. Betterly, Church, and Chase were charged with conspiring to commit terrorism, primarily based on testimony from Mo and Gloves, who said the three had plotted to attack police stations and President Obama's campaign headquarters and shoot an arrow at Mayor Emanuel's house.

The attorneys for the defense were convinced that the spying operation was far more extensive than the work of Mo and Gloves. Prosecutors initially listed other police officers as potential witnesses in the case, and records indicated that FBI agents had also been working on surveillance. In a court filing, defense attorneys asked to see additional police intelligence reports. But Cook County judge Thaddeus Wilson rejected the motion, saying it went beyond the charges against the NATO Three.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 6 of 6

The three protesters ended up sitting in jail for more than a year before their case came to trial. In February 2014 a jury cleared them of the terrorism charges, and in April, Wilson sentenced each of them to between five and eight years in prison, much less than the 14 years sought by state's attorney Anita Alvarez.

That was the end of the NATO Three case—but not the end of police spying.

Police officials authorized another investigation on November 7 of last year. Four individuals or groups were listed as subjects, but their names were blacked out in the records provided to us.

The authorization came two days after a rally against police shootings was held outside police headquarters in Bronzeville.

Organizer Page May believes undercover officers have attended meetings of We Charge Genocide, a group that coordinated the rally outside police headquarters. She says she's also seen police filming public protests since the shooting of Michael Brown by police in

Ferguson, Missouri, last year. "It seemed really ominous," she says. "I'm a black, queer woman, and this is the thing that scares me the most about the organizing I do."

Chicago Police Department spokesman Marty Maloney says police work to protect free speech rights and have closed down streets for protest marches in recent months.

"CPD cannot specifically discuss open investigations," he wrote in an e-mailed statement. "However, we always ensure any investigations are done to further protect residents' rights and conducted in full compliance with the Constitution. In no way does CPD ever target those critical of the police."

The department's own rules state that surveillance of protest groups should be undertaken only if they would serve a "reasonable law enforcement purpose," which can include any investigation "intended to address unlawful conduct." Officials must then spell out the purpose and scope of the surveillance before getting approval from the police superintendent's general counsel.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014CH-15338
PAGE 7

After we received the documents, we asked the Illinois attorney general's office to review whether the police department was violating the FOIA law by redacting the reports.

A couple weeks later, a lawyer for the state ordered police officials to explain how releasing records of closed investigations could "obstruct an ongoing investigation" or "jeopardize the safety of undercover personnel."

In response, a police department lawyer wrote: "It is also the position of the Department that redacted information in the records . . . [is] exempt from disclosure."

He went on to explain his reasoning by writing that—well, we don't know what he wrote, because the explanation was also blacked out.

In other words, citizens don't even have the right to know why they can't know why police are spying on them.

**THERE'S MORE OUT THERE THAN
WHAT ZILLOW'S SHOWING YOU.**

Search more MLS-listed, for-sale properties on [realtor.com](#)



THE WALL STREET JOURNAL.

WSJ.com

September 21, 2011, 10:33 PM ET

How 'Stingray' Devices Work

By Jennifer Valentino-DeVries

Law enforcement and the military are using devices called "stingrays" to track cellphones, as described in a story in today's Wall Street Journal. The government considers the devices sensitive information, and not much is known publicly about how they are used. But it's possible to get a good idea of how they work based on public documents and interviews with technology experts.

The systems involve an antenna, a computer with mapping software, and a special device. The device mimics a cellphone tower and gets the phone to connect to it. It can then collect hardware numbers associated with the phone and can ping the cellphone even if the owner isn't making a call. This can be done through walls — something that is useful in finding suspects as well as victims of crimes or accidents.

There are two ways to use the devices, says Matt Blaze, a computer science professor at the University of Pennsylvania and a former researcher at AT&T Labs.

One way is to point the antenna at a location and collect the hardware numbers there. These numbers can be used to determine which phones are in a given place at a given time.

The devices also can be used to locate a phone when the officers know the numbers associated with it but don't know precisely where it is. In that case, the officers can drive around until they get a signal from the target phone while pinging it.

Once a signal is found, the stingray setup measures its strength and can provide a general location on the map. The officer can then move to another location and again measure the signal strength.

By collecting the signaling information from several locations, the system can triangulate the location of the phone more precisely.

Mr. Blaze said stingrays alter the normal behavior of cellular devices. In addition, the stingray was used in mode that allowed it to force the broadband card to communicate.

"They are getting your card to do something it doesn't normally do," Mr. Blaze said. "It's pairing with a simulated base station rather than the usual base station."

The exact way these stingray devices work is one of the big questions in a case currently playing out in U.S. District Court for the District of Arizona. The defense in that case wants to know just how the stingray was able to locate a mobile broadband card in an apartment building. The card was key in the later arrest

Exhibit 1-C

of the defendant on fraud charges.

Related article: [‘Stingray’ Phone Tracker Fuels Constitutional Clash](#)

Copyright 2015 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our [Subscriber Agreement](#) and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 2 of 2

5 Cal. L. Rev. Circuit 259

California Law Review Circuit

May, 2014

**TO UNSEAL OR NOT TO UNSEAL: THE JUDICIARY'S ROLE IN PREVENTING
 TRANSPARENCY IN ELECTRONIC SURVEILLANCE APPLICATIONS AND ORDERS**

Brian L. Owsley ^{a1}

Copyright © 2014 California Law Review, Inc., Brian L. Owsley

INTRODUCTION

For eight years, I served as a United States magistrate judge in the Corpus Christi Division of the Southern District of Texas. In our division, we dealt with a large number of criminal matters, some of which required me to review sealed applications for search warrants, pen registers, trap and trace devices, and other various forms of electronic surveillance, such as those pursuant to the Stored Communications Act.¹ During my term, I signed orders granting hundreds of such applications,² and all of these applications and orders were *260 routinely sealed at the request of the United States Attorney because they involved ongoing criminal investigations.³

It makes sense that they were initially sealed so as to prevent any targets of the investigation from learning that they were indeed being investigated. Otherwise, these suspects might destroy evidence of their crimes, intimidate witnesses from cooperating, or flee the jurisdiction. Eventually, however, these applications and orders should have been unsealed. Documents are not supposed to remain sealed forever. Indeed, the Supreme Court has explained that, as a general rule, judicial records are to be open to the public, in part so that citizens may “keep a watchful eye on the workings of public agencies.”⁴

The process of unsealing electronic surveillance applications and orders falls squarely within a magistrate judge's duties.⁵ This Essay discusses my experience when I attempted to unseal a number of old applications and orders, and analyzes the ramifications of the judiciary's reluctance to unseal such documents.

I.

**ONE MAGISTRATE JUDGE'S FAILED ATTEMPT TO UNSEAL
 APPLICATIONS FOR ELECTRONIC SURVEILLANCE ORDERS**

In April 2013, as I was taking care of various administrative details before leaving the bench, I decided that I was going to unseal most, if not all, of the electronic surveillance applications and orders that I had considered and signed while I served as a magistrate judge unless there was some compelling reason to keep them sealed, such as an ongoing criminal investigation. I did not view this decision as a particularly controversial one. Moreover, I did not consider the matters involved to be extraordinarily interesting to anyone in particular. I instead thought that if I did not unseal these documents, they were likely to remain sealed for all of eternity. I felt that the reason for keeping most, if not all, of the documents sealed no longer existed because the criminal cases that *261 formed the bases of the applications were long over. I also thought that government works best when it is transparent.

I began the process of unsealing these documents by compiling a list of each sealed application that I had previously handled. I then divided the applications into three groups based on when they were filed. Initially, I issued individual orders for each application in the oldest group, explaining that I would unseal the materials unless I received an objection from the United

Exhibit 2-D

States Attorney within a specified time period. This first group contained applications that were all over five years old, so it was quite likely that the investigations were no longer ongoing if arrests had not been made, as the federal criminal statute of limitations would likely have run. Alternatively, any target that was prosecuted would likely have been convicted and sentenced already. After this first wave of orders, I subsequently issued individual orders in two more waves, addressing the remaining two groups of applications.

While I waited for the government to decide whether to object to the unsealing of any applications, I spoke with the supervisory Assistant United States Attorney for the Corpus Christi office regarding my orders. In response to his questions, I explained that his office did not need to file anything if it did not object to the release. Interestingly, because the files in the first group were so old, his office did not even have records regarding each application. Moreover, because they were all still sealed, the other Assistant United States Attorneys and staff could not review them. Ultimately, the supervisory Assistant United States Attorney filed a single global request in each application affected by my show-cause order seeking authority for staff members to review the applications in the clerk's office in order to get the basic information he felt was necessary to respond to my order.

The deadline to respond to the first wave of orders came and went without any objections from the United States Attorney. Consequently, I issued individual orders instructing the Clerk of the Court to unseal the relevant applications and orders and to make them electronically available. I then turned my attention to other matters.

A few days after issuing the orders to unseal the first wave of applications, one of the district judges summoned me into his chambers. He told me that he had learned of my orders to unseal the various applications and that he was not going to allow them to go forward. We discussed the matter briefly, and I explained that the United States Attorney had not objected to the unsealing. I noted that the orders I had issued only affected old cases. I also told the judge that although the sealing of the documents was necessary when the applications were filed, keeping them sealed was no longer necessary, and the federal Courts, like the rest of the federal government, should operate with some transparency. The judge indicated that the United States Attorney's decision not to object was unimportant because its attorneys could not be relied upon to safeguard the all of the relevant interests. In the end, he issued an order *262 quashing my hundreds of orders to unseal. Additionally, his order contained virtually no reasoning or analysis justifying the continued sealing of any of the applications: "The Order of United States Magistrate Judge Brian Owsley providing for notice of unsealing of orders and associated pen register and trap and trace applications is VACATED. Those orders and their applications will remain sealed until further order of the Court."⁶ Of course, the judge's order was also sealed.⁷

It is unusual that a district judge would sua sponte issue an order quashing orders to unseal. If the United States Attorney had filed a motion before the district judge in response to my original order, seeking to bar me from going forward with the unsealing, then the district judge would be in a proper position to address the matter.⁸ Similarly, if the United States Attorney had filed objections indicating the reasons why the applications should remain sealed, but I had nonetheless ordered that they should be unsealed, then the United States Attorney could appeal my order to the district judge, and the district judge would again be in a proper position to address the matter. However, because no party had sought relief or action from the district judge regarding the matter, it struck me as highly irregular for the judge to intervene. Such an intervention was analogous to a trial court rendering a decision in some action and, without any appeal, the appellate court issuing a ruling reversing the trial judge's decision. Furthermore, he perpetuated the sealing of these hundreds of documents, seemingly without ever reviewing any of them.

The district judge's approach here was additionally problematic because the unsealing of files by a magistrate judge is not only permissible but routinely done.⁹ Indeed, a magistrate judge within the same court, the Southern District of Texas, has routinely unsealed similar applications and orders.¹⁰ This demonstrates magistrate judges are able to unseal such documents and that there is no reason to continue sealing all of these documents. Thus, not only is *263 there a problem with the continued sealing of documents, but there is also a problem in the Court appearing inconsistent and arbitrary in its approach to this issue.

III.

WHY DOES SEALING DOCUMENTS IN PERPETUITY MATTER?

Why is all of this important? Maybe it is not. After all, most of these applications and orders are fairly straightforward and routine. In my experience these applications dealt with common crimes in our division: narcotics trafficking, the smuggling of undocumented aliens, child pornography, etc.¹¹ However, they almost never involved any novel issues of law or high-profile investigations. In other words, they would be of little interest to most people.

Nevertheless, even if no one ever wanted to or wants to view these applications and orders, they should still be unsealed and made available barring some extraordinary circumstance that would justify keeping them sealed.¹² Federal courts do not sit as a Star Chamber, deciding matters while cloaked in secrecy.¹³ Indeed, public policy and the U.S. Constitution favor the unsealing of such documents: “A government operating in the shadow of secrecy stands in complete opposition to the society envisioned by the Framers of our Constitution.”¹⁴

Furthermore, even though the applications and orders were routine on an individual level, the privacy implications of perpetually sealed surveillance orders might alarm the public. One need only look at the recent public uproar over NSA's electronic surveillance program to know that most people are very concerned about these invasions of privacy. Unfortunately, continued sealing of applications and orders regarding pen registers, trap and trace devices, search warrants, and § 2703(d) orders¹⁵ prevents the public from understanding the scope of the matters involved and from serving its role as a check on government action.

***264** Given that these documents should be unsealed, one must consider which parties should be responsible for initiating the process. The failure to request the unsealing of old applications can be attributed partly to inertia. In the narrative that I described, the party originally seeking to have the applications and orders sealed no longer felt they needed to be sealed,¹⁶ but this did not mean that the party would actively seek to have them unsealed. Indeed, during my term, the United States Attorney never requested to unseal any of these types of documents. Busy federal prosecutors rightly focus more on the present and future investigation and prosecution of criminal activity, not the reexamination of long-concluded cases and investigations.

Additionally, the targets of such surveillance would seemingly have some interest in unsealing these applications. However, they often have much more pressing concerns, such as staving off charges or a conviction. Moreover, their defense attorneys have little incentive or strategic basis for wasting time focusing on such applications. Defense attorneys would have received the substantive information obtained through the surveillance orders when an Assistant United States Attorney attempted to use it in the course of prosecution. In addition, federal prosecutors would be required to provide any information that formed the basis for the applications or any exculpatory evidence obtained pursuant to the court orders.¹⁷ Even if defense attorneys were able to unseal and review these applications, the revealed information would be of little benefit for most of them, as there is no suppression remedy.¹⁸

That essentially leaves the courts to monitor and unseal these files when appropriate. However, as my former colleague United States Magistrate Judge Stephen Smith has explained, magistrate judges in the Houston Division of the Southern District of Texas issued 3,886 orders regarding electronic surveillance applications between 1995 and 2007.¹⁹ He further concluded that “[a]s of 2008, 99.8% of those orders remained sealed, long after the underlying criminal investigation was closed.”²⁰ Needless to say, there is also inertia on the part of ***265** federal judges, who, like prosecutors, are busy focusing on pending matters not long-closed ones.

To be sure, almost all of these sealed documents are routine in their focus. Nonetheless, as a whole, they paint a telling picture for those who care to look. One can see what types of crimes are investigated. Additionally, one can ascertain the information

that the United States Attorney typically relies on in filing its applications. Upon review of an application, additional research could reveal whether the subjects of the criminal investigation were ever indicted or convicted, as well as whether they were indicted or convicted of the offense that was originally being investigated.

CONCLUSION

How can the problem of unsealing electronic surveillance applications and orders best be addressed? As one might imagine, the solution lies with federal judges. Ideally, magistrate judges and district judges would ensure sealed documents, including those documents that are routinely unsealed in the applications and orders discussed here, would be routinely unsealed after a reasonable time period. Yet, as a practical matter, many judges just do not consider it an issue.

If judges cannot be relied upon to sort this problem out, what other options remain? Prosecutors and defense attorneys have little incentive to unseal documents. Congress is unlikely to enact any legislation on this issue any time soon.²¹ This essentially leaves the public. Individuals will have to make requests to open up access to the courts. Perhaps these requests can be made in conjunction with media interest and public service organizations just as those groups push for transparency by ensuring that newsworthy controversial hearings are open to the public. Eventually, one would hope that such actions would encourage the courts to return to their proper role in regulating the matter of unsealing these surveillance applications and orders in a more transparent fashion.

Footnotes

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 4 of 6

¹ Brian L. Owsley, Visiting Assistant Professor, Texas Tech University School of Law; BA, 1988, University of Notre Dame; JD, 1993, Columbia University School of Law; MIA, 1994, Columbia University School of International and Public Affairs. From 2005 until 2013, the author served as a United States magistrate judge for the United States District Court for the Southern District of Texas. This article was written in the author's private capacity. No official support or endorsement by the United States District Court for the Southern District of Texas or any other part of the federal judiciary is intended or should be inferred. I am very grateful for valuable comments and critiques provided by Jonah Horwitz and the Hon. Stephen Wm. Smith.

² See generally [FED. R. CRIM. P. 41](#) (search warrants); [18 U.S.C. § 3122 \(2014\)](#) (pen registers and trap and trace devices); [18 U.S.C. § 2703 \(2009\)](#) (disclosure of cell phone communications or records).

³ The number of sealed documents pertaining to these requests for electronic surveillance authorization is staggering. By one assessment, federal magistrate judges handle over thirty thousand such applications a year. Stephen Wm. Smith, [*Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*](#), 6 HARV. L. & POL'Y REV. 313, 322 (2012).

⁴ See [*Kamakana v. City & Cnty. of Honolulu*](#), 447 F.3d 1172, 1178 (9th Cir. 2006) (noting that a few narrow categories of documents are sealed by federal courts, including "warrant materials in the midst of a pre-indictment investigation"); [*United States v. Ketner*](#), 566 F. Supp. 2d 568, 589 (W.D. Tex. 2008) (explaining the need to seal documents relating to an investigation "to preserve the integrity of the Government's investigation and prevent witness intimidation").

⁵ Nixon v. Warner Commc'nns, Inc., 435 U.S. 589, 598 (1978) (citations omitted); see also [*In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703\(d\)*](#), 707 F.3d 283, 290 (4th Cir. 2013) ("the common law presumes a right to access *all* judicial records and documents" (emphasis in original)).

⁶ See [*In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703\(d\)*](#), 707 F.3d at 289 (stating that the authority to unseal surveillance applications and orders falls within the additional duties contemplated in the Federal Magistrates Act); see also [*In re Search of a Residence which is Situated on a Cul-De-Sac at 14905 Franklin Drive, Brookfield, Wis.*](#), 121 F.R.D. 78, 79 (E.D. Wis. 1988) ("The power to unseal is concomitant to the authority to seal.").

⁷ Order Vacating Order to Show Cause, [*In re the Appl. of the United States for an Order: \(1\) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device; & \(2\) Authorizing Release of Subscriber & Other Info No. 2:05-MC-50*](#), et al. (S.D. Tex.

Apr. 19, 2013) (citing 18 U.S.C. § 3123(d)(1)). Section 3123(d)(1) simply reiterates that “the order be sealed until otherwise ordered by the court.”

7 Id.

8 As a general rule, district judges conduct the first-line review of many decisions and orders issued by magistrate judges. However, such review presumes that there is some dispute being raised by a party. *See, e.g.,* 28 U.S.C. § 636(b)(1) (discussing review of a magistrate judge's proposed findings and recommendations only after a party has “serve[d] and file[d] written objections to such proposed findings and recommendations as provided by rules of court”).

9 *See, e.g., Search of a Residence which is Situated on a Cul-De-Sac at 14905 Franklin Drive, Brookfield, Wis., 121 F.R.D. at 79.*

10 *See In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders,* 562 F. Supp. 2d 876 (S.D. Tex. 2008) (holding that a fixed expiration date was to be set as to the sealing and non-disclosure of electronic surveillance orders so that they would be unsealed unless the Government filed a motion to continue the sealing).

11 *See, e.g., In re United States for an Order: (1) Authorizing Installation and Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Information; and (3) Authorizing the Disclosure of Location-Based Services,* No. Misc. 07-127, 2007 WL 3341736 (S.D. Tex. Nov. 7, 2007) (involving a narcotics trafficking investigation).

12 *See In re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders,* 562 F. Supp. 2d at 895 (“As a rule, sealing and non-disclosure of electronic surveillance orders must be neither permanent nor, what amounts to the same thing, indefinite.”).

13 *See Doe v. Tenenbaum,* 900 F. Supp. 2d 572, 609 (D. Md. 2012) (“This Court does not customarily sit as a Star Chamber, resolving of cases under the veil of a virtual seal.”).

14 Detroit Free Press v. Ashcroft, 303 F.3d 681, 710 (6th Cir. 2002); *accord* N.Y. Civil Liberties Union v. N.Y.C. Transit Auth., 684 F.3d 286, 299 (2d Cir. 2012).

15 Like pen registers and search warrants, federal magistrate judges routinely handle § 2703(d) orders, in which the government seeks all types of cellphone and internet subscribers' personal information, including name, address, driver's license number, social security number, and means and source of payment. *See* 18 U.S.C. § 2703(c)(2); *see also* Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 14-15 (2013).

16 In the case of pen registers and trap and trace devices, Congress has mandated that “the order be sealed until otherwise ordered by the court.” 18 U.S.C. 3123(d)(1). Interestingly, orders pursuant to the Stored Communications Act are not automatically sealed. *In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information,* 396 F. Supp. 2d 294, 309 (E.D.N.Y. 2005) (noting that “[t]he SCA does not mention sealing”).

17 *See generally* Brady v. Maryland, 373 U.S. 83 (1963).

18 *See* 18 U.S.C. § 2708 (limiting the remedies for violation of the Stored Communications Act); *accord* United States v. Perrine, 518 F.3d 1196, 1202 (10th Cir. 2008); United States v. Smith, 155 F.3d 1051, 1056 (9th Cir. 1998). Similarly, several federal appellate courts have concluded that there is no suppression remedy for the violation of the pen register statute. *See* United States v. Forrester, 512 F.3d 500, 512-13 (9th Cir. 2008); United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995); United States v. Thompson, 936 F.2d 1249, 1249-50 (11th Cir. 1991); *see also* Owsley, *supra* note 15, at 28-29 (discussing cases in which the Government argued that there was no suppression remedy).

19 Smith, *supra* note 3, at 325.

20 *Id.* at 325-26.

21 *See* Owsley, *supra* note 15, at 42 (noting that Congress is recalcitrant to enact legislation in matters concerning electronic surveillance); *see also* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 681, 687 (2011) (“Historically, Congress has dragged its heels in protecting communications privacy until the courts have demanded it.”).

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 5 of 6

5 CALRC 259

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 6 of 6

ELECTRONICALLY FILED
Page 7/2/2015 12:12 PM
2014-CH-15338
CALENDAR: 11
PAGE 1 of 29
CIRCUIT COURT OF
COOK COUNTY, ILLINOIS
CHANCERY DIVISION
CLERK DOROTHY BROWN

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA,

Plaintiff,

-v-

ROBERT HARRISON,

Defendant.

CRIMINAL No. 1:14-CR-00170-CCB

***AMICI CURIAE MEMORANDUM OF ACLU AND ACLU OF MARYLAND
IN SUPPORT OF DEFENDANT ROBERT HARRISON'S MOTIONS TO COMPEL
DISCLOSURE OF AND TO SUPPRESS EVIDENCE RELATED TO THE
GOVERNMENT'S USE OF A CELL SITE SIMULATOR***

TABLE OF CONTENTS

INTRODUCTION	1
ARGUMENT	2
I. USE OF THE STINGRAY VIOLATED THE FOURTH AMENDMENT	2
A. Stingray technology is both invasive and precise and therefore may be used, if at all, only pursuant to a warrant based on probable cause.	2
B. Even if Baltimore Police had obtained a warrant to use a stingray, which it failed to do, use of the stingray would still raise serious Fourth Amendment concerns.	8
II. THE GOVERNMENT'S APPLICATION CONTAINED MATERIAL MISREPRESENTATIONS INVALIDATING ANY PURPORTED JUDICIAL AUTHORIZATION TO USE A STINGRAY	9
A. The Order authorizing use of the stingray was based on a misleading Application for a pen register/trap and trace device that breached the government's duty of candor to the issuing judge.....	9
B. The lack of candor in the government's Application requires the court to hold a <i>Franks</i> hearing to examine the validity of the court order.....	15
III. THE LAW ENFORCEMENT PRIVILEGE DOES NOT APPLY IN THIS CASE	19
A. The law enforcement privilege is not relevant to the government's use of the stingray.....	19
B. There is an abundance of public information on stingrays such that the technology is no longer secret.....	21
1. Publicly Available Information about Baltimore Police Department's Stingray(s)	22
2. Public Information About Harris Corporation's Cell Site Simulator Devices	23
3. Information Released by the Federal Government.....	24
4. Information in Judicial Opinions and Records	25
CONCLUSION	27

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 2 of 29

INTRODUCTION

This case involves the surreptitious use of a cell site simulator, more commonly known as a “stingray,”¹ which is a cell phone surveillance device frequently used by law enforcement agencies across the country. These privacy-invasive devices are being employed with little to no oversight from legislative bodies or the courts due to law enforcement secrecy surrounding its use of the technology. Stingrays can be carried by hand, installed in vehicles, or mounted on aircraft.² The devices masquerade as the cellular phone towers used by wireless companies such as AT&T and T-Mobile, and in doing so, force *all* mobile phones within the range of the device to emit identifying signals, which can be used to locate not only a particular suspect, but any and all bystanders as well.

In Mr. Harrison’s case, Baltimore Police emitted signals into Mr. Harrison’s home to force a mobile phone in his possession to transmit its identification and location information. Mot. to Compel 2, ECF No. 28. The government contends that this search was constitutional because it obtained an order from the state court judge, Hon. Barry G. Williams, under the Maryland pen register/trap and trace statute, Md. Code Ann., Cts. & Jud. Proc. § 10-4B-01. Gov’t Resp. at 2-3, ECF No. 32. The government further argues that pursuant to the “law enforcement privilege,” it is under no obligation to disclose

¹ “StingRay” is the name for a line of cell site simulator technology sold by the Harris Corporation. Other Harris cell site simulator models include the “TriggerFish,” “KingFish,” and “Hailstorm.” Ryan Gallagher, *Meet the Machines That Steal Your Phone’s Data*, Ars Technica, Sept. 23, 2013, <http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data>. Stingrays, and other models of cell site simulators, are also called “IMSI catchers,” in reference to the unique identifier—or international mobile subscriber identity—of wireless devices that they track. Stephanie K. Pell and Christopher Soghoian, *Your Secret Stingray’s No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, Harv. J.L. & Tech. (May 15, 2014), <http://ssrn.com/abstract=2437678>. Although “StingRay” refers to a specific line of products, *amici* use the term “stingray” in this brief generically to refer to cell site simulators.

² Gallagher, *Meet the Machines*, *supra* note 1; see also Devlin Barrett, *Americans’ Cellphones Targeted in Secret U.S. Spy Program*, Wall St. J. (Nov. 13, 2014), <http://online.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533>.

specific information about the stingray device it used to track Mr. Harrison. *Id.* at 6–7. *Amici* explain why these arguments are wrong as a matter of law and corrosive to the judiciary’s role in our constitutional system, and therefore must be rejected. *Amici* include publicly available facts about the stingray’s capabilities in order to inform the Court of Fourth Amendment concerns unique to this technology, as well as to refute improper claims that the materials Mr. Harrison seeks are privileged.

ARGUMENT

I. USE OF THE STINGRAY VIOLATED THE FOURTH AMENDMENT.

A. Stingray technology is both invasive and precise and therefore may be used, if at all, only pursuant to a warrant based on probable cause.

Wireless carriers provide coverage through a network of base stations, also known as “cell sites,” that connect cell phones and other wireless devices to the regular telephone network. A stingray masquerades as a wireless carrier’s base station, prompting all wireless devices within range to communicate with it. Depending on the particular features of the device and how the operator configures them, stingrays can be used to identify nearby phones,³ to locate them with extraordinary precision,⁴ and can even block service, either to all devices in the area or to particular devices.⁵ Stingrays are commonly

³ A number of companies in addition to the Harris Corporation produce and sell cell site simulator equipment. See, e.g., CellXion Ltd., *UGX Series 330: Transportable Dual GSM / Triple UMTS Firewall and Analysis Tool*, <http://s3.documentcloud.org/documents/810703/202-cellxion-product-list-ugx-optima-platform.pdf> (last visited Oct. 24, 2014) (including as features, “[c]omprehensive identification of IMSI, IMEI and TMSI information” and “[s]imultaneous high speed acquisition of handsets (up to 1500 per minute), across up to five networks”).

⁴ See, e.g., Mem. from Stephen W. Miko, Resource Manager, Anchorage Police Department, to Bart Mauldin, Purchasing Officer, Anchorage Police Department (June 24, 2009), <http://files.cloudprivacy.net/anchorage-pd-harris-memo.pdf> (“[The] system allows law enforcement agencies . . . the ability to . . . [i]dentify location of an active cellular device to within 25 feet of actual location anywhere in the United States.”).

⁵ See, e.g., *UGX Series 330: Transportable Dual GSM / Triple UMTS Firewall and Analysis Tool*, CellXion Ltd., available at <http://s3.documentcloud.org/documents/810703/202-cellxion-product-list-ugx-optima-platform.pdf> (last visited Oct. 24, 2014) (including as features, “[c]omprehensive identification of IMSI, IMEI and TMSI information” and “[s]imultaneous high speed acquisition of handsets (up to 1500 per minute), across up to five networks”) (describing device’s ability to

used by law enforcement agencies in two ways: to collect the unique international mobile subscriber identity numbers associated with all phones in a given location, or to ascertain the location of a particular phone “when the officers know the numbers associated with it but don’t know precisely where it is.”⁶

Use of a stingray constitutes a search within the meaning of the Fourth Amendment. Assuming such searches are ever permissible, *see infra* Part I.B, at a minimum they require a warrant based on probable cause. This is so for several reasons.

First, the devices broadcast invisible electronic signals that penetrate walls of Fourth Amendment-protected locations, including homes, offices, and other private spaces occupied by the target and innocent third parties in the area. Stingrays force cell phones within those spaces to transmit data to the government that they would not otherwise reveal to the government, and allow agents to determine facts about the phone and its location that would not otherwise be ascertainable without physical entry. By pinpointing suspects and third parties while they are inside constitutionally protected spaces, stingrays invade reasonable expectations of privacy. *See Kyllo v. United States*, 533 U.S. 27, 34 (2001) (thermal imaging to detect heat from home constituted search); *United States v. Karo*, 468 U.S. 705, 715 (1984) (monitoring of beeper placed into can of ether that was taken into residence constituted search).⁷

⁶[d]isable all handsets except operationally friendly”); Miko Mem., *supra* note 4 (“[The] system allows law enforcement agencies . . . the ability to . . . [i]nterrupt service to active cellular connection [and] [p]revent connection to identified cellular device.”).

⁷Jennifer Valentino-DeVries, *How ‘Stingray’ Devices Work*, Wall St. J. (Sept. 21, 2011), <http://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work/>.

⁷By way of additional illustration, take the Supreme Court’s recent observation that “nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower.” *Riley v. California*, 134 S. Ct. 2473, 2490 (2014). In this situation, “[t]he [stingray] might disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider ‘intimate.’” *Kyllo*, 533 U.S. at 38. To protect such intimate details, “the Fourth Amendment draws ‘a firm line at the entrance to the house.’” *Id.* at 39 (quoting *Payton v. New York*, 445 U.S. 573, 590 (1980)).

In addition, stingrays effectively trespass into protected spaces, as they send electronic signals that penetrate the walls of homes and offices in the vicinity in order to seek information about devices in interior spaces. *See Silverman v. United States*, 365 U.S. 505, 509 (1961) (use of “spike mike,” a microphone attached to spike inserted into walls of house, constituted “unauthorized physical penetration into the premises” giving rise to a search); *United States v. Jones*, 132 S. Ct. 945, 949 (2012) (installation and monitoring of GPS on suspect’s vehicle constituted search because of “physical intrusion” “for the purpose of obtaining information”). No search warrant, let alone a pen register order, would permit the police to search the homes of every house in a neighborhood. Yet, with the stingray, the police can do just that, searching every home, vehicle, purse, and pocket in a given area without anyone ever learning that their devices were searched by the police.

Second, the devices can pinpoint an individual with extraordinary precision, in some cases “with an accuracy of 2 m[eters].”⁸ *United States v. Rigmaiden*, a criminal case from the District of Arizona, is one of the few cases in which the government’s use of stingrays has been litigated. In it, the government conceded that agents used the device while wandering around an apartment complex on foot, and that the stingray ultimately located the suspect while he was inside his unit. *See United States v. Rigmaiden*, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *15 (D. Ariz. May 8, 2013). In another case in Florida, *State v. Thomas*, a Tallahassee Police officer testified about how, using a handheld cell site simulator, he “quite literally stood in front of every door and window” in a large apartment complex “evaluating all the handsets in the area” until he narrowed down the specific apartment in which the

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 6 of 29

⁸ See, e.g., PKI Electronic Intelligence GmbH, *GSM Cellular Monitoring Systems*, 12, http://www.pki-electronic.com/2012/wp-content/uploads/2012/08/PKI_Cellular_Monitoring_2010.pdf (device produced by a competitor to the Harris Corporation can “locat[e] ... a target mobile phone within an accuracy of 2 m[eters]”).

target phone was located.⁹ In Baltimore itself, two people have recently alleged that the government used a stingray device to track their precise locations.¹⁰ In one of the cases, police reportedly used a stingray to track a person within a single city block, and were able to determine that the person carrying the phone was in fact riding on a bus.¹¹ Accurate electronic location tracking of this type requires a warrant because it intrudes on reasonable expectations of privacy. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgement) (“[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.”); *id.* at 955 (Sotomayor, J., concurring); *Tracey v. State*, No. SC11-2254, 2014 WL 5285929, at *19 (Fla. Oct. 16, 2014) (“[T]he use of [a suspect’s] cell site location information emanating from his cell phone in order to track him in real time was a search within the purview of the Fourth Amendment for which probable cause was required.”).

Further, to the extent the government uses stingray devices without a warrant while walking on foot immediately outside people’s homes to ascertain information about interior spaces, it impermissibly intrudes on constitutionally protected areas. *See Florida v. Jardines*, 133 S. Ct. 1409 (2013) (government’s entry into curtilage with trained dogs to sniff for drug odors emanating from interior of home constitutes search).

Third, stingrays search the contents of people’s phones by forcing those phones to transmit their electronic serial number and other identifying information held in electronic storage on the device, as well as the identity of the (legitimate) cell tower to which the phone was most recently connected and other stored data. *See* Stip. at 2, ECF No. 32-1. As the Supreme Court explained in no

⁹ Transcript of Suppression Hr’g 14, 17, *State v. Thomas*, No. 2008-CF-3350A (Fla. 2d Cir. Ct. Aug. 23, 2010) [hereinafter “*Thomas Transcript*”], available at https://www.aclu.org/files/assets/100823_transcription_of_suppression_hearing_complete_0.pdf.

¹⁰ Justin Fenton, *Judge Threatens Detective with Contempt for Declining to Reveal Cellphone Tracking Methods*, Balt. Sun, Nov. 17, 2014, <http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-officer-contempt-20141117-story.html>.

¹¹ *Id.*

uncertain terms this year, searching the contents of a cell phone requires a warrant. *Riley v. California*, 134 S. Ct. 2473 (2014).

Fourth, Stingrays impact third parties on a significant scale. In particular, they interact with and capture information from innocent bystanders' phones by impersonating one or more wireless companies' cell sites and thereby triggering an automatic response from all mobile devices on the same network in the vicinity.¹² The government in *Rigmaiden* and *Thomas* conceded as much. See *Rigmaiden*, 2013 WL 1932800, at *20; *Thomas* transcript at 14. This is so even when the government is using a stingray with the intent to locate or track a particular suspect; collection of innocent bystanders' phone-identifying data and location information is inevitable and unavoidable using current stingray technology. Thus, when using a stingray the police infringe on the reasonable expectations of privacy of dozens or hundreds of innocent non-suspects, amplifying the Fourth Amendment concerns. Although there is a serious question whether dragnet searches of this nature are ever allowed by the Fourth Amendment, *see infra* Part I.B, use of this technology must at least be constrained by a probable cause warrant that mandates minimization of innocent parties' data.¹³ Cf. *Berger v. New York*, 388 U.S. 41, 57–59 (1967).

Finally, stingrays can, as a side-effect of their normal use, disrupt the ability of phones in the area to make calls. Harris Corporation, the company that manufactures the StingRay, and at least one of its competitors have apparently taken steps to ensure that 911 emergency calls are not

¹² See, e.g., Hannes Federrath, Multilateral Security in Communications, *Protection in Mobile Communications*, 5 (1999), http://epub.uni-regensburg.de/7382/1/Fede3_99Buch3Mobil.pdf ("possible to determine the IMSIs of all users of a radio cell"); Daehyun Strobel, Seminararbeit, Ruhr-Universität, *IMSI Catcher* (July 13, 2007), http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf. ("An IMSI Catcher masquerades as a Base Station and causes every mobile phone of the simulated network operator within a defined radius to log in.").

¹³ See Adam Lynn, *Tacoma Police Change How They Seek Permission to Use Cellphone Tracker*, News Tribune, Nov. 15, 2014, http://www.thenewstribune.com/2014/11/15/3488642_tacoma-police-change-how-they.html?sp=/99/289/&rh=1 (explaining that upon learning that police had been using cell site simulators without informing courts of such, judges in Tacoma, Washington, began requiring law enforcement agencies that want to use the devices to swear in affidavits that they will not store data collected from third parties who are not targets of the investigation).

disrupted.¹⁴ However, emergency calls to doctors, psychologists, and family members may be blocked while the stingray is in use nearby. This is invasive in general, raises possible conflicts with federal law, *see 47 U.S.C. § 333*, and can have enormous consequences for anyone in an emergency situation trying to make an urgent call for assistance. To avoid effecting an unreasonably invasive or destructive search, *see United States v. Ramirez*, 523 U.S. 65, 71 (1998), use of stingrays must be strictly constrained.

In light of these factors, use of a stingray is presumptively invalid unless the government obtains a valid warrant based on probable cause. *See Arizona v. Gant*, 556 U.S. 332, 338 (2009) (explaining that searches without a warrant are ““per se unreasonable”” (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967))). The government did not obtain a warrant to use a stingray device in this case. In fact, it did not request authorization to use a stingray at all, but misled the court by seemingly applying for an order authorizing installation of a run-of-the-mill pen register device. *See infra* Part II.A. The underlying Order was made pursuant to Maryland’s Pen Registers and Trap and Traces Devices Statute, which authorizes installation of such a device “if the court finds that the information likely to be obtained by the installation and use is *relevant to an ongoing criminal investigation.*” Md. Code Ann., Cts. & Jud. Proc. § 10-4B-04 (emphasis added). The government’s invocation of probable cause in its pen register application¹⁵ and the court’s reference to probable cause in the order¹⁶ do not transform a pen register/trap and trace order into a warrant. Warrants require not just a probable cause showing, but also must “describe with particularity the items to be seized [in order to ensure] that a citizen is not subjected

¹⁴ Barrett, *supra* note 2.

¹⁵ Appl. at 2, *In Re Appl. of Md. For an Order Authorizing the Installation & Use of a Device Known as a Pen Register/Trap & Trace Over 443-803-6749*, No. 1:14-cr-00170-CCB (Circ. Ct. Md. Feb. 5, 2014) (Defendant filed this document as ECF No. 29-1)

¹⁶ Order at 1, *In Re Appl. of Md. For an Order Authorizing the Installation & Use of a Device Known as a Pen Register/Trap & Trace Over 443-803-6749*, No. 1:14-cr-00170-CCB (Circ. Ct. Md. Feb. 5, 2014) (Defendant filed this document as ECF No. 29-1)

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 9 of 29

to ‘a general, exploratory rummaging in [his personal] belongings.’” *United States v. Hurwitz*, 459 F.3d 463, 470 (4th Cir. 2006) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)); *see also* Fed. R. Crim. P. 41 (setting out requirements for issuance of a warrant in federal courts); Md. Code Ann., Crim. Proc. § 1-203 (same, for state courts). Warrants also involve a strict requirement of notice to the target of the search, a default requirement that the warrant be executed in the daytime hours, a time limit on execution of the warrant, and other protections. Fed. R. Crim. P. 41 (e)(2)(C)(ii), (f)(2); Md. Code Ann., Crim. Proc. § 1-203 (a)(5)-(6). Moreover, warrants must be accompanied by a sworn affidavit based on personal knowledge of an investigating officer and setting forth the basis for probable cause. Md. Code Ann., Crim. Proc. § 1-203(a)(2)(i)(3); Fed. R. Crim. P. 41(d). The pen register application at issue here was merely signed by a police detective and the facts therein were not sworn to under oath. Because use of a stingray constitutes a search, the government must, at the very least, secure a warrant before employing such a device. The government’s insertion of information in support of a finding of probable cause in its Application suggests that it understood these concerns; as such, the government should have applied for a proper search warrant.

B. Even if Baltimore Police had obtained a warrant to use a stingray, which it failed to do, use of the stingray would still raise serious Fourth Amendment concerns.

Even in instances where the government obtains a warrant, stingray use raises serious constitutional concerns due to the dragnet nature of the device’s surveillance and the collateral impacts of the device’s broadcasts on innocent third parties. As discussed above, stingrays collect identifying and location information about dozens or hundreds of innocent bystanders’ phones, send electronic signals through the walls of nearby homes and offices, learn otherwise private information about the locations of phones inside those spaces, and interfere with bystanders’ phone calls. The Fourth

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 10 of 29

Amendment was “the product of [the Framers’] revulsion against” “general warrants” that provided British “customs officials blanket authority to search where they pleased for goods imported in violation of the British tax laws.” *Stanford v. Texas*, 379 U.S. 476, 481–82 (1965). Stingrays, inevitably interact with and collect data from the phones of innocent third parties as to whom there is no individualized suspicion, let alone probable cause. Authorization for such sweeping surveillance raises the type of concerns that animate the prohibition on general warrants. *See United States v. Leon*, 468 U.S. 897, 899 (1984) (“[A] warrant may be so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid.”); *Doe v. Broderick*, 225 F.3d 440, 453 (4th Cir. 2000) (“The expectation that one generally remains free from warrantless searches in the privacy of the home is at the heart of the Fourth Amendment, but the Supreme Court has long recognized that searches of office buildings and commercial premises in the absence of a search warrant grounded upon probable cause are unreasonable as well.”) (internal citations omitted). Furthermore, interrupting and preventing dozens or hundreds of people’s cell phone calls, including urgent and important calls, in the course of tracking a single suspect raises serious questions about the reasonableness of the search. *See United States v. Ramirez*, 523 U.S. 65, 71 (1998).

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 11 of 29

II. THE GOVERNMENT’S APPLICATION CONTAINED MATERIAL MISREPRESENTATIONS INVALIDATING ANY PURPORTED JUDICIAL AUTHORIZATION TO USE A STINGRAY.

A. The Order authorizing use of the stingray was based on a misleading Application for a pen register/trap and trace device that breached the government’s duty of candor to the issuing judge.

The government’s stingray search did not fall within the scope of its Application. First, the government misled the court in requesting what appeared to be a run-of-the-mill pen register/trap and

trace order. Second, its Application contained no mention of a stingray device, much less any explanation of how such a device operates, the immense privacy implications for innocent third parties, or the fact that regular use of the stingray can disrupt phone calls nearby.

Courts recognize a pen register as a device that records the numbers dialed by a particular telephone and a trap and trace device as recording the incoming numbers to a telephone. *See Smith v. Maryland*, 442 U.S. 735, 736 & n.1 (1979); *see also* Md. Code Ann., Cts. & Jud. Proc. § 10-4B-01 (c)(1)-(d)(1). The government sought a pen register order to authorize use of a “cellular tracking device,” but Maryland’s pen register statute makes no provision for, or even mention of, a “cellular tracking device.”¹⁷ *See generally*, Appl., *Appl. for Pen Register*, No. 1:14-cr-00170-CCB; Md. Code Ann., Cts. & Jud. Proc. § 10-4B-01. Without a description from the government as to what it meant by “cellular tracking device,” it would have been near-impossible for the issuing judge to know that the government was in fact referring to a stingray. Even more unlikely would have been the court’s independent understanding that unlike a pen register/trap and trace device, a stingray broadcasts signals that penetrate the walls of every private home in its vicinity, and is incapable of targeting only one phone or person, but instead searches every mobile phone in range.

The portion of the government’s Application that purportedly sought authorization to use a stingray is vague, brief, and buried in a single paragraph:

¹⁷ Under federal law, pen register orders may not be used to obtain location information. *See* 47 U.S.C. § 1002(a)(2) (“[W]ith regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices . . . , such call identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number.”). Although the Maryland pen register statute does not include this limiting language, use of information collected under the state statute in a federal prosecution that would not be obtainable using the analogous federal statute raises concerns. Moreover, as of October 1, 2014, law enforcement in Maryland must obtain a search warrant before tracking the location of a cell phone. Md. Code Ann. Crim. Proc. § 1-203.1, enacted as S.B. 698, 2014 Md. Laws Ch. 191. The Maryland legislature has now clearly forbidden use of a pen register order to obtain real-time location information.

“...the [government]...shall initiate a signal to determine the location of the subject’s mobile device on the service provider’s network or with such other reference points as may be reasonably available, Global Position System Tracing and Tracking, Mobile Locator tools, R.T.T. (Real Time Tracking Tool), Precision Locations and any and all locations...”

Appl. at 6-8, *Appl. for Pen Register*, No. 1:14-cr-00170-CCB. There is no explanation of what these “tools” are, how they operate, or how they will be used. In addition, there is absolutely no indication in the Application or the Order that the authorization will subject potentially unlimited numbers of innocent third parties to dragnet surveillance, none of whom will ever receive notice that their phones were tracked, and that the search will intrude into constitutionally protected spaces. The government’s lack of specificity fails its duty of candor to the courts. *See United States v. Comprehensive Drug Testing, Inc.* (CDT) 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (Kozinski, J. concurring) (“A lack of candor in this or any other aspect of the warrant application must bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized data.”). By neglecting to apprise the court that it intended to use a stingray, what the device is, and how it works, the government prevented the court from exercising its constitutional function of ensuring that searches are not overly intrusive and that all aspects of the search are supported by probable cause, described with particularity, and conducted pursuant to a warrant.

The role of the court in enforcing the requirements of the Fourth Amendment is key. When judges have learned that police departments are seeking to use stingray devices and understood the capabilities of those devices, they have limited the scope of orders and demanded that the government be more candid in its requests.¹⁸ In a recent federal investigation in New Jersey, for example, the government submitted an application for a pen register order to use a stingray that included

¹⁸ Or, they have thrown out evidence altogether. *See supra* note 11.

significantly more detail than was provided in this case, even stating that: the device will “mimic[] one of Sprint’s cell towers to get the Target [phone] to connect to it;” “[b]ecause of the way the Mobile Equipment sometimes operates, its use has the potential to intermittently disrupt cellular service to a small fraction of Sprint’s wireless customers within its immediate vicinity;” and “data [will be] incidentally acquired from phones other than the Target.” Appl. at 6-8, *Appl. for Pen Register*, No. 1:14-cr-00170-CCB; Order, *Order for Pen Register*, No. 1:14-cr-00170-CCB; *United States v. Williams*, No. 13-00548 (KM) (D.N.J. 2014). Based on this description of the intrusive nature of the technology, and recognizing that a pen register order cannot authorize such an intrusion, the federal magistrate judge reviewing the application modified the government’s proposed order by hand to prohibit the government from using the stingray “in any private place or where [FBI agents] have reason to believe the Target [phone] is in a private place.” Order at 5, *Order for Pen Register*, No. 1:14-cr-00170-CCB.

More recently, a local newspaper investigation in Tacoma, Washington, revealed that police had used a stingray more than 170 times over five years but had concealed their intent to do so from judges when seeking court orders.¹⁹ Once local judges learned from a reporter that they had been unwittingly authorizing stingray use, they collectively imposed a requirement that the government spell out whether it is seeking to use a stingray device in future pen register applications.²⁰ Law enforcement agencies that want to use the device must now swear in affidavits that they will not store data collected from third parties who are not targets of the investigation.²¹ Similarly, after the local newspaper in Charlotte, North Carolina, revealed that police had been using stingrays for eight years

¹⁹ Lynn, *Tacoma Police Change How They Seek Permission to Use Cellphone Tracker*, *supra* note 14.

²⁰ *Id.*

²¹ *Id.*

pursuant to pen register orders, but had not made their intent to do so explicit in their applications, a judge denied an application for such an order, a first for that court.²²

Here, had the government candidly told Judge Williams that it intended to use a stingray, he could have denied the application without prejudice to a subsequent application providing further details about the technology, imposed limits on use of the device, or denied the application and invited the government to apply for a search warrant instead. A federal magistrate judge recently denied a pen register application to use a stingray on these grounds. *In re Application for an Order Authorizing Installation and Use of a Pen Register and Trap and Trace Device*, 890 F. Supp. 2d 747 (S.D. Tex. June 2, 2012). As the same magistrate judge explained in denying a statutory application for cell site records of *all* subscribers from several cell towers, an understanding of “the technology involved” is necessary to “appreciate the constitutional implications of” the government’s application, particularly where, as here, the technology entails “a very broad and invasive search affecting likely hundreds of individuals in violation of the Fourth Amendment.” *In re Application for an Order Pursuant to 18 U.S.C. § 2703(D)*, 930 F. Supp. 2d 698 (S.D. Tex. 2012).

In another case, a federal magistrate judge denied a pen register application on the ground that use of a stingray is too intrusive because of the impact on third parties. See *In re Application for an Order Authorizing Use of a Cellular Telephone Digital Analyzer*, 885 F.Supp. 197, 201 (C.D. Cal. 1995) (denying statutory application to use stingray because, *inter alia*, “depending upon the effective range of the digital analyzer, telephone numbers and calls made by others than the subjects of the investigation could be inadvertently intercepted”). That stingrays obtain information about third parties

²² Fred Clasen-Kelly, *CMPD’s Cellphone Tracking Cracked High-Profile Cases*, Charlotte Observer, Nov. 22, 2014, www.charlotteobserver.com/2014/11/22/5334827/cmpds-cellphone-tracking-cracked.html.

“creates a serious risk that every warrant for [a stingray] will become, in effect, a general warrant,” to search persons as to whom there is no probable cause. *See CDT*, 621 F.3d at 1176.

The government here failed to provide Judge Williams with essential information about the nature and scope of the search it sought to conduct. Indeed, the lack of government candor to the courts and Judge Williams’ actual response once apprised of the government’s activities is highlighted by two ongoing prosecutions in state court. At a November 17 suppression hearing, Judge Williams threatened to hold a Baltimore Police detective in contempt of court if he did not explain how the city tracked a phone to locate the defendant in that case.²³ The detective refused to respond to the defense attorney’s questions about the stingray device used, citing a “nondisclosure agreement” with the FBI.²⁴ Judge Williams responded that the detective “[does not] have a nondisclosure agreement with the court.”²⁵ After the heated exchange, the prosecution decided to withdraw the phone evidence rather than answer the judge’s questions.²⁶ Likewise, in a September hearing in a different case, Judge Williams pressed a Baltimore police officer to answer the defense’s questions about how he tracked a phone to the defendant. *See Transcript of Suppression Hearing at 29-30, State of Maryland v. Batty*, Case No. 113078021 (Circ. Ct. Md., Balt. Cnty., Sept. 16, 2014), 29–30. When the officer explained only that “[t]his kind of goes to Homeland Security issues,” the judge ordered the tracking evidence excluded, explaining: “I mean, this is simple. You can’t just stop someone and not give me a reason, State, and you know that.” *Id.* In light of Judge Williams’s reaction to government concealment in those cases, it is not unreasonable to believe that had the government given some indication of how it

²³ See Fenton, *Judge Threatens Detective With Contempt*, *supra* note 11.

²⁴ *Id.*

²⁵ *Id.*

²⁶ *Id.*

intended to use the pen register order, he would have demanded further information before issuing the order, and may well have denied the application altogether.

The police's tracking of Mr. Harrison's person was invalid due to a misleading application. The government's "lack of candor," was highly consequential to Mr. Harrison's case, and he has a right to corroborate his claims with evidentiary information from the government. *CDT*, 621 F.3d at 1170 (Kozinski, C.J., concurring).

B. The lack of candor in the government's Application requires the court to hold a *Franks* hearing to examine the validity of the court order.

The government's omission of information about the stingray from its Application prevented the court from exercising its constitutional oversight function and renders the Order invalid. At a minimum, Mr. Harrison is entitled to an evidentiary hearing on whether the omission of information about the cell site simulator was intentional and material. *See Franks v. Delaware*, 438 U.S. 154 (1978). A defendant seeking a *Franks* hearing based on omission of information must make a showing that "omissions were 'designed to mislead, or . . . made in reckless disregard of whether they would mislead' and that the omissions were material." *United States v. Clenney*, 631 F.3d 658, 664 (4th Cir. 2011) (alteration and emphasis in original) (quoting *United States v. Colkley*, 899 F.2d 297, 301 (4th Cir.1990)). If the court finds that "'inclusion [of the omitted material] in the affidavit would defeat probable cause,'" *id.*, "the search warrant must be voided and the fruits of the search excluded." *Franks*, 438 U.S. at 155.²⁷ Although the government obtained and relied on a pen register order, not a warrant, in this case, there is no reason why the *Franks* rule should not apply. A material omission or misrepresentation to the issuing judge should void the order and result in exclusion of evidence gathered pursuant to it.

²⁷ Courts have consistently held that "[s]uppression remains an appropriate remedy if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth." *Leon*, 468 U.S. at 897–98.

The government made serious omissions and misrepresentations with respect to its intended use of a stingray demonstrating a reckless disregard for the truth. It completely left out any description of the type of equipment it was seeking to use; in fact, its Application makes absolutely no mention of a “stingray,” “cell site simulator” or “IMSI catcher.” Instead, on its face, the government’s Application appears to be a routine request for a pen register, which is a completely different surveillance technology with significantly lesser surveillance capabilities than a cell site simulator with none of the side effects inflicted upon innocent third parties.

The misrepresentation in this case is not an isolated incident; law enforcement and prosecutors across the country have systematically concealed information about stingrays from courts. For example, documents obtained from the FBI show that it has a longstanding policy of concealing information about stingrays.²⁸ An email produced in discovery in *Rigmaiden* stated that the investigative team “need[ed] to develop independent probable cause of the search warrant … FBI does not want to disclose the [redacted] (understandably so).”²⁹ In the same case, prosecutors conceded that the government had not made a “full disclosure to the magistrate judge [who issued the original order authorizing the surveillance] with respect to the nature and operation of the [StingRay] device [used to locate Rigmaiden].”³⁰ The reason for that lack of candor, the DOJ later told the court, was “because of the

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CR-15338
PAGE 18 of 29

²⁸ See City’s Verified Answer, Affidavit of Bradley S. Morrison at 2, *Hodai v. City of Tucson*, No. C20141225 (Ariz. Super. Ct. Mar. 4, 2014). (“[T]he FBI has, as a matter of policy, for over 10 years, protected this specific electronic surveillance equipment and techniques from disclosure, directing its agents that while the product of the identification or location operation can be disclosed, neither details on the equipment’s operation nor the tradecraft involved in use of the equipment may be disclosed.”).

²⁹ Exhibit 34 to Discovery & Suppression Issues at 51, *United States v. Rigmaiden*, 844 F. Supp. 2d 982 (D. Ariz. July 27, 2011) (No. 08-cr-00814-DGC) (emphasis added) (Email from Denise L Medrano, Special Agent, Phoenix Field Office, to Albert A. Childress (July 17, 2008 6:01 AM)), https://www.aclunc.org/sites/default/files/Rigmaiden_ECF_No.587-2_Exhibits_34.pdf.

³⁰ Transcript of Motion to Suppress at 81, *United States v. Rigmaiden*, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC).

sensitive nature of the device in terms of concerns out of the disclosure to third parties.”³¹ An email released by the U.S. Attorney’s Office for the Northern District of California via a Freedom of Information Act request explains that “many” law enforcement agents in that district were using stingrays under the auspices of pen register orders, but without “mak[ing] that explicit” in the application; even worse, this occurred *after* the federal magistrates had expressed “collective concerns” that pen register orders would not suffice to authorize use of the device.³² As explained above, in Tacoma, Washington, the government obtained more than 170 orders ostensibly justifying stingray use in recent years, but judges did not know that they had been authorizing use of stingrays until informed of such by a local newspaper report.³³ In Florida, police in the Sarasota area released an email showing that, “at the request of U.S. Marshalls [sic],” in warrant affidavits local police officers “simply refer to [information from a cell site simulator] as ‘. . . information from a confidential source regarding the location of the suspect.’ To date this has not been challenged . . .”³⁴

And in Baltimore, police are invoking a secret nondisclosure agreement with the federal government to justify affirmative concealment of information about stingray use from judges and defense counsel.³⁵

All of this indicates that the government’s omission of information about stingrays—or affirmative misrepresentation that it is instead using a “pen register” device or obtaining information from a “confidential source”—is hardly innocent. It seems clear that misrepresentations and omissions pertaining to the government’s use of stingrays are intentional. The issue is not whether the government

³¹ *Id.*

³² Email from Miranda Kane, USACAN, to USACAN-Attorneys-Criminal listserv (May 23, 2011 11:55 AM) https://www.aclu.org/files/assets/doj_emails_on_stingray_requests.pdf.

³³ Lynn, *Tacoma Police Change How They Seek Permission to Use Cellphone Tracker*, *supra* note 14.

³⁴ Email from Kenneth Castro, Sergeant, Sarasota Police Dep’t, to Terry Lewis, (Apr. 15, 2009, 11:25 EST), https://www.aclu.org/sites/default/files/assets/aclu_florida_stingray_police_emails.pdf.

³⁵ Fenton, *Judge Threatens Detective With Contempt*, *supra* note 11.

should have followed-up on or disclosed facts not of its own making. The government cannot disclaim responsibility for knowing what device it has chosen to use.

Nor can ignorance about the technology excuse any omission. The functioning of the technology has constitutional significance. It is therefore incumbent on the government to understand the technology and disclose it to the courts. *See In re Application for an Order Pursuant to 18 U.S.C. § 2703(D)*, 930 F. Supp. 2d 698 (S.D. Tex. 2012) (rejecting application for so-called “cell tower dump,” i.e., all information from specified cell towers: “[I]t is problematic that neither the assistant United States Attorney nor the special agent truly understood the technology involved in the requested applications. Without such an understanding, they cannot appreciate the constitutional implications of their requests. They are essentially asking for a warrant in support of a very broad and invasive search affecting likely hundreds of individuals in violation of the Fourth Amendment.”).

Moreover, the government’s omissions were material to Judge William’s decision to grant the order. *See supra* Part II.A. The government’s request seemingly targeted a small group of alleged conspirators, not potentially thousands of innocent parties. Had the government clearly explained that it was not seeking to use a pen register at all, but rather a device that interacts with and searches the phones of many third parties by sending signals through the walls of homes and into private spaces, the court’s decision almost certainly would have been affected.

In short, the Application failed to alert the issuing judge that the government intended to use a stingray, misleadingly stated it intended to use a “pen register,” and failed to provide basic information about what the technology is and how it works. The omissions were intentional and material. Mr. Harrison is therefore entitled to suppression or a *Franks* hearing, to ensure that the government is not permitted to conduct searches pursuant to an invalid court order.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CR-15338
PAGE 20 of 29

III. THE LAW ENFORCEMENT PRIVILEGE DOES NOT APPLY IN THIS CASE.

A. The law enforcement privilege is not relevant to the government's use of the stingray.

The government argues that Mr. Harrison's motions to compel disclosure and to suppress evidence should be dismissed on the basis of a "privilege applicable to information about sensitive law-enforcement techniques." Gov't Resp. at 6, ECF No. 32. The government does not, however, support this contention with legal precedent relevant to Mr. Harrison's case, and aside from a single citation to the Supreme Court's decision in *Roviaro v. United States*, 353 U.S. 53 (1957), does not even cite to mandatory case law within this Circuit. In *Roviaro*, the Court recognized a privilege to protect the identity of police informants to secure the important governmental interest in receiving information about criminal events from members of the public. *Id.* at 59. Here, where Mr. Harrison is seeking information about a tool that was used to obtain key evidence in the prosecution's case against him—in violation of the Fourth Amendment—and where information about the device and technique used to gather that evidence is already publicly available and widely known, there is no analogous public interest. Any claims from the government that other investigations will be hampered by disclosure are conclusory, especially in light of public information already available. See *infra* Part III.B.

Other cases cited by the government are likewise unavailing. In *United States v. Harley*, 682 F.2d 1018, 1020 (D.C. Cir. 1982), the D.C. Circuit allowed the government to withhold "the location of a police surveillance post" in order to protect "the safety of the cooperating apartment owner or tenant." The basis for that holding is indistinguishable from the rule set forth in *Rovario*, and no analogous concern applies here. Likewise, in *United States v. Van Horn*, 789 F.2d 1492, 1508 (11th Cir. 1987), the Eleventh Circuit held that the government could withhold the "precise locations where [surveillance cameras] are hidden or their precise specifications." Here, Mr. Harrison does not seek a precise

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CR-15338
PAGE 21 of 29

description of the path police followed while operating the stingray or technical documents detailing its “precise specifications.” Rather, he seeks investigative reports, identities of operating officers, and similar records that bear on the nature and scope of the Fourth Amendment violation. And to the extent Mr. Harrison did seek specifications of the stingray device used to locate him, that information is already public and therefore application of the privilege is waived. *Infra* Part III.B.

While the facts of *Roviaro*, involving withholding the identity of a human informant, do not compare with the facts at hand, the Supreme Court did articulate limiting guidance that is instructive here:

The scope of the privilege is limited by its underlying purpose. Thus, where the disclosure of the contents of a communication will not tend to reveal the identity of an informer, the contents are not privileged. Likewise, *once the identity of the informer has been disclosed* to those who would have cause to resent the communication, *the privilege is no longer applicable*.

Roviaro, 353 U.S. at 60-61 (emphasis added). This Court has likewise recognized a limited privilege, stating, “[t]he purpose behind the privilege is to prevent interference with an on-going investigation,” as opposed to an investigation that has been closed. *United States v. Lang*, 766 F. Supp. 389, 404 (D. Md. 1991). To invoke the privilege, police must first “make a substantial threshold showing that there are specific harms likely to accrue from disclosure of specific materials.” *Bellamy-Bey v. Baltimore Police Dep’t*, 237 F.R.D. 391, 393 (D. Md. 2006). The court then employs a balancing test to weigh “whether ‘disclosure of specific information would result in specific harm to identified important interests’ against the relevance of the documents to the plaintiff’s case and the injury to the public and plaintiff of non-disclosure.” *Id.* (citing *King v. Conde*, 121 F.R.D. 180, 190, 198 (E.D.N.Y. 1988)). “The test dictates that ‘[b]lanket and generalized assertion of privilege is not sufficient to overcome the presumption of discoverability.’” *Martin v. Conner*, 287 F.R.D. 348, 351 (D. Md. 2012) (internal citation omitted).

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 22 of 29

Here, the government has not made a substantial threshold showing that specific harms will accrue from the disclosure; even had it done so, it has still not shown that those harms would outweigh the potential injury to Mr. Harrison's case.

B. There is an abundance of public information on stingrays such that the technology is no longer secret.

Regardless of whether the government could otherwise meet its burden to invoke the privilege, the abundance of public information on stingrays renders the issue moot. In fact, stingrays have been the subject of front page stories in leading newspapers,³⁶ featured in Hollywood movies³⁷ and television dramas,³⁸ and are even available for sale over the Internet from one of many non-U.S. based surveillance technology vendors.³⁹ Legal scholars have published lengthy academic articles describing the history of the technology, its use by the government, and its capabilities.⁴⁰ Computer science graduate students have even published detailed theses and research papers about the surveillance methods used by the stingray.⁴¹ As much as the Baltimore police and federal agencies would like this technology to be a secret, the reality is that the secret was out a long time ago.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 23 of 29

³⁶ See Ellen Nakashima, *Little-Known Surveillance Tool Raises Concerns by Judges, Privacy Activists*, Wash. Post (Mar. 27, 2013), http://www.washingtonpost.com/world/national-security/little-known-surveillance-tool-raises-concerns-by-judges-privacy-activists/2013/03/27/8b60e906-9712-11e2-97cd-3d8c1afe4f0f_story.html; Jennifer Valentino-DeVries, 'Stingray' Phone Tracker Fuels Constitutional Clash, Wall St. J. (Sept. 22, 2011), <http://online.wsj.com/article/SB1000142405311904194604576583112723197574.html>.

³⁷ See Zero Dark Thirty at 00:80:38 (Sony Pictures 2012).

³⁸ See The Wire: Middle Ground at 00:12:57 (HBO television broadcast Dec. 12, 2004) (dialogue between two characters) ("Remember those analog units we used to use to pull cell numbers out of the air? . . . We used to have to follow the guy around, stay close while he used the phone." "New digitals . . . bing, we just pull the number right off the cell towers.").

³⁹ See Letter from Rep. Alan M. Grayson to Tom Wheeler, Chairman, Fed. Commc'nns Comm'n (July 2, 2014), http://grayson.house.gov/images/pdf/rep_grayson_letter_to_federal.communications_commission_chairman.pdf (making reference to a Chinese online merchant and stating that "IMSI catchers can apparently 'be bought openly' from online retailers for as little as \$1800").

⁴⁰ See Pell and Soghoian, *Your Secret Stingray's No Secret Anymore*, *supra* note 1; See also Heath Hardman, *The Brave New World of Cell-Site Simulators*, Alb. L. Rev. (May 22, 2014), <http://dx.doi.org/10.2139/ssrn.2440982>.

⁴¹ See Dennis Wehrle, *Open Source IMSI-Catcher* (Oct. 28, 2009) (unpublished Masters thesis, University of Freiburg), https://github.com/tom-mayer/imsi-catcher-detection/blob/master/Papers/Thesis%20KS/Ausarbeitung-Dennis_Wehrle.pdf. See also Daehyun Strobel, *IMSI Catcher*, 13 (2007) (seminar paper, Ruhr-Universitat Bochum), http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf

1. Publicly Available Information about Baltimore Police Department's Stingray(s)

In addition to the vast amount of public information describing the capabilities of the stingray technology, the City of Baltimore has officially documented the Baltimore Police Department's purchase and use of the technology. According to publicly available minutes of Baltimore Board of Estimates meetings, the City has made at least three purchases of cell site simulators and related equipment from the Harris Corporation:

- At the Board's February 4, 2009 meeting, it awarded \$132,800 to Harris Corporation for a "Cell Phone Tracking System" for the police department.⁴²
- At the Board's June 9, 2010 meeting, it extended its warranty with Harris Corporation for a "Cell Phone Tracking System" for an additional \$30,000.⁴³
- At the Board's January 23, 2013 meeting, it agreed to pay Harris Corporation \$99,786 for a "Hailstorm Cell Phone Tracker Upgrade" on behalf of the police department.⁴⁴

Together, the city has spent over \$250,000 for stingray technology, and has disclosed this fact to the public. This disclosure is now widely known, and has been the subject of articles in the Baltimore media and national news outlets.⁴⁵

⁴² Available at <http://comptroller.baltimorecity.gov/minutes/2009-02-04.pdf>.

⁴³ Available at http://comptroller.baltimorecity.gov/minutes/1767-1899_2010-06-09.pdf

⁴⁴ Available at http://comptroller.baltimorecity.gov/minutes/0179-0279_2013-01-23.pdf (The Hailstorm is an upgrade to the stingray that enables law enforcement agencies to track modern smartphones that use "4G" the latest mobile network technology.). See, Cyrus Farivar, *Cities Scramble to Upgrade "Stingray" Tracking as End of 2G Network Looms*, Ars Technica (Sept. 1, 2014), <http://arstechnica.com/tech-policy/2014/09/cities-scramble-to-upgrade-stingray-tracking-as-end-of-2g-network-looms/>

⁴⁵ The Baltimore Sun recently explained, for example, that "[r]ecords shows [sic] that the Baltimore Police Department purchased a stingray for \$133,000 in 2009." Fenton, *Judge Threatens Detective with Contempt*, *supra* note 11. See also Gallagher, *Meet the Machines*, *supra* note 1 (citing Baltimore's purchase of a Hailstorm).

2. Public Information About Harris Corporation's Cell Site Simulator Devices

Detailed information about the technical specifications and capabilities of stingrays are also publicly available from patent applications submitted by the Harris Corporation.⁴⁶ Harris has even publicly filed photos of its devices with the U.S. Patent and Trademark Office.⁴⁷ Harris Corporation's own publicly available promotional materials describe the capabilities and features of its cell site simulators. *See Appendix A.*⁴⁸

Documents made public by state and local governments as part of their cell site simulator procurement processes reveal similar details. For example, the Anchorage, Alaska, Police Department's purchase request for a "Kingfish" cell site simulator describes many of its capabilities, including the ability to:

- Identify location of an active cellular device to within 25 feet of actual location anywhere in the United States;
- Track the route of any active cellular device and record tracking information for evidentiary purposes;
- Mimic the functional appearance of an active cellular service tower
- Interrupt service to active cellular connection; and

⁴⁶ Competitors to the Harris Corporation have also published detailed information on how their stingray devices work. *See, e.g.*, PKI, *GSM Cellular Monitoring Systems*, *supra* note 9. *See also*, United States Patent No. 7,592,956, Rodney Keith McPherson & David James Lanza (Inventors), Harris Corp. (Assignee) (Sept. 22, 2009), available at <http://patft.uspto.gov/netahtml/PTO/search-bool.html> (enter "7,592,956" into search field).

⁴⁷ Available at <http://tsdr.uspto.gov/documentviewer?caseId=sn76303503&docId=SPE20130404144554#docIndex=2&page=1>; <http://tsdr.uspto.gov/documentviewer?caseId=sn77316689&docId=SPE20140514151847#docIndex=1&page=1>; <http://tsdr.uspto.gov/documentviewer?caseId=sn76303814&docId=SPE20140213150610#docIndex=2&page=1>.

⁴⁸ See Harris, StingRay and AmberJack Product Descriptions, available at <http://egov.ci.miami.fl.us/Legistarweb/Attachments/34769.pdf>; Harris, KingFish Product Description, <http://egov.ci.miami.fl.us/Legistarweb/Attachments/34771.pdf> at 2; *see also* Gallagher, *Meet the Machines*, *supra* note 1 (describing Harris Corporation's line of cell site simulators).

- Prevent connection to identified cellular device (“No Service”)⁴⁹

3. Information Released by the Federal Government

The federal government itself has released significant information about its use of cell site simulators. In response to a Freedom of Information Act request from the Electronic Privacy Information Center, the U.S. Department of Justice has released thousands of pages of documents about the use of cell site simulators in criminal investigations.⁵⁰ Likewise, the Department of Justice Electronic Surveillance Manual describes the capabilities of cell site simulators:

Law enforcement possesses electronic devices that allow agents to determine the location of certain cellular phones by the electronic signals that they broadcast. This equipment includes an antenna, an electronic device that processes the signals transmitted on cell phone frequencies, and a laptop computer that analyzes the signals and allows the agent to configure the collection of information. Working together, these devices allow the agent to identify the direction (on a 360 degree display) and signal strength of a particular cellular phone while the user is making a call. By shifting the location of the device, the operator can determine the phone’s location more precisely using triangulation.⁵¹

The Manual also explains the legal process that federal agents are required to obtain in order to use cell site simulators.⁵² In addition, the Federal Communications Commission has released information about regulation of cell site simulators, including letters from local police departments seeking permission to use the devices on the public radio spectrum.⁵³

⁴⁹ Memo. From Stephen W. Miko, Anchorage Police Dep’t, to Bart Mauldin, Anchorage Police Dep’t (June 24, 2009), available at <http://files.cloudprivacy.net/anchorage-pd-harris-memo.pdf>.

⁵⁰ See Electronic Privacy Information Center, *EPIC v. FBI – Stingray/Cell Site Simulator*, <https://epic.org/foia/fbi/stingray> (last visited Nov. 24, 2014).

⁵¹ Dep’t of Justice, *Electronic Surveillance Manual*, 44 (June 2005), <http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf>.

⁵² See *Electronic Investigative Techniques*, U.S. Atty’s Bull., Sept. 1997, 13–14 (discussing use of digital analyzers and cell site simulators), http://www.justice.gov/usao/eousa/foia_reading_room/usab4505.pdf.

⁵³ Letter from Julius P. Knapp, FCC, to Christopher Soghoian (Feb. 29, 2012), available at <http://files.cloudprivacy.net/FOIA/FCC/fcc-stingray-reply.pdf>

4. Information in Judicial Opinions and Records

Judicial opinions and court documents from around the country reveal ample details about how cell site simulators are used in particular investigations. The U.S. District Court for the District of Utah, for example, detailed testimony by an FBI agent describing, step-by-step, how he used a cell site simulator “to determine, with a reasonable degree of certainty, a fairly narrow geographical location where an individual is located while a cell call is being placed.” *United States v. Allums*, No. 2:08-CR-30 TS, 2009 WL 806748, at *1 (D. Utah, Mar. 24, 2009). In a Wisconsin case, police officers testified in a suppression hearing in open court about their use of a cell site simulator to track a cell phone signal to a particular apartment building. Motion Hearing Transcript at 13–16, *State v. Tate*, No. 09CF002842 (Wis. Cir. Ct., Apr. 22, 2011), *appeal pending*, No. 2012AP000336-CR (Wis. Argued Oct. 3, 2013). In a federal case in California, the court docketed a copy of the government’s application for an order authorizing use of a cell site simulator, which included a detailed description of how the device would be used:

A cell site simulator is a mobile device that captures the signaling information—the phone number, serial number, etc.—of cell phones within the vicinity. The cell site simulator mimics a cell site tower in that it reads signaling information broadcast in public by cell phones turned on in the area. After locating [the suspect] through physical surveillance, agents will position the cell site simulator nearby. Any cell phone that [the suspect] possesses (if turned on), as well as other cell phones nearby, will transmit their signaling information to the cell site simulator. Agents will repeat the process multiple times at different locations and times. By identifying the signaling data common to each capture—i.e., the signaling information that comes up each time—agents can determine the signaling information for a phone used by [the suspect].

Motion to Suppress Cell Site & Simulated Cell Site Evidence, Ex. B-1 at 2 n.2, *United States v. Espudo* (No. 12-CR-0236-IEG) 954 F. Supp. 2d 1029 (S.D. Cal. filed Apr. 8, 2013). In *Rigmaiden*, the U.S. District Court for the District of Arizona included a list of factual admissions by the government

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CR-15338
PAGE 27 of 29

concerning its use of a cell site simulator in the case. *Rigmaiden*, 844 F. Supp. at 995. A 2013 indictment filed in the Northern District of Illinois describes use of a cell site simulator (called a “digital analyzer device”) to identify a suspect’s cell phone number. Complaint, Affidavit of Robert Lukens at 8 n.1, *United States v. Arguijo*, No. 13-CR-0155 (N.D. Ill. Feb. 13, 2013). A 2006 opinion from the Southern District of Indiana describes law enforcement’s use of a cell site simulator “to pinpoint the multi-unit residence located at [the building address] as the precise location of a particular cell phone believed to be used by or otherwise connected with [the suspect].” *United States v. Bermudez*, No. IP05-0043-CR05-BF, 2006 WL 3197181, at *1 (S.D. Ind. June 30, 2006), *aff’d sub nom. United States v. Amaral-Estrada*, 509 F.3d 820 (7th Cir. 2007). In the District of New Jersey, a search warrant filed on the public docket by the government granted the FBI authority to use a stingray and described in detail its capabilities. Search Warrant to Obtain Location, Other Data, & Telephone Records for a Cellular Telephone Facility, *In Re Application of the United States for the Authorization to Obtain Location Data Concerning a Cellular Tel. Facility Currently Assigned Telephone Number (908) 448-3855*, Mag. No. 12-3092 (D.N.J. 2012). And in Florida, a police officer explained in court, step by step, how he used a stingray in a particular investigation, the capabilities of the device, and its impact on third parties.⁵⁴ These and other descriptions of stingray use in public judicial records belie the government’s claim that the information Mr. Harrison seeks is privileged.

* * *

The publicly available information about stingrays, including information about the Baltimore Police Department’s use of them, fatally undermines the government’s claim that information about the stingray in this case cannot be disclosed. See, e.g., Order Unsealing Suppression Hearing Transcript,

⁵⁴ *Thomas* Transcript at 10–23, *supra* note 10.

State v. Thomas, Case No. 37 2008-CF-3350A (Fla. 2d Cir. Ct. June 11, 2014). (rejecting government invocation of the law enforcement privilege and ordering information about stingray use in a criminal investigation to be disclosed). This Court should reject the government's attempt to shield important information about the legality and constitutionality of government conduct from public view.

CONCLUSION

For the foregoing reasons, the government's use of the stingray and collection of cell phone location information about Mr. Harrison pursuant to an invalid court order violated the Fourth Amendment and is not subject to a law enforcement exception. *Amici* respectfully urge the court to grant Mr. Harrison's motions to compel disclosure and suppress evidence.

Respectfully submitted,

/s/ David Rocah

David Rocah (Bar No. 27315)
Counsel of Record for Amici
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., Ste. 350
Baltimore, MD 21211
Phone: (410) 889-8555
Email: rocah@aclu-md.org

Nathan Freed Wessler⁵⁵
Of counsel
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad St., 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Email: nwessler@aclu.org

Dated: November 25, 2014

⁵⁵ Drafting assistance provided by Samia Hossain, Brennan Fellow, American Civil Liberties Union Foundation, New York, NY (recent law graduate; application for admission to New York State bar to be filed).

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
CALENDAR: 11
PAGE 1 of 7
CIRCUIT COURT OF
COOK COUNTY, ILLINOIS
CHANCERY DIVISION
CLERK DOROTHY BROWN

A Police Gadget Tracks Phones? Shhh! It's Secret

By MATT RICHTEL MARCH 15, 2015



Joe Simitian, a Santa Clara County, Calif., supervisor, pressed for more information about the StingRay surveillance device. Jim Wilson/The New York Times

A powerful new surveillance tool being adopted by police departments across the country comes with an unusual requirement: To buy it, law enforcement officials must sign a nondisclosure agreement preventing them from

Email

Share

Tweet

Save

More

Exhibit 1-F

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 2 of 7

saying almost anything about the technology.

Any disclosure about the technology, which tracks cellphones and is often called StingRay, could allow criminals and terrorists to circumvent it, the [F.B.I.](#) has said in an affidavit. But the tool is adopted in such secrecy that communities are not always sure what they are buying or whether the technology could raise serious privacy concerns.

The confidentiality has elevated the stakes in a longstanding debate about the public disclosure of government practices versus law enforcement's desire to keep its methods confidential. While companies routinely require nondisclosure agreements for technical products, legal experts say these agreements raise questions and are unusual given the privacy and even constitutional issues at stake.

“It might be a totally legitimate business interest, or maybe they’re trying to keep people from realizing there are bigger privacy problems,” said Orin S. Kerr, a privacy law

ton University. "What's the secret that they're

By Clare Major and Vanessa Carr 2:17

Securing Your Phone

lispote three weeks ago in Silicon Valley, where a sheriff asked county officials to spend \$502,000 on the technology. The Santa Clara County sheriff, Laurie Smith, said the technology allowed for locating cellphones — belonging to, say, terrorists or a missing person. But when asked for details, she offered no technical specifications and acknowledged she had not seen a product demonstration.

Buying the technology, she said, required the signing of a nondisclosure agreement.

"So, just to be clear," Joe Simitian, a county supervisor, said, "we are being asked to spend \$500,000 of taxpayers' money and \$42,000 a year thereafter for a product for the name brand which we are not sure of, a product we have not seen, a demonstration we don't have, and we have a nondisclosure requirement as a precondition. You want us to vote and spend money," he continued, but "you can't tell us more about it."

The technology goes by various names, including StingRay, KingFish or generically, cell site simulator. It is a rectangular device, small enough to fit into a suitcase, that intercepts a cellphone signal by acting like a cellphone tower.

The technology can also capture texts, calls, emails and other data, and prosecutors have received court approval to use it for such purposes.

Cell site simulators are catching on while law enforcement officials are adding other digital tools, like video cameras, license-plate readers, drones, programs that scan billions of phone records and gunshot detection sensors. Some of those tools have invited resistance from municipalities and legislators on privacy grounds.

The nondisclosure agreements for the cell site simulators are overseen by the Federal Bureau of Investigation and typically involve the Harris Corporation, a multibillion-dollar defense contractor and a maker of the technology. What has opponents particularly concerned about StingRay is

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 3 of 7

that the technology, unlike other phone surveillance methods, can also scan all the cellphones in the area where it is being used, not just the target phone.

“It’s scanning the area. What is the government doing with that information?” said Linda Lye, a lawyer for the American Civil Liberties Union of Northern California, which in 2013 [sued the Justice Department](#) to force it to disclose more about the technology. In November, in a response to the lawsuit, the government said it had asked the courts to allow the technology to capture content, not just identify subscriber location.

The nondisclosure agreements make it hard to know how widely the technology has been adopted. But news reports from around the country indicate use by local and state police agencies stretching from Los Angeles to Wisconsin to New York, where the state police use it. Some departments have used it for several years. Money for the devices comes from individual agencies and sometimes, as in the case of Santa Clara County, from the federal government through Homeland Security grants.

Christopher Allen, an F.B.I. spokesman, said “location information is a vital component” of law enforcement. The agency, he said, “does not keep repositories of cell tower data for any purpose other than in connection with a specific investigation.”

A fuller explanation of the F.B.I.’s position is provided in two publicly sworn affidavits about StingRay, including one filed in 2014 in Virginia. In the affidavit, a supervisory special agent, Bradley S. Morrison, said disclosure of the technology’s specifications would let criminals, including terrorists, “thwart the use of this technology.”

“Disclosure of even minor details” could harm law enforcement, he said, by letting “adversaries” put together the pieces of the technology like assembling a “jigsaw puzzle.” He said the F.B.I. had entered into the nondisclosure agreements with local authorities for those reasons. In addition, he said, the technology is related to homeland security and is therefore subject to federal control.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 4 of 7

In a second affidavit, given in 2011, the same special agent acknowledged that the device could gather identifying information from phones of bystanders. Such data “from all wireless devices in the immediate area of the F.B.I. device that subscribe to a particular provider may be incidentally recorded, including those of innocent, nontarget devices.”

But, he added, that information is purged to ensure privacy rights.

In December, two senators, Patrick J. Leahy and Charles E. Grassley, [sent a letter](#) expressing concerns about the scope of the F.B.I.’s StingRay use to Eric H. Holder Jr., the attorney general, and Jeh Johnson, the secretary of Homeland Security.

The Harris Corporation declined to comment, according to Jim Burke, a company spokesman. Harris, based in Melbourne, Fla., has \$5 billion in annual sales and specializes in communications technology, including battlefield radios.

Jon Michaels, a law professor at the University of California, Los Angeles, who studies government procurement, said Harris’s role with the nondisclosure agreements gave the company tremendous power over privacy policies in the public arena.

“This is like the privatization of a legal regime,” he said. Referring to Harris, he said: “They get to call the shots.”

For instance, in Tucson, a journalist asking the Police Department about its StingRay use was given a copy of a nondisclosure agreement. “The City of Tucson shall not discuss, publish, release or disclose any information

RECENT COMMENTS

augustborn March 17, 2015

It may one day make sense for the government to enlist all US internet capable devices and conscript them into becoming a sleeping massive...

FreeRange March 17, 2015

And the Santa County supervisors approved it anyway? Sounds like time for a recall! We're supposed to put our trust in protecting our...

Steen March 17, 2015

When the FBI, NSA and likes say "Trust us!" I tend not to. With zero oversight, and being a top secret proprietary piece of equipment - it...

[SEE ALL COMMENTS](#)

pertaining to the product," it read, and then noted: "Without the prior written consent of Harris."

The secrecy appears to have unintended consequences. [A recent article](#) in The Washington Post detailed how a man in Florida who was accused of armed robbery was located using StingRay.

As the case proceeded, a defense lawyer asked the police to explain how the technology worked. The police and prosecutors declined to produce the machine and, rather than meet a judge's order that they do so, the state gave the defendant a plea bargain for petty theft.

At the meeting in Santa Clara County last month, the county supervisors voted 4 to 1 to authorize the purchase, but they also voted to require the adoption of a privacy policy.

(Sheriff Smith argued to the supervisors that she had adequately explained the technology and said she resented that Mr. Simitian's questioning seemed to "suggest we are not mindful of people's rights and the Constitution.")

A few days later, the county asked Harris for a demonstration open to county supervisors. The company refused, Mr. Simitian said, noting that

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 6 of 7

“only people with badges” would be permitted. Further, he said, the company declined to provide a copy of the nondisclosure agreement — at least until after the demonstration.

“Not only is there a nondisclosure agreement, for the time being, at least, we can’t even see the nondisclosure agreement,” Mr. Simitian said. “We may be able to see it later, I don’t know.”

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 7 of 7

Stingray spying: FBI's secret deal with police hides phone dragnet from courts

Non-disclosure agreement in Florida reveals chain of secrecy across US
Federal authorities maintain 'totalitarian' control over local law enforcement

Jessica Glenza in Los Angeles and Nicky Woolf in New York

Friday 10 April 2015 10.49 EDT

The FBI is taking extraordinary and potentially unconstitutional measures to keep local and state police forces from exposing the use of so-called "Stingray" surveillance technology across the United States, according to documents obtained separately by the Guardian and the American Civil Liberties Union.

Multiple non-disclosure agreements (NDAs) revealed in Florida, New York and Maryland this week show federal authorities effectively binding local law enforcement from disclosing any information - even to judges - about the cellphone dragnet technology, its collection capabilities or its existence.

In an arrangement that shocked privacy advocates and local defense attorneys, the secret pact also mandates that police notify the FBI to push for the dismissal of cases if technical specifications of the devices are in danger of being revealed in court.

The agreement also contains a clause forcing law enforcement to notify the FBI if freedom of information requests are filed by members of the public or the media for such information, "in order to allow sufficient time for the FBI to seek to prevent disclosure through appropriate channels".

The strikingly similar NDAs, taken together with documents connecting police to the technology's manufacturer and federal approval guidelines obtained by the Guardian, suggest a state-by-state chain of secrecy surrounding widespread use of the sophisticated cellphone spying devices known best by the brand of one such device: the Stingray.

Made by Florida-based Harris Corporation, the Stingray and similar devices are known as IMSI-catchers or cell-site simulators.

Often not much bigger than a suitcase, the devices are easily portable. They gather information by imitating cellphone towers, scooping up metadata from all devices that connect to the fake tower. Experts told the Guardian that the devices may also be capable of gathering content from phones that connect to them.

Exhibit 1-G

The secrecy required by such NDAs is perhaps why information on the use of Stingrays by local police forces remains scarce after years of probing by civil-liberties advocates - and why the true scale of the technology's use is unknown. But other documents recently obtained by the Guardian and the ACLU hint at how widespread the practice might be.

The ACLU has shown that at least 48 agencies across 20 states likely use the devices. Documents obtained by the Guardian show police from states as such as Texas, Florida, Washington, Minnesota, Virginia, Florida, Maryland, Illinois, Arizona, and California utilize the devices.

The Florida agreement - obtained from the Hillsborough County sheriff's office by the Guardian after a series of Stingray-related Freedom of Information Act requests sent over the past seven months - reads in part:

"The Florida Department of Law Enforcement will, at the request of the FBI, seek dismissal of the case in lieu of providing, or allowing others to use or provide, any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation."

Law enforcement agencies that sign NDAs similar to the one in Hillsborough County are barred from providing "any information" about the Stingray-style devices in search warrants, pre-trial hearings, testimony, grand jury proceedings, in appeals or even in defense discovery. Per the agreement, police can only release the "evidentiary results" obtained with the device.

ELECTRONICALLY FILED
APR 7 2015
PAGE 1 OF 14
AP If the police think a prosecutor is "considering" including such information in a trial, they must notify the FBI, "to allow sufficient time for the FBI to intervene to protect the information/technology and information from disclosure and potential compromise."

In other words, police can tell the courts about the information they found with the portable spy gadgets - just not how they found it.

"It reminds me of what happens in totalitarian countries: you don't know what the hell is going on," said law professor Bruce R Jacob, the former dean of Stetson law school in Florida, when shown a copy of the NDA for Hillsborough County, which includes the Tampa metropolitan area.

"That's an interference by the FBI and this company, and FDLE in the operation of the local courts," he said.

In response to a detailed list of questions from the Guardian, the FBI sent a copy of an affidavit from 2014 by supervising special agent Bradley Morrison, chief of the agency's tracking technology unit.

The FBI affidavit states that the agency believes cell-site simulator devices are exempt from discovery because information "could easily impair use of this investigative method", and affirms the agency's policy of secrecy on the matter.

“Disclosure of even minor details about the use of cell site simulators may reveal more information than their apparent insignificance suggests because, much like a jigsaw puzzle, each detail may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself,” the affidavit states.

The Florida department of law enforcement (FDLE) and its subsidiary in the Hillsborough County sheriff’s office did not respond to requests for details from the Guardian. Harris Corp said Thursday it could not comment.

The FBI’s extreme secrecy: ‘Interfering with the courts’

Two additional versions of similar Stingray NDAs – only with different county names – were obtained this week, one following a lawsuit against the Erie County sheriff’s office by the ACLU of West New York, and the other by a Baltimore defense attorney trying a city carjacking case.

An equipment grant authorization document obtained by the Guardian from the Federal Communications Commission (FCC) states that local police must coordinate with the FBI to use Harris Corporation’s devices. “State and local law enforcement agencies must advance coordinate with the FBI the acquisition and use of the equipment authorized under this authorization,” the document states.

And similar NDAs have also been obtained – albeit in heavily redacted form – in Washington state and Minnesota.

The dynamic we’re seeing is the federal government leaning heavily on local police,” ACLU staff attorney Nathan Freed Wessler said. “Even departments who have said that they would like to be more transparent are being prevented from doing so by this agreement that they’re being forced to sign.”

The provision for pushing cases for dismissal rather than reveal information about Stingray capabilities and scope, he said, represented “the FBI’s consistent policy of making local police maintain extraordinary and extreme secrecy”.

Jacob, the law professor who has reviewed the pacts, said they were “interfering with the operation of the courts” and judges’ ability to evaluate whether a search and seizure involving Stingray technology is even constitutional under the fourth amendment. He said the NDA could also interfere with fair hearings, allowing some defendants to walk free while others are convicted on the basis of the evidence obtained with such devices.

“The defendant who finds out about this is able to get his case dismissed, and the other defendant can’t? That’s unfair.”

From Baltimore to Tampa to Stingray HQ: ‘Your phone calls are at risk’

Despite the sweeping NDAs that law enforcement offices like the Hillsborough County sheriff have signed, local departments have recently struggled to keep a lid on their use of the dragnet.

In Baltimore on Tuesday, police revealed another example of the FBI non-disclosure agreement in court - and also that they had used Stingray technology 4,300 times since 2007, according to defense attorney Joshua Insley. In other cities across the country - from Texas and Minnesota to California and Washington state - the Guardian has obtained invoices, purchase orders and training documents confirming the use of Stingrays.

In June 2014, according to a training request obtained by the Guardian, Hillsborough County detective Mark Gilbertson wrote that the FDLE would pay \$5,000 for 11 days of "necessary training" at the Harris Corporation's base in Melbourne, Florida, on a \$780,000 "piece of cellular equipment".

The exact type of device remains unclear, but the request said the training was "vital to the sheriff's office" and that "only" one other employee at the office was "actively trained in this equipment".

In its freedom of information response to the Guardian, the Hillsborough sheriff's office refused to hand over any training materials, saying they were the property of Harris Corporation and "proprietary". The NDA bars "direct or indirect statements to the media" about Harris corporation equipment.

ELECTRONICALLY FILED
6/30/2015 12:12:13 PM
Case No. 14-1447-A
Page 4 of 4John Sawicki, a former police officer who founded Forensic Data Corp, a company that consults attorneys on technological evidence, said "one of the problems we have is we don't know for sure" what Stingrays specifically can even do, wherever they are used.

"When you get an officer into a deposition and ask what the capability of the device is, they say, 'Well I can't get into it because of the NDA.' We're left to speculate a bit as to what the device can do," he said.

"We believe that, at least in some cases, the device has the ability to pull content, so all the sudden your text messages are at risk, your phone calls are at risk, and your data transmission, potentially."

The NDAs drastically reduce courts' access to documents on the devices. With provisions that restrict defense attorneys' discovery, pre-trial motions, testimony and even court orders, defense attorneys say even basic due process has become frustratingly difficult.

For example, the FBI-police pact would make it impossible to determine whether local law enforcement were properly trained to operate the surveillance devices.

In most cases, law enforcement only need to apply for a court order known as a 'PEN register' to use a Stingray, based on 1986 legislation designed to track outgoing calls from a land-line phone.

Brian Owsley, a former Texas judge and now law professor at the Indiana Institute of Technology, said the judicial standard for granting PEN register applications was "very low" - it does not require 'probable cause' - and woefully inadequate to cover technology with bulk collection capabilities like Stingray. He also said judges themselves may not

understand how powerful the devices are.

In any case, Owsley said, police officers from any jurisdiction with access to the devices could also simply choose to use them off the books.

When judges attempt to compel the FDLE to release information about the tracking devices, the state police agency must forward such notices to the assistant director of the FBI's Operational Technology Division, and to the chief of the Technology Tracking Unit in Quantico, Virginia. Freedom of Information requests are also forwarded to the two department heads.

This kind of sweeping secrecy has led to tense exchanges in courtrooms, and the crumbling of prosecution's cases, as they attempt to maintain secrecy. City councils may even be unaware that the police departments they oversee are using the devices if the local force has signed similar agreements with the FBI.

Now, defense attorneys appear to be catching on to the practice. In Tallahassee, Florida, the ACLU has amassed a list of more than 300 cases where they believe Stingrays have been used to locate clients, and at least one Florida case recently came undone when defense attorneys began to dig into the involvement of Stingrays.

APPEAL FILED
12:14-cr-00158
Attorneys started asking questions about how police found her client.

ELECTRONICALLY FILED
12:14-cr-00158
PAGE 5 OF 5

More news

Topics

FBI

Surveillance

New York

Maryland

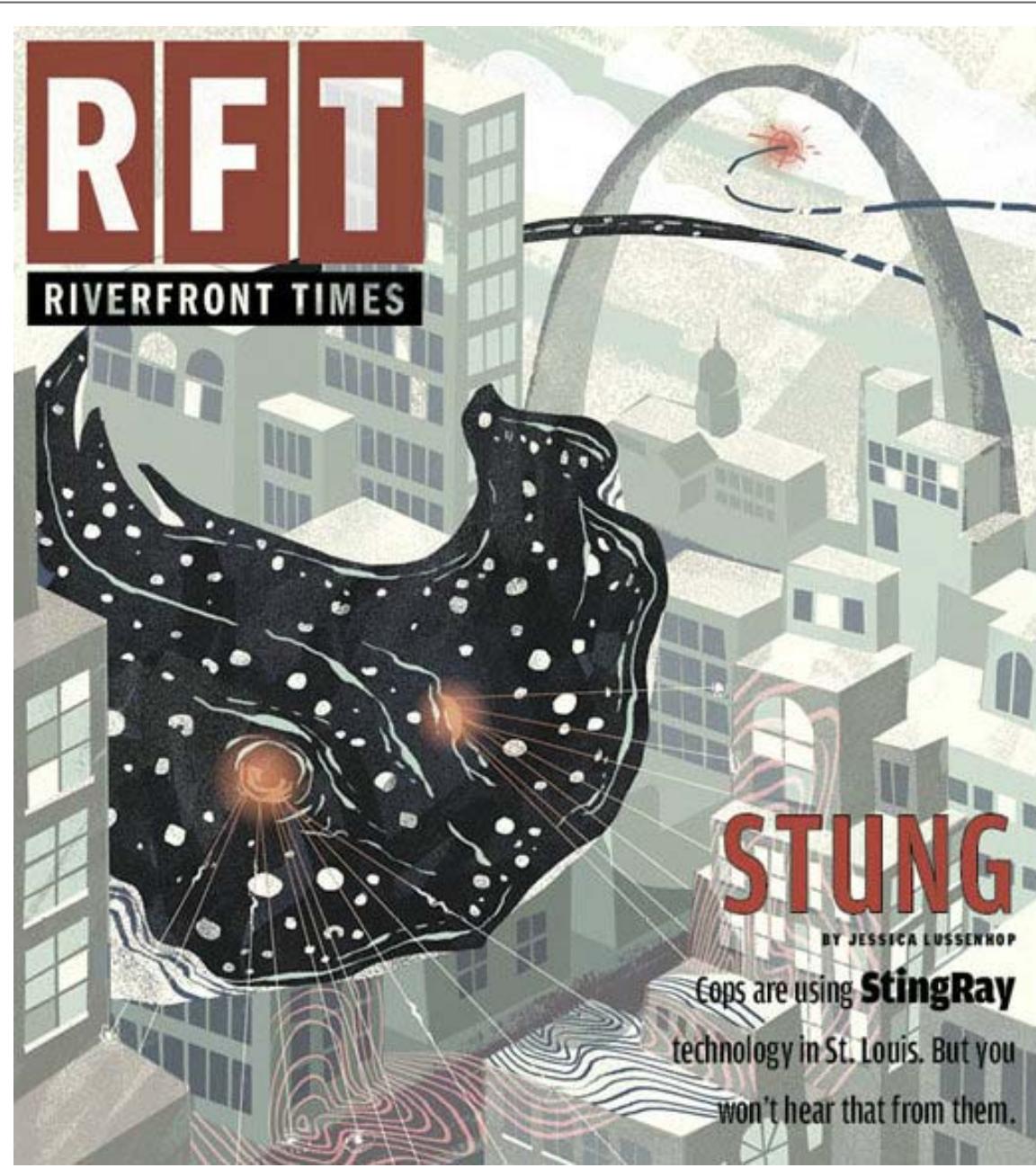
Florida

More...

St. Louis Police Have Used StingRay Technology for Years -- They Just Won't Talk About It

By Jessica Lussenhop

Published Wed., May 20 2015 at 8:00 AM



There were some very bad vibes in downtown St. Louis on the night of October 28, 2013. The Cardinals had just lost Game 5 in the World Series, and the Rams had a pathetic showing against the Seahawks at Edward Jones Stadium. The streets were jammed bumper to bumper with disgruntled fans trying to make it home, and so Brandon Pavelich and Julia Fischer — two college friends on a kinda-sorta first date — decided to walk around a bit before attempting to leave the area.

Then they heard fast footsteps, and the next thing they knew, two men had guns pointed at their heads. They demanded money and cell phones.

Pavelich paused.

"Show him we're serious and shoot him," he remembers one of the men saying.

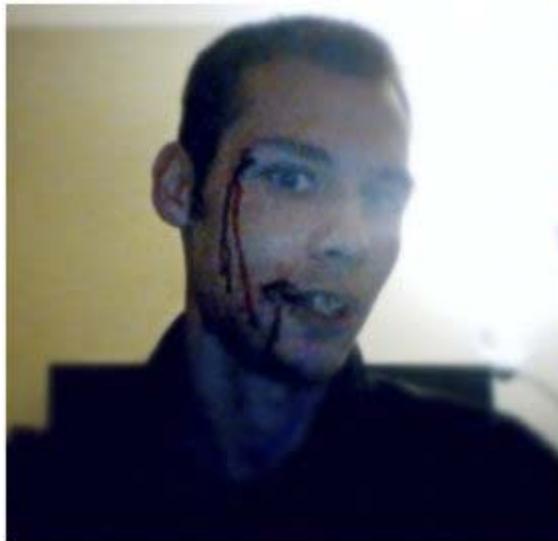
Instead, a gun smashed into Pavelich's face, opening a gash in his forehead and chin, and chipping a tooth. One of the men reached into Pavelich's pockets as he was reeling, and grabbed his iPhone and cash. They took Fischer's iPhone as well, and ran.

Luckily, Pavelich and Fischer found a St. Louis police officer nearby. They soon learned theirs was the last in a string of muggings that evening. In total, seven victims had their phones taken, though Pavelich was the only one who had to spend the night in a hospital getting stitches.

Fischer recalls that the police behaved as if they were hot on the trail of the stolen phones.

"They did say that they're tracking it," she says. She assumed that meant they were using the phones' GPS or something like the Find My iPhone app.

By the next day, four suspects were in custody, including a supposed lookout and a getaway driver. They were found in a hotel room in Caseyville, Illinois, allegedly with the stolen phones. Among the recovered property, Pavelich was able to identify the case he'd had on his phone. It seemed like a done deal.



Courtesy Brandon Pavelich

Brandon Pavelich just after the attack, and a few days afterward.

But a year and a half later, as the trial date for three of the men got closer, Fischer called the prosecutor to find out when she needed to be in court. That's when he told her they'd dropped the charges.

"The reasoning was, there came up some legal issues that would cause insurmountable issues so that they wouldn't be able to continue with the case," says Fischer. "That's really all that they told me."

Two weeks later a story in the *St. Louis Post-Dispatch* helped shed some light on what happened. Titled "Controversial secret phone tracker figured in dropped St. Louis case," it explained that investigators had used a relatively new tracking device called a cell site simulator to trace one of the stolen phones. It was so accurate — more accurate than GPS — that it was able to pinpoint the exact hotel room where the accused thieves were holed up.

The technology is often referred to by a brand name: StingRay. When deployed, StingRay forces any cell phones in the area to send it a signal, the same way that a phone normally sends a signal to cell towers. Even if a cell phone is not in use, it still transmits its phone number and electronic serial number to the device.

Once a tool used by federal officials for combating terrorism, in the last decade StingRay-type devices have been approved for use by local law-enforcement agencies. Officers have been using the technology under the purview of the FBI — and only under strict orders not to disclose anything about it even in court.

The *Post-Dispatch* story about Pavelich and Fischer's case hypothesized that authorities were backing away from the charges because they did not want to be forced to put a police intelligence officer on the stand and reveal how StingRay works — that government secrecy was essentially more important than a conviction. That did not sit well with Pavelich.

"I got hurt by these guys pretty bad, and they're just walking free now. It pissed me off a little bit," he says.

It may not be quite as simple as that. The St. Louis Circuit Attorney's Office has insisted repeatedly that the use of a StingRay is not why they dropped the case against the four suspected robbers.

"Contrary to the opinion of defense attorneys and to recent reports in the media, the dismissal of the cases was not related in any way to any technology used in the investigation," Lauren Trager, a public information officer for the circuit attorney, said in a statement. She declined to answer further questions about the case, as it is now considered a closed record.

Regardless of why the case was thrown out, it shows that one thing long suspected by local activists is now certain: St. Louis police are using StingRay devices or ones with similar data-capturing capabilities in their investigations.

Until recently, First Amendment watchdog groups like the ACLU said only that it was "probable" that StingRays were being used in St. Louis. But this case, along with documents obtained by *Riverfront Times*, are beginning to shed some light on the practice locally.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
7/2/2014 CHG PAGE 3

And now that StingRay is here, privacy advocates have a host of concerns: that innocent people's data may be collected without their knowledge, that merely deploying the device is equivalent to unconstitutional search and seizure, and that it may be used to spy on those simply exercising their legal right to free speech.

Local attorneys, journalists and citizens have joined those in other American cities (at least 51 state and local jurisdictions by the ACLU's count) who are struggling to understand StingRay, and are finding a wall of law-enforcement silence on the other side of their questions.

"It's ridiculous," says Hanni Fakhoury, senior staff attorney for the Electronic Frontier Foundation, a civil-liberties advocacy nonprofit. "It's secrecy for the sake of secrecy. It's not actually a public-safety issue now."

[\[View as a single page.\]](#)

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 4 of 13



Ray Downs

Ferguson.

In the dizziest days following Michael Brown's death in Ferguson, it was common to hear someone in a protest on West Florissant or out in front of the police station complaining that her cell phone was acting up — dropped calls, weird tones and clicks. Thomas Harvey, an attorney and executive director of the ArchCity Defenders, remembers many of his activist clients fretting that they were being electronically monitored.

"The night of the non-indictment, everyone's phone was shutting off or turning on. They couldn't use Google Maps. I had the same thing happen to me," he recalls. "There's no way for me to know what caused that."

(St. Louis County Police spokesman Brian Schellman says his department does not have a StingRay unit, but plenty of other law-enforcement agencies were on the scene in north county, including St. Louis and the FBI.)

While StingRay provides many benefits to law enforcement, how its capabilities will affect the general populace isn't as clear. Many people, like the protesters in Ferguson, worry their phones are being monitored while simply exercising First Amendment rights. They have some reason to be paranoid — federal authorities have admitted that StingRay can cause nearby phones to act glitchy, and in at least one instance, a law-enforcement agency has been open about wanting to monitor protesters: The Miami-Dade Police Department requested an emergency purchase of a StingRay just prior to the Free Trade Area of the Americas conference in 2003.

"Based on the history of these conferences, the department anticipated criminal activities directed at attendees and conference sites facilitated by the use of cellular phones," the request reads. "Wireless phone tracking systems utilized by law enforcement have proven to be an invaluable tool in both the prevention of these offenses and the apprehension of individuals attempting to carry out criminal activities."

There's also documented use of StingRay to track alleged perpetrators' movements, which civil-liberties advocates call a violation of the suspect's Fourth Amendment rights to be free from unreasonable search and seizure — because the signal travels into private spaces, through walls.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 5 of 13



Courtesy of Daniel Rigmaiden

Daniel Rigmaiden in Arizona.

The first court case where the government acknowledged the existence of StingRay technology came out of a tax-fraud prosecution in Arizona in 2008, in which police used the tracker to locate the wireless broadband modem or "AirCard" of a man named Daniel Rigmaiden. Rigmaiden had been using it to access the Internet and submit fake tax returns, netting about \$500,000 over the course of three years.

"I knew the instant I was arrested that they had to track down my AirCard," Rigmaiden says now. "There wasn't any other flaw in my methods."

The "flaw," as he puts it, was assuming that law enforcement would reserve the use of high-tech tracking technology for terrorism or kidnapping cases — not a lowly tax frauder. Turns out police use StingRay for a wide range of cases — which left Rigmaiden and his AirCard a sitting duck for the investigators hot on his trail.

As Rigmaiden mounted a pro se defense, he compelled federal investigators to produce tens of thousands of pages of documents. That paperwork, along with the testimony he obtained, gave the world its first glimpse at how the technology works.

Rigmaiden was unsuccessful in his argument that the StingRay sweep was unconstitutional. However, rather than getting more than twenty years in prison, prosecutors offered him time served in exchange for a guilty plea. The Arizona man got out of prison a year ago and now works to combat StingRay secrecy.

"Every citizen has a duty to make sure the Constitution is upheld," he says. "I have the opportunity to do it in this particular area."

Since Rigmaiden's case, dribs and drabs of information about the technology have come out of other criminal cases, but government secrecy has ruled the day. That may be about to change. Earlier this month the U.S. Department of Justice announced that it would review use of the technology by all forms of federal law enforcement including the FBI, the DEA and the U.S. Marshals.

"They wouldn't call it an investigation. It seems to be a reevaluation of their policy," says Nathan Wessler, attorney for the Speech, Privacy, and Technology Project at the American Civil Liberties Union. "It's crucial that local law enforcement follow suit immediately, including in St. Louis."

ELECTRONICALLY FILED
7/2/2015 12:12 PM
1 PAGE OF 132

In St. Louis, former Division 16 Circuit Court Judge Jack Garvey says the first he heard of the "magical" technology that could track phones was during his regular Wednesday meeting with former police chief Dan Isom and Circuit Attorney Jennifer Joyce in 2011. At the time, he says, the cell site simulator belonged to the local branch of the U.S. Secret Service (apparently St. Louis has one of those, too).

"Isom says, 'We can use this device that is sitting in the back of a parking garage at police headquarters,'" recalls Garvey.

In those early days, Garvey agreed to sign off on warrants allowing the police to use the Secret Service's device to look for phones taken from crime victims. They had to provide the serial number for the phone and the cell service provider.

The police and the prosecutors kept this new-fangled tactic tightly under wraps. But Garvey says he spoke openly about the warrants and was astonished no defense attorney ever followed up with questions during the year he was signing them.

"It was a joke," he says. "We were yukking it up back then."

At some point after Garvey moved to the 17th Division and was no longer the primary judge signing

the warrants, the way cell site simulator technology was used at the department changed. The same month that Isom announced his retirement, the board of commissioners for the St. Louis Metropolitan Police Department put out an invitation for bids for a "Stingray II System" and the installation of the system in a Chevrolet Tahoe. StingRay units are relatively portable — some are about the size of a suitcase, and can be installed in vehicles and taken on the road.

At this point, StingRay deployment is more like an old-fashioned game of cops-and-robbers than an omniscient Big Brother seeing and knowing all. According to the ACLU the device is often hooked up to a laptop in a police car, and officers drive around as the laptop display shows them whether the signal is getting hotter or colder. Some authorities have even described walking with handheld units through large apartment buildings until they were certain which room had the phone inside.

Although several companies produce this type of product for law enforcement, the leader is Florida-based Harris Corporation, which is also the only company that calls its devices "StingRay."

"Harris is kind of like the Apple corporation of the surveillance world. It's really easy to use their stuff," says Rigmaiden. "The other stuff is more complicated."

Prices for these types of devices range from \$16,000 to \$400,000 for a suite of technology.

It's not clear whether the St. Louis Police Department successfully purchased the StingRay, or decided to continue using loaners from some other federal jurisdiction. An attorney for the city denied a Sunshine Request for any purchasing paperwork, saying the documents would "reveal trade secrets and commercial or financial information." Isom wouldn't comment on where the purchase stood at the time of his departure, and Police Chief Sam Dotson has not responded to interview requests.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
BCH-RF
PAGE 7
The department did respond to *RFT*'s request for applications for search warrants or orders authorizing the use of cell site simulators. That request yielded two examples. To Garvey, they're unrecognizable from the orders he signed four years ago.

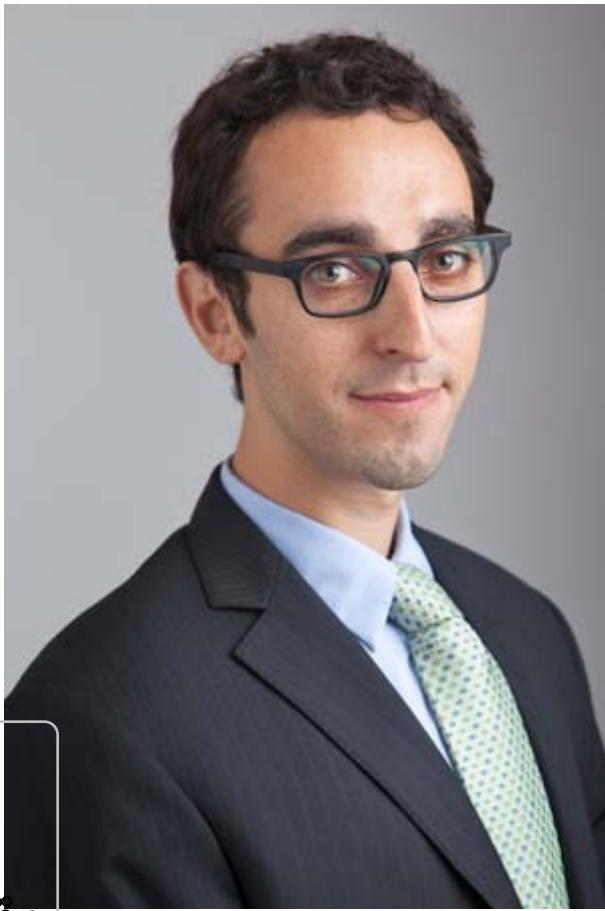
"It's more of a broad thing. My search warrants that we were doing were, 'This is the phone of this person, this is the serial number of this phone,'" he says. "Something happened. Either the cops got a new machine, or they're running it from a new machine."

The two example applications given to *RFT* are called "pen register applications," more commonly understood as applications to install a device that reads which numbers are being dialed — and which are incoming — on a landline. But the new application paperwork broadens the language to include "cell site activations," "call detail records in an electronic format" and, most densely, "24-hour a day assistance to include switch based solutions including precision location pursuant to probable cause based information queries and all reasonable assistance to permit the aforementioned Agencies to triangulate target location."

That last, almost inscrutable paragraph is the closest the documents come to referring directly to StingRay usage.

To Wessler of the ACLU, the very vagueness of that language makes it unconstitutional.

"This violates the Fourth Amendment," he concludes after reviewing *RFT*'s documents. "Nothing in the



Courtesy of the ACLU.

The secrecy in cities across the country has been so extraordinary," says Nathan Wessler, staff attorney for the ACLU.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014CH-15338
PAGE 13

applications suggests that police will be using cell site simulators. Nor do the applications explain to the judge the capabilities of cell site simulators."

It's also simply too easy for police to obtain pen register application approval, Wessler says, as opposed to the higher burden of proving probable cause for a warrant. To obtain a warrant, police have to show there's a preponderance of evidence — as spelled out in the Fourth Amendment — that makes their search necessary.

For a pen register application, all cops have to show is that it could help the investigation. And because of the extremely vague and/or technical language in the applications, judges may have no idea they're authorizing use of a StingRay — the term simply never appears in the document.

Privacy advocates are also concerned about what happens to the data from innocent bystanders in the area who may have their phones swept.

A good analogy, says the ACLU's Nathan Wessler, is a game of Marco Polo: "The device yells 'Marco!' and all the [nearby] phones are forced to yell back 'Polo!' The StingRay can then be used to hone in on the signal from the suspect's phone and locate him/her based on the strength and direction of the signal. But

all the while, every other phone is still being forced to yell 'Polo!' over and over, letting the StingRay know that they are in the area too."

It's those other phones that have some activists worried.

"What is done with all that data that's irrelevant? Are they keeping that information, or are they deleting it?" asks Electronic Frontier Forum attorney Fakhouri. "These things identify phones in the area; they don't necessarily listen in on phone conversations or capture data. But that is a technical limitation. What that means is, they are configured not to do that, but we don't know how they're *not* doing that."

One thing appears to be similar from the days when Garvey was signing off on the StingRay warrants: the ones obtained by *RFT* show that, locally, the device has only been used to track the phones of victims, rather than perpetrators or activists.

The two heavily redacted pen register applications provided by the police department are both from homicide cases in which the alleged murderer is thought to have stolen the victim's phone.

"Victim _____ registered a hotel room on _____ and prepaid through _____. Witnesses at the scene reported hearing a loud argument near the victim's room earlier in the week," reads one of the applications. "Detective _____ stated an _____ wall charger located in _____ hotel room;

however no _____ was located in his room or on his person."

The second application describes a drug deal gone bad, with one fatality. "A suspect pulled a long barreled firearm and began firing shots at the victims. _____ was able to flee the residence through a second floor window and later discovered the other victims had been shot. During this incident victim _____ disclosed his cellular phone had been stolen."

Both applications were approved for 60 days, and the judge — whose name is also redacted — agreed that the orders be sealed.

Garvey says at least one StingRay warrant he signed off on caught a murderer, a guy who was strolling out of a Walmart with the stolen phone in his pocket.

"I'm telling you, it's doing miracle work," he says.

St. Louis Pen Register Applications and Orders

ELECTRONICALLY FILED
7/2/2015 12:12 PM
533813

SHOW ME MORE LIKE ST. LOUIS PEN REGISTER APPLICATIONS AND ORDERS
SIMILAR TO ST. LOUIS PEN REGISTER APPLICATIONS AND ORDERS

BACK TO DOC

More from [Jessica Lussenhop](#)

Previous | Next

[PERF Report -- Overcoming the Challenges 5 1 15 \(1\)](#)

[Jessica Lussenhop](#)

[Johnson, Dorian charging documents](#)

[Jessica Lussenhop](#)

[Dorian Johnson vs. Ferguson](#)

[Jessica Lussenhop](#)

[Michael Brown Civil Lawsuit](#)

[Jessica Lussenhop](#)

[ACLU Sues Pine Lawn, Sylvester Caldwell, Former Police Chief](#)

[Jessica Lussenhop](#)

[Kimber Edwards stay](#)

[Jessica Lussenhop](#)

[Larry Flynt opinion death penalty](#)

[Jessica Lussenhop](#)

[Journalists Sue St. Louis County Police](#)

[Jessica Lussenhop](#)

[Search Warrant for Jeffrey L. Williams](#)

[Jessica Lussenhop](#)

[Joy Arnold lawsuit against City of Florissant](#)



[Google Street View](#)

Carnahan Courthouse

ELECTRONICALLY FILED
7/2/2015 12:12 PM
Case No. 14-01-338
PAGE 10 OF 13

For assistant public defender Megan Beesley, her journey down the StingRay rabbit hole began with five little words: "A proven law enforcement technique."

Beesley, who works out of the Carnahan Courthouse downtown, remembers the phrase leaping out at her when she read the police report from the post-Game 5 robberies on October 28, 2013. Her client was one of the men arrested for his role in the string of muggings, and the line was used as the only explanation for how authorities managed to find him and his alleged accomplices in the hotel room in Caseyville.

"A proven law enforcement technique" seemed almost like the cop-speak equivalent of *Seinfeld's* "yadda yadda yadda."

"It seemed like a very odd sentence to me," she says.

Beesley got the chance to ask about the phrase at a November 7, 2014, deposition of St. Louis police detective John Anderson.

"I just said, 'What does this mean?' The detective acted really weird, looks at the prosecutor, who acts really weird," she recalls. "They go outside and talk. He comes back in and awkwardly refuses to answer."

At a subsequent hearing, Anderson again said he could not answer, Beesley recalls, because of a "non-disclosure agreement that had to do with the FBI. So that confirmed to me that this was probably a StingRay."

In order to use the technology, sheriffs and police chiefs have historically had to sign a non-disclosure agreement with the FBI and the Harris Corporation agreeing not to provide the public with any

information about how it works. According to an affidavit given by a supervisory FBI agent in a 2014 case in Virginia, if a prosecutor were to disseminate technical information about StingRay to media with international readership, it could constitute a violation of the Arms Control Export Act, which is a felony. That blanket of silence also covers court proceedings.

St. Louis police refused even to allow the *Riverfront Times* to view any non-disclosure agreement it may have with its cell site simulator provider or the FBI, declining our Sunshine Act request.

One such agreement, obtained from the Erie County Sheriff's Office in New York State, reads: "If the Erie County Sheriff's Office learns that a District Attorney, prosecutor, or a court is considering or intends to use or provide any information concerning the Harris Corporation wireless collection equipment...the Erie County Sheriff's Office will immediately notify the FBI in order to allow sufficient time for the FBI to intervene to protect the equipment/technology and information from disclosure and potential compromise."

In a handful of incidents around the country, prosecutors have dropped cases, offered plea deals or withdrawn evidence rather than disclose information about StingRay. That happened in Baltimore, Maryland; Tacoma, Washington; and Tallahassee, Florida — and even in homicide cases.

"It is troubling that their use of this extraordinary secrecy is getting in the way of proper government functions," says Wessler. "I suspect part of what this secrecy is protecting is constitutional violations."

Christopher Allen, a spokesman for the FBI Office of Public Affairs, says that the purpose of the non-disclosure agreements is to prevent criminals from learning how the technology works and figuring out a way to avoid it.

ELECTRONICALLY FILED
7/2/2015 12:42 PM
PAGE 11 OF 11
Specific capabilities of certain equipment used by law enforcement agencies are considered Law Enforcement Sensitive, since their public release could harm law enforcement efforts by compromising future use of the equipment," he said in a statement. "As a last resort, after exhausting all other legal means to protect LES information, the NDA does require state and local law enforcement to drop a criminal case rather than compromising the future use of the technique by disclosing LES information."

He insists, however, that the FBI has never forced any jurisdiction to dismiss a case because of the agreement.

Regardless, Beesley is convinced that by dropping charges against her client, the St. Louis circuit attorney is helping honor a non-disclosure agreement signed by the city police. She and her colleagues scoured their current caseload and found the phrase "a proven law enforcement technique" in four different police reports.

"I think that's the closest we've come to the cops acknowledging this," she says.

Riverfront Times contacted several defense attorneys and only found one additional case with the "proven law enforcement technique" verbiage in the police report. Nick Williams, a criminal defense lawyer whose client was arrested and charged in a different robbery case, says he noticed the phrase even before the *Post-Dispatch* piece and has alerted the prosecutor at the circuit attorney's office to his concerns. His client's next court date is in June.

"It begs the question of whether or not there is an official policy in place, and if so, what is that

policy?" says Williams. "The way in which this is being used on a local level is certainly an infringement on an individual's Fourth Amendment rights.

"A person has a right to privacy, and an infringement on that privacy should be protected against."

Although St. Louisans are just waking up to the fact that StingRay is swimming in their back yards, the secrecy surrounding the technology is beginning to drop away across the country. That's starting with increased willingness by local law enforcement to simply admit that they are using the devices.

For example, Baltimore disclosed recently that it deployed the technology 4,300 times since 2007. In Tallahassee, a police investigator admitted they'd used it 200 times. (The *Post-Dispatch* puts the number of approved pen register applications locally at 80.)

Legislators are showing increasing discomfort with StingRay. Ten states, including Illinois, Florida and Maryland, have passed some kind of legislation designed to force local law enforcement to obtain a warrant before using cell-phone-tracking technology. A bill Daniel Rigmaiden helped to shape just passed in Washington State.

Even the federal government is paying more than lip service to the idea that its warrantless deployment of StingRay technology may be unconstitutional. Soon after, to the announcement by the DOJ that they will review the usage of the technology, the FBI went even further in a May 14 article in the *Washington Post*. The agency told the newspaper that its officers will now apply for a warrant before using StingRay, and that it's OK for local law enforcement to acknowledge the use of the technology, as long as details about how it works are kept secret.

ELECTRONICALLY FILED
72/2015 12:12 PM
PAGE 1 OF 5
CHS
It's kind of throwing local agencies under the bus a little bit," says Wessler. "Now the FBI's saying, 'No, no, no, that's not what we really meant,' which is a helpful clarification now, but there are years' worth of cases where defense attorneys were kept completely in the dark, as well as judges, and that needs to be remedied right now."

Not everyone in the criminal justice system may be on board with the technology's black-box status either. Judge Garvey, who has praised the usage of StingRay, does not agree with the secrecy imposed by the nondisclosure agreements.

"I think the FBI — they're kind of dumb," he says. "They're being overly federal about the whole thing."

When the last of the four alleged Game 5 muggers had her case dropped in a St. Louis courtroom on April 27, Assistant Circuit Attorney Tanja Engelhardt made an interesting statement as reported by the *Post-Dispatch*. She let slip that though StingRay practices in St. Louis haven't been litigated yet, "They will be. This isn't the case."

In a statement to *Riverfront Times*, Trager nudged the sentiment slightly further: "The technology has been used around the country and has withstood challenges in the past. The legality of this technology has recently been challenged in this jurisdiction, and we anticipate it will be litigated in a court of law."

As for Brandon Pavelich, he's more confused than ever about his case. If it wasn't dismissed because

of StingRay, what happened?

"If that's the big controversial issue, and that's not it, what the heck could it be?" he says. "That feels super sketchy. What are these guys doing?"

Then again, Pavelich says, it's not as though he just had his eyes opened to the fact that the criminal justice system doesn't always function properly. He has two brothers who've been in and out of the prison for years, he says, mostly for non-violent drug offenses and parole violations. He's not naïve.

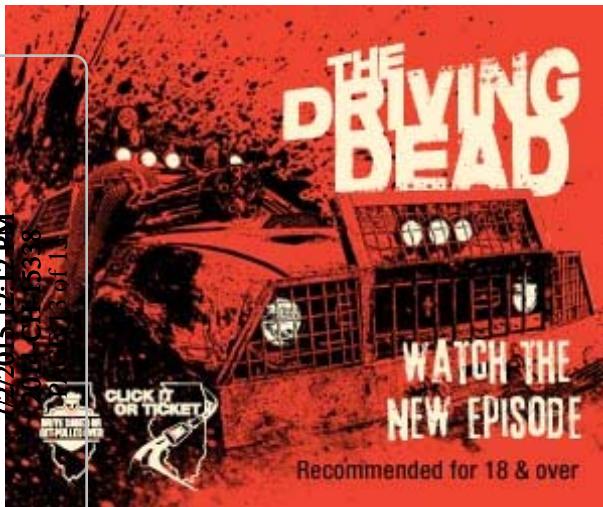
"I really see the system as being stupid anyway," he sighs. "I'm not entirely surprised these things are happening."

Additional (and crucial) reporting by Chris McDaniel.

Email feedback or tips to the author at Jessica.Lussenhop@RiverfrontTimes.com.

[Follow @lussenpop](#)

ELECTRONICALLY FILED
72/2015-12-12 PM
B614-B3-8
1 of 1



IMSI Catcher

Daehyun Strobel

13.Juli 2007

Seminararbeit
Ruhr-Universität Bochum



Chair for Communication Security
Prof. Dr.-Ing. Christof Paar

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 2 of 28

Contents

1	Introduction	1
2	GSM (Global System for Mobile Communications)	3
2.1	Mobile Station	4
2.2	Base Station and Base Station Controller	4
2.3	Mobile Switching Center	5
2.4	Authentication	5
2.5	GSM Encryption	6
2.6	Weaknesses	7
3	UMTS (Universal Mobile Telecommunications System)	9
3.1	Authentication	9
3.2	Inter-operation with GSM	11
4	IMSI Catcher	13
4.1	GSM	13
4.1.1	Modes of Operation	13
4.2	UMTS	15
4.3	Drawbacks	16
4.4	Legal Foundation	17
5	Conclusion	19

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 4 of 28

1 Introduction

On July 29, 2005, Osman Hussain was arrested in an apartment in Rome, suspected of having placed a bomb on July 21 in a London tube station. The British Police had provided the Italian counterparts with two mobile numbers linked to him. Within 48 hours, his location was found by tracking and tapping his mobile phone ([BBC05]).

A statistic of the German Federal Network Agency shows, that this example is not an individual case (see Figure 1.1). While the landline phone monitoring stays nearly constant, there is a strong upward trend concerning the mobile phone monitoring. Alone in 2006, there have been over 35.000 orders imposed by law.

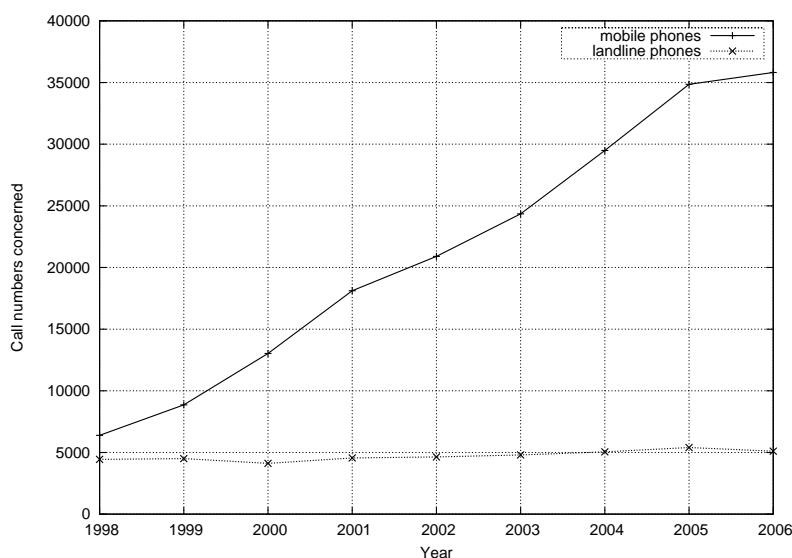


Figure 1.1: Statistics of the judicial monitoring measures of telecommunications in Germany ([BUN07])

The fact is, that tracking and tapping a mobile phone in the GSM network is not a difficult task. The operators of the telecommunication networks are obligated to permit a monitoring for the entitled authorities. Another method, and actually the more interesting one, is the assignment of an IMSI Catcher. The IMSI Catcher is an expensive device to identify, track and tap a mobile phone user in such a way, that even the network operator cannot notice anything.

In this paper, we will discuss the proceeding of this device and the necessary conditions in detail (see Chapter 4). Chapters 2 and 3 will obtain the background knowledge of the network standards GSM and UMTS, which we will need for comprehension. The conclusion is given in Chapter 5.

2 GSM (Global System for Mobile Communications)

GSM is the most common standard for mobile communication. It is used in more than 200 countries and territories all over the world. The architecture can be illustrated as a hierachic system of mainly 4 different network components (see Figure 2.1), which are

- Mobile Stations (**MS**),
- Base Stations (**BS**),
- Base Station Controllers (**BSC**) and
- Mobile Switching Centers (**MSC**).

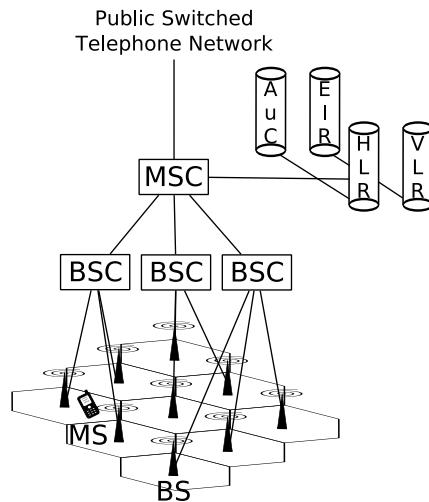


Figure 2.1: Simplified architecture of a GSM network

In the following we will discuss the functions of these components and the communication between them, to figure out the points of weaknesses in GSM.

2.1 Mobile Station

A Mobile Station can be seen as a mobile phone with a Subscriber Identification Module (**SIM**), a removable smart card. Every mobile phone has a unique 15-digit serial number, called International Mobile Equipment Identity (**IMEI**). In practice, this can be used to prevent stolen phones from accessing a network.

The identification of the subscriber is effected with the help of the SIM. It contains the International Mobile Subscriber Identity (**IMSI**), which is also a 15-digit number, concatenated of

1. the mobile country code (**MCC**): 3 digits,
2. the mobile network code (**MNC**): 2 or 3 digits and
3. the mobile subscriber identification number (**MSIN**): maximum 10 digits.

Furthermore, two algorithms are implemented on the SIM:

- The authentication algorithm A3 and
- the key generation algorithm A8.

For both algorithms, a 128 bit secret key K_i is needed that is also stored on the SIM.

2.2 Base Station and Base Station Controller

The wireless connection of a Mobile Station and a Mobile Switching Center is realized by a Base Station¹. Therefore, the area is divided into several cellular networks with one Base Station for each cell. The size of the cell depends basically on the geographic features of the area and consequently on the range of the stations. But also the number of possible calls, that have to be handled simultaneously, has to be considered, since it is limited by the number of available channels. Hence, in densely populated areas, the cells often have a diameter of only a few hundred meters, whereas in sparsely populated areas several kilometers are usual.

In subway stations or large buildings *Relais Stations* are installed to ensure high connectivity. These Relais Stations act like a Repeater in wired networks. They simply amplify and relay incoming signals to the nearest Base Station.

However, Base Stations are not only responsible for the connectivity. They are also needed for encryption and decryption of communication data.

As the name implies, on the next higher level the Base Station Controller manages the collaboration of the Base Stations and induces power controlling if

¹A Base Station is also referred to as Base Transceiver Station, Radio Base Station or Node B.

necessary. If a Mobile Station moves from one cell to another during a call, the Base Station Controller accomplishes a *handoff*². The connection is transferred to the second Base Station to avoid a termination of the call. The assumption is, that both Base Stations are linked with the same Base Station Controller. Otherwise the handoff has to be managed by the Mobile Switching Center.

2.3 Mobile Switching Center

The Mobile Switching Center has the role of a mobility management. It is responsible for the authentication, routing, handoffs over different Base Station Controllers, connection to the landline, etc.. For this purpose, there are 4 data bases available ([SCH06]):

- Home Location Register (**HLR**): There is only one HLR in one GSM network, which stores personal informations of the subscriber, e.g. the IMSI, the phone number³ or the GSM services.
- Visitor Location Register (**VLR**): Every MSC has its own VLR. It holds dynamic informations of the subscribers that are under the jurisdiction of the respective MSC. The informations are mostly copies of the personal informations, stored in the HLR.
- Authentication Center (**AuC**): The AuC holds the access data of every subscriber, particularly the secret key K_i of the SIM.
- Equipment Identity Register (**EIR**): As already mentioned, it is possible to prevent mobile phones from accessing the network. To realize this, the IMEI numbers of banned or stolen phones are kept in the EIR.

2.4 Authentication

If a Mobile Station wants to access a network, a challenge-response protocol is used to authenticate the subscriber (see Figure 2.2). After sending the security capabilities (see also Section 2.5), the Mobile Station is induced to transmit its IMSI to the VLR. The VLR forwards the IMSI to the HLR and receives a 128 bit random number $RAND$, a 32 bit signed response $SRES$ and a session key K_c . Only $RAND$ is passed to the mobile station. Together with the secret key K_i , these are the two inputs of the authentication algorithm A3. As output, the signed response $SRES'$ is generated, which is returned to the VLR. If $SRES$ and $SRES'$ match, the authentication request will be accepted, otherwise it will be discarded.

²In Britain, the term *handover* is more common.

³Also called Mobile Subscriber ISDN number (MSISDN).

As a security measure, the VLR assigns a Temporary Mobile Subscriber Identity (**TMSI**) to the Mobile Station to reduce the frequent transmission of the IMSI. This helps to avoid being identified or tracked. In further sessions, this TMSI can be used as identity response.

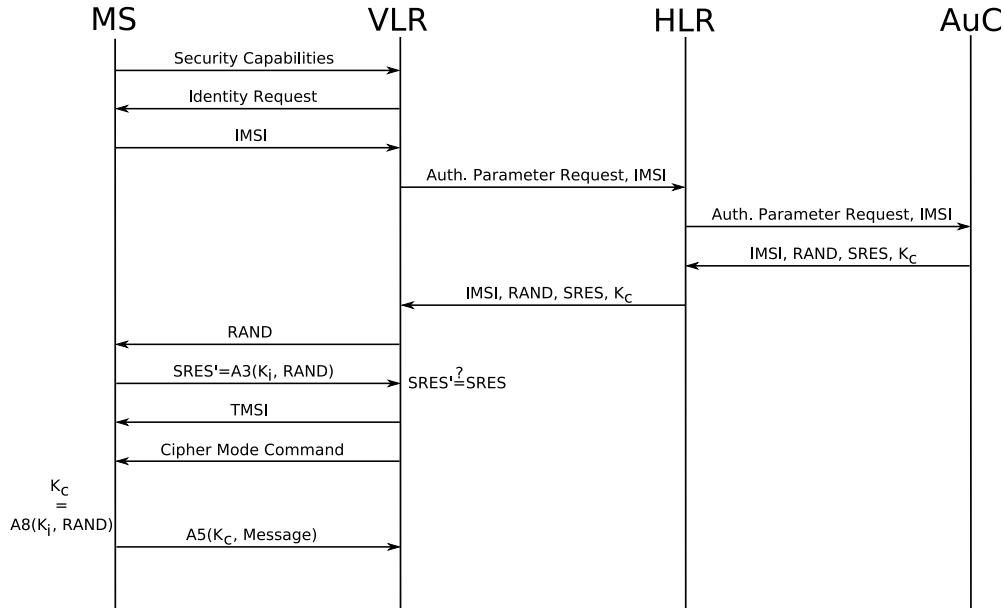


Figure 2.2: Authentication and encryption in GSM

2.5 GSM Encryption

To provide communication privacy, the stream cipher A5 is implemented on every mobile phone. It is a combination of three (A5/1) or four (A5/2) linear feedback shift registers (LFSRs) which encrypts and decrypts the communication data, if needed. The session key K_c , used in this algorithm, is generated by the algorithm A8 on the SIM with the input $RAND$. In this case, $RAND$ is the same random number as it is used in the authentication process. As an alternative, A5/0 encloses no encryption at all.⁴

In the security capabilities, the Mobile Station specifies, which encryption algorithms are supported. The Base Station chooses one of these and informs the Mobile Station with the cipher mode command.

⁴A5/1 is mostly used in Europe. An exception is France, where the encryption is disabled. This is why A5/0 is also called 'French mode' ([SPY05]).

2.6 Weaknesses

GSM has a few weaknesses, but regarding to the use of an IMSI Catcher, we will focus in Chapter 4 on point 1.

1. The authentication process considers only a one-sided authentication. The Mobile Station has to prove, that it is permitted to access the network, but there is no verification of the Base Station.
2. *Security by obscurity*: Since the beginning of GSM, the algorithms A3, A8 and A5 have not been published and always kept secret. But with the help of reverse engineering a number of serious weaknesses have been identified. In April 1998, Ian Goldberg and David Wagner released an article about cloning a GSM SIM ([ISA98]) and in April 2000, Alex Biryukov, Adi Shamir and David Wagner presented a paper about real time cryptanalysis of A5/1 on a PC ([BSW01]). The successor A5/2 is even more insecure and is not used as standard any more.
3. The encryption is only applied for the wireless transmission. That means, every communication is sent in plain text from the Base Station to the gateways.
4. For technical reasons, it is necessary for a Mobile Station to transmit the current location in short periods to the Base Station. This can be abused to track and record the movement profile of a subscriber.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 12 of 28

3 UMTS (Universal Mobile Telecommunications System)

UMTS is a mobile phone standard of the third generation (3G) and is a successor of GSM. It is characterized by a significant faster data transfer rate and a richer range of services compared to GSM. Built on the security of GSM, the following features have been added:

- Mutual entity authentication between Mobile Station and the Home Environment, the equivalent to MSC/HLR,
- a sequence number generator to guarantee freshness in the authentication process,
- integrity, using a MAC for the authentication process,
- A5/3, also known as *Kasumi*, a block cipher with a key size of 128 bits (for further details, see also [3GP01]).

3.1 Authentication

The authentication in UMTS is more complicated than in GSM. A secret key K is shared by the Universal Subscriber Identity Module (**USIM**) and the Home Environment (**HE**). Instead of A3 and A8,

- the authentication functions f_1 , f_2 and
- the key generating functions f_3 , f_4 , f_5

are used as follows (see also Figure 3.1):

The Home Environment

1. generates a sequence number SQN and a 128 bit random number $RAND$,
2. computes
 - a) $MAC = f_1(K, (SQN||RAND||AMF))$, with the authentication management field AMF ,
 - b) the expected user response $XRES = f_2(K, RAND)$,

- c) cipher key $CK = f3(K, RAND)$,
 - d) integrity key $IK = f4(K, RAND)$,
 - e) anonymity key $AK = f5(K, RAND)$,
 - f) authentication token $AUTN = SQN \oplus AK || AMF || MAC$,
 - g) $AV = RAND || XRES || CK || IK || AUTN$ and
3. sends the authentication vector AV to the Service Network (**SN**), the equivalent to MSC/VLR.

If the Mobile Station sends its request, the Service Network responses with $RAND$ and $AUTN$.

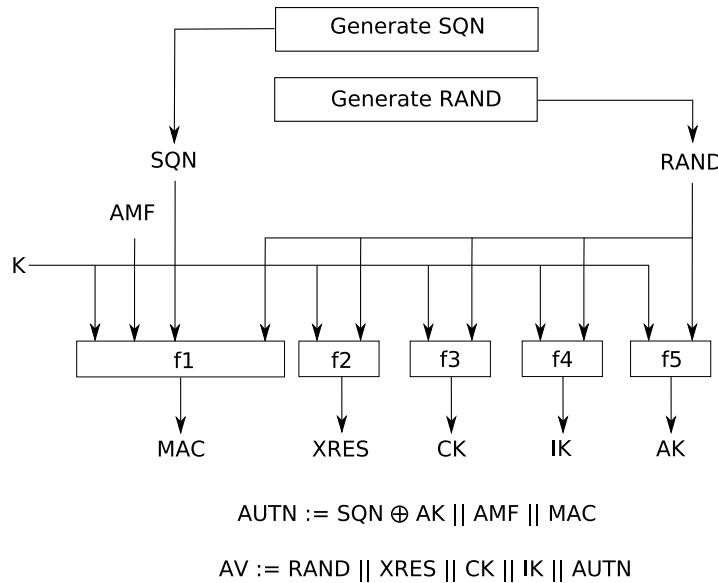


Figure 3.1: Generation of an authentication vector ([3GP99])

On the other side, the user proceeds as shown in Figure 3.2.
The USIM

1. computes
 - a) $AK = f5(K, RAND)$,
 - b) $SQN = (SQN \oplus AK) \oplus AK$,
 - c) $MAC' = f1(K, (SQN || RAND || AMF))$
2. checks if
 - a) $MAC' = MAC$,
 - b) SQN is valid,

3. computes

- a) $RES = f2(K, RAND)$,
- b) $CK = f3(K, RAND)$,
- c) $IK = f4(K, RAND)$ and

4. sends RES to the Service Network.

The Service Network checks if $RES = XRES$. If one of these comparison fails, a new authentication vector is generated.

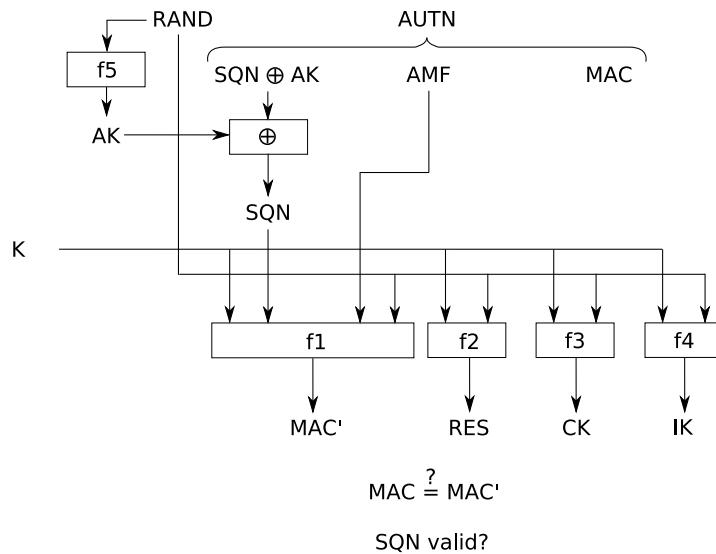


Figure 3.2: User authentication function in the USIM ([3GP99])

3.2 Inter-operation with GSM

To provide a high network coverage, the UMTS standard allows for inter-operation with GSM ([MEY04]). Therefore, not only UMTS, but also GSM Base Stations are connected to the Service Network. These GSM Base Stations neither support integrity protection nor the UMTS encryption algorithms. However, to guarantee mutual authentication, the authentication data generated by the Home Environment and Mobile Station are simply passed through. Only the cipher mode is chosen by the Base Station. The session key K_c that is needed for the GSM encryption, is computed from the integrity key IK and the cipher key CK as follows ([WET04]):

1. Split the 128 bit keys IK and CK into 64 bit keys, such that

$$IK = IK_1 || IK_2 \text{ and } CK = CK_1 || CK_2$$

2. Compute $K_c = CK_1 \oplus CK_2 \oplus IK_1 \oplus IK_2$

Figure 3.3 shows the UMTS authentication protocol with a GSM Base Station. That this inter-operation does not only brings advantages, can be seen in Section 4.2.

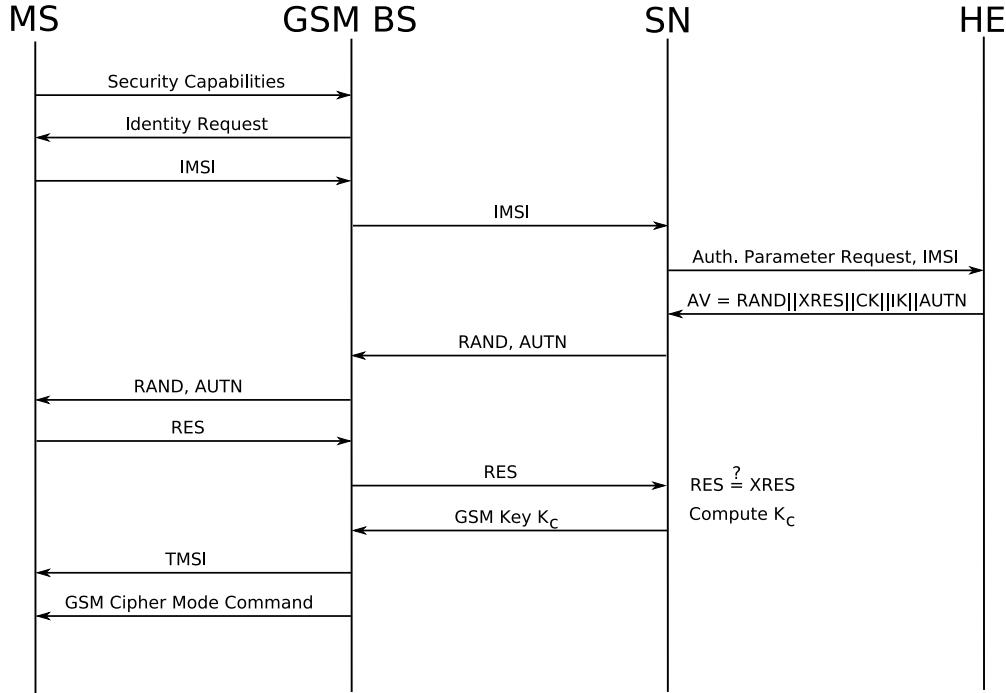


Figure 3.3: Authentication in UMTS with GSM Base Station

4 IMSI Catcher

In 1996, the German company *Rohde & Schwarz* presented the first IMSI Catcher GA 090 in Munich. The idea of an IMSI Catcher was originally to identify a subscriber by forcing to transmit the IMSI. With the help of the network operator, it is possible to determine the associated phone number. In 1997, the successor GA 900 allows the owner not only to identify, but also to tap outgoing phone calls.

4.1 GSM

4.1.1 Modes of Operation

In GSM, both devices take advantage of the one-sided authentication. As already mentioned, it is not necessary to authenticate a Base Station to a Mobile Station. An IMSI Catcher exploits this weakness and masquerades to a Mobile Station as a Base Station. With a signal strength up to 25 watt, it can theoretically supply a radius of several kilometers¹. Additionally, the GA 900 in combination with an own SIM, has the functionality to act like a Mobile Station and to perform a man-in-the-middle attack. Figure 4.1 shows the modified GSM protocol.

Identifying an IMSI

Every mobile phone has the requirement to optimize the reception. If there are more than one Base Station of the subscribed network operator accessible, it will always choose the one, with the strongest signal. An IMSI Catcher masquerades as a Base Station and causes every mobile phone of the simulated network operator within a defined radius to log in. With the help of a special identity request, it is able to force the transmission of the IMSI, instead of a TMSI. A similar procedure can be used to identify the IMEI.

Tapping a Mobile Phone

Figure 4.1 shows the functionality as communications intercept station of the GA 900. In this case, the IMSI Catcher, which acts as a Base Station, behaves

¹Compared to 50 watt of a Base Station.

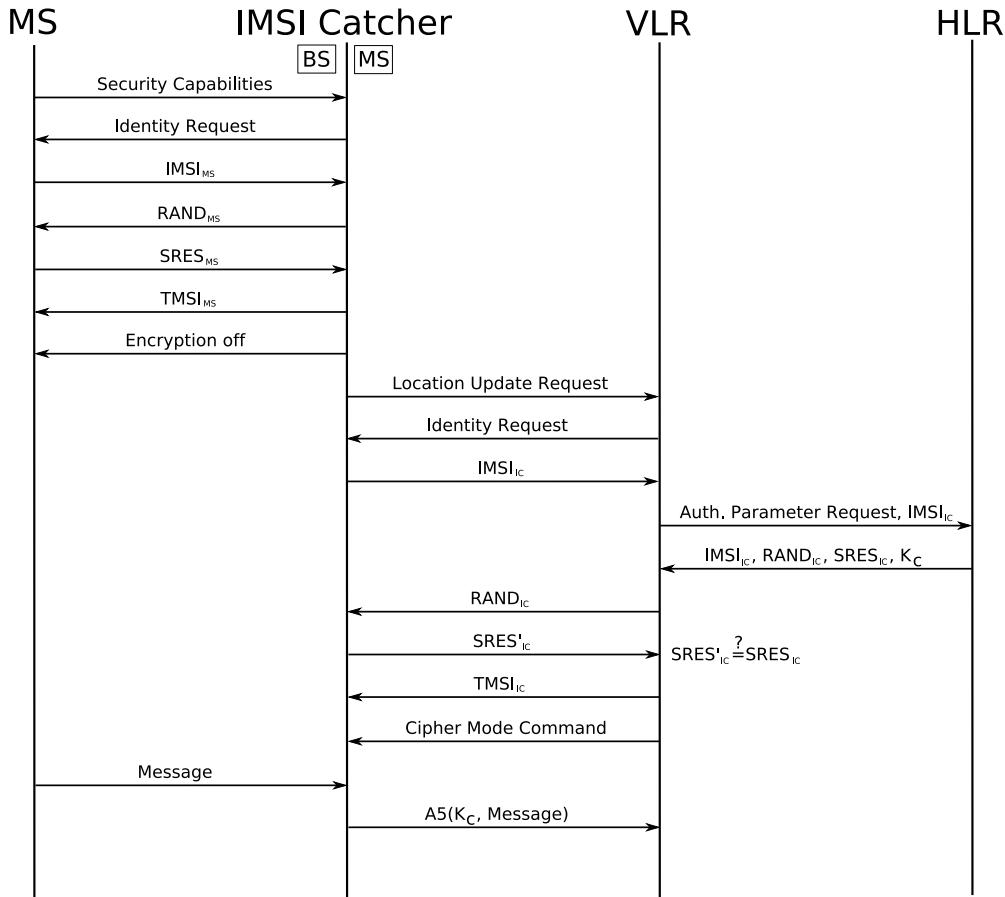


Figure 4.1: Man-in-the-middle attack with an IMSI Catcher

simultaneously like a Mobile Station to the real Base Station. After the authentication process, it uses the fact, that the encryption can simply be disabled from the Base Station. Hence, it can encrypt the plain text traffic from the Mobile Station and pass it to the Base Station.

Since the IMSI Catcher establishes a regular connection with a SIM, it is not possible to tap more than one phone call at the same time. It should be also clear, why incoming phone calls cannot be patched through. The subscriber has no direct connection to the network operator. Hence, he is not approachable for incoming calls.

A man-in-the-middle attack without a SIM may also be possible ([FOX02]). Then, in the authentication process, the IMSI Catcher simply passes the authentication data from the Mobile Station to the Base Station and the other way around. But in this scenario, the the encryption to both sides has to be disabled, since the attacker is not in the possession of the session key K_c . On the one side,

it can be realized by sending the cipher mode command A5/0 to the Mobile Station, but the problem is to induce the no-encryption mode to the Base Station. Sending only A5/0 in the security capabilities will probably not succeed, due to the security standard of GSM. Hence, to establish a regular connection with a SIM may be less complicated.

Position Fixing

As one can imagine, an IMSI Catcher is not able to localize a Mobile Station. There is only the functionality to verify the presence in a defined area. Localization or tracking can be realized by the network operator. Due to the permanent location update process with the Base Station, the Mobile Station reveals the GSM cell, it is currently located at. This may be, depending on the size of the cell, a radius of a few hundred meters to several kilometers. In addition, signal strength or signal propagation delay can be used to rise the accuracy. Hence, in combination with an IMSI Catcher, the localization can be improved enormously.

4.2 UMTS

Since UMTS uses mutual entity authentication, the man-in-the-middle attack as seen on GSM is not successful. The IMSI Catcher is not in the possession of the secret key K and hence, cannot generate the authentication vector AV . For the same reason, the identification of the IMSI cannot be realized in this way.

However, in 2005, Ulrike Meyer and Susanne Wetzel described an attack that exploits the inter-operation with GSM ([MEY04]). It is also a man-in-the-middle attack, but executed in three phases:

1. The IMSI or a valid TMSI of the victim has to be found out. This is easy, since it is sent in the beginning of an authentication process.
2. The impersonation as the victim to the Server Network. The attacker sends the IMSI to the Server Network and waits, until the random number $RAND$ and the authentication token $AUTN$ is returned, before he disconnects (see Figure 4.2). The combination $RAND$ and $AUTN$ is saved for the later use.
3. The IMSI Catcher masquerades as a GSM Base Station and the $RAND$ and $AUTN$ is sent to the victim. When there is not too much time elapsed since the second phase, the token is fresh and is accepted by the Mobile Station. The attacker cannot verify the response RES , which is not important, and gives the GSM cipher mode command A5/0 to the Mobile Station (Figure 4.3).

To forward the communication data, a regular connection is needed, since it is not possible to impersonate the victim to the Server Network at the same time. Hence, the attacker has to possess an own USIM to connect to the network.

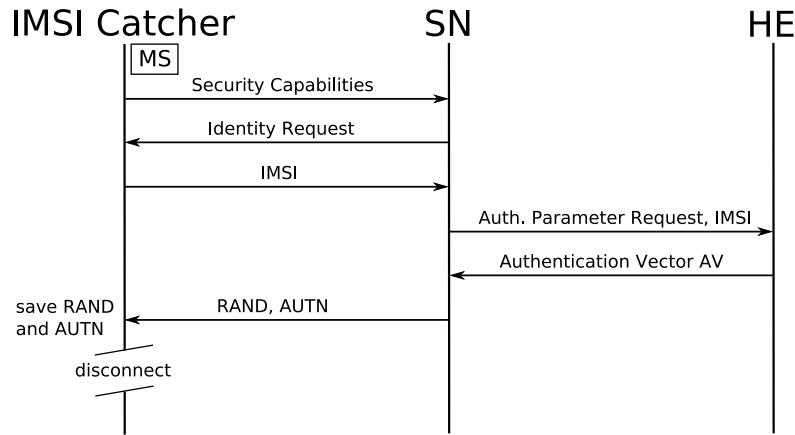


Figure 4.2: Attacker obtains currently valid authentication token ([MEY04])

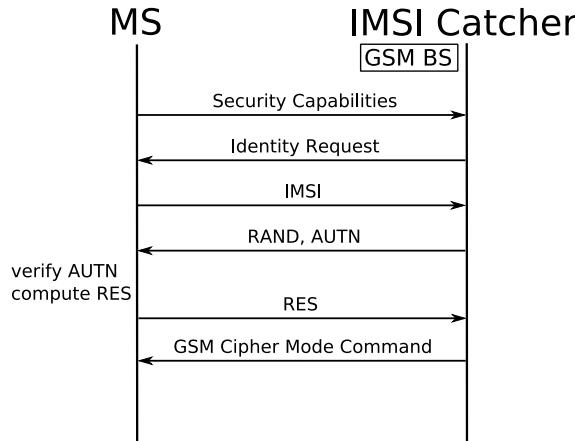


Figure 4.3: Authentication of the attacker as a GSM Base Station ([MEY04])

4.3 Drawbacks

The assignment of an IMSI Catcher has a number of drawbacks:

- It must be ensured, that the mobile phone of the observed person is in standby mode and the correct network operator is found out. Otherwise, for the Mobile Station, there is no need to log into the simulated Base Station.
- Depending on the signal strength of the IMSI Catcher, numerous IMSIs can be located. The Problem is to find out the right one.
- All mobile phones in the catchment area have no access to the network. Incoming and outgoing calls cannot be patched through for these subscribers.

Only the observed person has an indirect connection.

- There are some disclosing factors. In most cases, the operation cannot be recognized immediately by the subscriber. But there are a few mobile phones that show a small symbol on the display, e.g. an exclamation point, if encryption is not used. Another point is the calling number. Since the network access is handled with the SIM/USIM of the IMSI Catcher, the receiver cannot see the number of the calling party. Of course, this also implicates that the tapped calls are not listed in the itemized bill.
- The assignment near the Base Station can be difficult, due to the high signal level of the original Base Station.

4.4 Legal Foundation

Since September 11, 2001, also in Germany largest efforts to prevent terroristic attacks have been launched. One consequence is the increased non-disputable assignment of the IMSI Catcher. In August 14, 2002, §100i was introduced, which allows the police in an urgent suspicion to identify the IMSI and the IMEI with technical devices. What has been illegally accomplished before ([HEI01]), is now legal, on the optimistic assumption of the Federal Ministry of the Interior that a restriction of the mobile phones in the catchment area takes only 10 seconds ([BUN02]).

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 22 of 28

5 Conclusion

The one-sided authentication of GSM is a serious weak point, which is exploited by the IMSI Catcher. After identifying the IMSI and IMEI with a masquerade attack, outgoing calls can be tapped with a man-in-the-middle attack.

In many articles, the authors assume, due to the launch of UMTS, that the IMSI Catcher will not play a large role in the future. But GSM had a strong development in the whole world in the last years and at the beginning of 2006 over 1.7 billion subscribers. The change-over to UMTS will last for a long time, above all, because one needs a special UMTS supporting mobile phone. In addition, the UMTS coverage is moderate. Hence, the inter-operation with GSM will probably remain, so that a man-in-the-middle attack will be still possible.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 24 of 28

List of Figures

1.1	Statistics of the judicial monitoring measures of telecommunications in Germany ([BUN07])	1
2.1	Simplified architecture of a GSM network	3
2.2	Authentication and encryption in GSM	6
3.1	Generation of an authentication vector ([3GP99])	10
3.2	User authentication function in the USIM ([3GP99])	11
3.3	Authentication in UMTS with GSM Base Station	12
4.1	Man-in-the-middle attack with an IMSI Catcher	14
4.2	Attacker obtains currently valid authentication token ([MEY04]) . .	16
4.3	Authentication of the attacker as a GSM Base Station ([MEY04])	16

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 26 of 28

Bibliography

- [3GP99] 3GPP: *Authentication management field ver2*, URL: http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_06_9910/docs/s3-99348,%20CR33102-017%20authentication%20management%20field%20ver2.rtf, 1999.
- [3GP01] 3GPP: *3GPP TS 35.202 V3.1.1*, URL: <http://www.3gpp.org/TB/other/algorithms/35202-311.pdf>, 2001.
- [BBC05] BBC UK: *Tracking a suspect by mobile phone*, URL: <http://news.bbc.co.uk/2/low/technology/4738219.stm>, 2005.
- [BSW01] ALEX Biryukov, ADI SHAMIR AND DAVID WAGNER: *Real Time Cryptanalysis of (A5/1) on a (PC)*, Lecture Notes in Computer Science, Vol. 1978, URL: <http://www isaac.cs berkeley.edu isaac gsm press html>, 2001.
- [BUN07] BUNDESNETZAGENTUR: *Statistik der strafprozessualen Überwachungsmaßnahmen der Telekommunikation*, URL: <http://www.bundesnetzagentur.de/media/archive/9710.pdf>, 2007.
- [BUN02] BUNDESREGIERUNG: *Rechtliche Zulässigkeit von so genannten IMSI-Catchern*, Bundestag printed paper 14/6885, URL: <http://dip.bundestag.de/btd/14/068/1406885.pdf>, 09/10/2001.
- [FOX02] DIRK FOX: *Der IMSI-Catcher*, Datenschutz und Datensicherheit 26, 2002.
- [HEI01] HEISE: *Polizei mit IMSI-Catcher auf Lauschangriff*, URL: <http://www.heise.de/newsticker/meldung/20094>, 08/11/2001.
- [ISA98] ISAAC: *Smartcard Developer Association Clones Digital GSM Cellphones*, URL: <http://www isaac cs berkeley edu isaac gsm press html>, 1998.
- [MEY04] ULRIKE MEYER AND SUSANNE WETZEL: *A Man-in-the-Middle Attack on UMTS*, URL: <http://www.cs.stevens.edu/swetzelt/publications/mim.pdf>, 2005.

- [SCH06] JÖRG SCHWENK: *Mobilfunk: Systembersicht, Systemsicherheit, Teil 3: Mobilfunk*, URL: http://www.nds.rub.de/lehre/vorlesungen/systemsicherheit/Systemsicherheit_3_Mobilfunk_v05.pdf, 2006.
- [SPY05] SPYWORLD: *Interception of GSM Cell-phones*, URL: http://www.spyworld-actu.com/IMG/_article_PDF/article_288.pdf, 2005.
- [WET04] ULRIKE MEYER AND SUSANNE WETZEL: *On the impact of GSM Encryption and Man-in-the-Middle Attacks on the Security of Interoperating GSM/UMTS Networks*, Proceedings of IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC2004), IEEE, 2004.

Harvard Journal of Law & Technology
Volume 28, Number 1 Fall 2014

**YOUR SECRET STINGRAY'S NO SECRET ANYMORE: THE
VANISHING GOVERNMENT MONOPOLY OVER CELL PHONE
SURVEILLANCE AND ITS IMPACT ON NATIONAL SECURITY
AND CONSUMER PRIVACY**

*Stephanie K. Pell & Christopher Soghoian**

TABLE OF CONTENTS

TABLE OF CONTENTS.....	1
I. INTRODUCTION	2
II. AN INTRODUCTION TO CELL PHONE SURVEILLANCE TECHNOLOGY.....	8
A. <i>An Approximate History of Cellular Phone Surveillance Technology</i>	13
B. <i>Uses of Direct Surveillance Technology</i>	16
III. "KNOWN KNOWNS": CASE LAW AND DOJ GUIDANCE.....	19
A. <i>The 1995 Digital Analyzer Magistrate Opinion</i>	20
B. <i>The 1997 DOJ Guidance</i>	23
C. <i>The 2001 USA PATRIOT Act Amendments to Pen/Trap Statute and Guidance in the 2005 Electronic Surveillance Manual</i>	26
D. <i>2012 Cell Site Simulator ("StingRay") Magistrate Opinion</i>	27
E. <i>The Rigmaiden Federal Prosecution</i>	29
IV. THE GOVERNMENT'S SECRET STRINGRAY	34
A. <i>Lack of Disclosure to the Courts</i>	35
B. <i>Secrecy via Regulatory Restrictions and Non-Disclosure</i>	

* Pell is an Assistant Professor & Cyber Ethics Fellow at West Point's Army Cyber Institute and an Affiliate Scholar at Stanford's Center for Internet & Society. She is a former Counsel to the House Judiciary Committee and has held several positions in the Department of Justice, including Senior Counsel to the Deputy Attorney General and Assistant U.S. Attorney in the Southern District of Florida.

Soghoian is the Principal Technologist with the Speech, Privacy, and Technology Project at the American Civil Liberties Union and a Visiting Fellow with the Information Society Project at Yale Law School. The opinions expressed in this Article are the authors' alone and do not reflect the official position of their respective employers or any part of the United States Government.

The authors wish to thank Matt Blaze, Ian Brown, Alan Butler, Susan Freiwald, Allan Friedman, Jean-Pierre Hubaux, Eric King, Susan Landau, Linda Lye, Aaron K. Martin, Valtteri Niemi, Karsten Nohl, Brian Owsley, Christopher Parsons, Christopher Prince, John Scott-Railton, Greg Rose, Seth Schoen, Jennifer Valentino-DeVries, David Wagner, Nicholas Weaver, several individuals who have asked to remain anonymous, and the attendees of their session at the 2013 Privacy Law Scholars Conference.

<i>Agreements</i>	37
<i>C. Federal FOIA and State Public Records Act Responses</i>	39
V. A SECRET NO MORE	40
<i>A. The Globalization of Cellular Interception Technology</i>	41
<i>B. The Democratization of Cellular Interception Technology</i>	46
1. Low Cost Software-Defined Radio-Based Active Interception	47
2. Lower Cost Active Interception with Femtocells.....	49
3. Advances in Passive Interception.....	50
VI. OUR VULNERABLE CELLULAR NETWORKS CAN BE AND ARE EXPLOITED BY OTHERS	55
<i>A. Foreign Governments</i>	55
<i>B. Non-Government Use of Cellular Surveillance Technology</i>	57
VII. A HIGH PRICE TO PAY FOR THE FICTION OF SECRECY	59
VIII. FOCUSING ON CYBERSECURITY	63
IX. PROTECTING OUR COMMUNICATIONS	67
<i>A. Securing Cellular Networks</i>	68
<i>B. “Over-the-Top” Secure Communication Apps</i>	71
<i>C. Counter-Surveillance Technology</i>	73
X. CONCLUSION.....	75

I. INTRODUCTION

“... [T]HOU WILT NOT TRUST THE AIR WITH SECRETS.” —
SHAKESPEARE, TITUS ANDRONICUS¹

During a 1993 congressional oversight hearing on the integrity of telephone networks,² security researcher Tsutomu Shimomura used a “software hack” to turn an analog cellular phone into a scanner that enabled all present in the hearing room to hear the live conversations of nearby cellular phone users.³ Shimomura had been granted immunity to perform this demonstration under the watchful gaze of a nearby

1. WILLIAM SHAKESPEARE, TITUS ANDRONICUS, act 4, sc. 2.

2. *Telecommunications Network Security: Hearing Before the Subcomm. on Telecomm. & Fin. of the H. Comm. on Energy & Commerce*, 103d Cong. 1 (1993) [hereinafter *Telecommunications Network Security Hearing*] (statement of Rep. Markey, Chairman, Subcomm. on Telecomm. & Fin. of the H. Comm. on Energy & Commerce).

3. *Id.* at 8–9.

agent from the Federal Bureau of Investigation (“FBI”).⁴ The event was a practical demonstration of what Subcommittee Chairman Ed Markey called “the sinister side of cyberspace.”⁵

The demonstration illustrated a significant security vulnerability impacting then-widely used analog cellular phone networks: calls were not encrypted as they were transmitted over the air and could, therefore, be intercepted with readily available equipment,⁶ such as an off-the-shelf radio scanner or a modified cellular phone.

Although the threat demonstrated by Shimomura was clear, Congress and the Federal Communications Commission (“FCC”) took no steps to mandate improvements in the security of analog cellular calls.⁷ Such a technical fix would have required wireless carriers to upgrade their networks to support more secure telephone technology, likely at significant cost.⁸ Instead, Congress outlawed the sale of new radio scanners capable of intercepting cellular signals and forced scanner manufacturers to add features to their products to prevent them from being tuned to frequencies used by analog cell phones.⁹

4. See *Immunity Needed; Markey Panel Sees Dark Side of Electronic Frontier*, COMM. DAILY (Apr. 30, 1993), available at <https://w2.eff.org/Privacy/Newin/Cypherpunks/930430.communications.daily>.

5. *Telecommunications Network Security Hearing*, *supra* note 2, at 1 (statement of Rep. Markey, Chairman, Subcomm. on Telecomms. & Fin. of the H. Comm. on Energy & Commerce).

6. See Simson L. Garfinkel, *Understanding Cellular Telephone Security and Privacy*, SIMSON.NET (2007), http://simson.net/ref/security_cellphones.htm (“[Analog cell phones] were the first cellular telephones. Developed in the 1970s and deployed in the 1980s . . . [t]hese phones transmit voice as an analog signal without any encryption or scrambling.”).

7. See *Telecommunications Network Security Hearing*, *supra* note 2, at 9 (statement of Rep. Markey, Chairman, Subcomm. on Telecomms. & Fin. of the H. Comm. on Energy & Commerce) (“[L]ast year we passed legislation to ban scanners, but we clearly did not ban cellular phones. However, cellular phones can be reprogrammed as a scanner with a relatively rudimentary knowledge of the technology. Tens of thousands of people know how to do it.”). In a submission to the FCC, the cellular industry association opposed proposals for the FCC to focus on the cellular interception vulnerabilities rather than the availability of radio scanners capable of intercepting cellular phone calls. See FED. COMM’NS COMM’N, REPLY COMMENTS OF THE CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION ON AMENDMENT OF PARTS 2 AND 15 TO PROHIBIT MARKETING OF RADIO SCANNERS CAPABLE OF INTERCEPTING CELLULAR TELEPHONE CONVERSATIONS 4 (1993) [hereinafter CTIA REPLY COMMENTS], available at <http://apps.fcc.gov/ecfs/document/view;jsesionid=fTGkSn3c0CsJjGhv2tsDQQktvyhfXkHpW2JPnr9pPhxQ9sC88Cp!-1864380355!1357496456?id=1120040001> (“Rather than proposing to strengthen the Commission’s proposed rules, however, these parties would have the Commission weaken or abandon its proposals and place the [privacy] burden solely on cellular carriers or manufacturers . . . With the enactment of Section 403(a), the time for such an argument is past.”).

8. See Craig Timberg & Ashkan Soltani, *By Cracking Cellphone Code, NSA Has Ability To Decode Private Conversations*, WASH. POST (Dec. 13, 2013), http://www.washingtonpost.com/business/technology/2013/12/13/e119b598-612f-11e3-bf45-61f69f54fc5f_story.html (“Upgrading an entire network to better encryption provides substantially more privacy for users . . . But upgrading entire networks is an expensive, time-consuming undertaking . . .”); Babbage, *infra* note 271. Such network upgrades would also have neutralized analog interception devices, which were then used by U.S. government agencies.

9. See FED. COMM’NS COMM’N, REP. & ORD. FCC 93-201, AMENDMENT OF PARTS 2 AND 15 TO PROHIBIT MARKETING OF RADIO SCANNERS CAPABLE OF INTERCEPTING

This action by Congress, however, did nothing to prevent the potential use of millions of existing interception-capable radio scanners already in the homes and offices of Americans to intercept telephone calls.¹⁰

In 1997, four years after the FCC enacted congressionally mandated regulations banning the sale of scanning equipment capable of intercepting cellular signals,¹¹ a couple from Florida recorded a conference call between several senior Republican politicians, including then Speaker of the House Newt Gingrich, which they were able to intercept because one of the call's participants was using a cellular phone.¹² Although the couple did not intend to critique U.S. communications policy when they turned on their radio scanner, their act was high-profile proof that Congress' response to the analog interception threat was not successful.¹³ What ultimately fixed the analog phone interception problem was not further congressional action but, rather, the wireless industry's migration away from easily intercepted analog

CELLULAR TELEPHONE CONVERSATIONS (1993) [hereinafter FCC REPORT AND ORDER], available at <http://apps.fcc.gov/ecfs/document/view;jsessionid=CyspSn3R1KqpKlzc9pwb5GyypnrQ4nnGMqFqtNpQyFYbhWZ2r1c!1357496456!-1864380355?id=1145780001> (made in response to Sec. 403 of the Telephone Disclosure and Dispute Resolution Act, Pub. L. 102-556 (1992)) (codified as amended at § 47 U.S.C. 302a(d) (requiring that within 180 days of enactment, the FCC shall prescribe and make effective regulations denying equipment authorization)). However, as the FCC made clear in its report, this prohibition does not apply to companies that "market[] [analog cellular interception technology] to law enforcement agencies . . ." *Id.* at 7. Such a law enforcement exemption had been requested by the Harris Corporation, and supported by the cellular industry association. See CTIA REPLY COMMENTS, *supra* note 7, at 8 ("CTIA supports the Harris Corporation's request that the Commission modify its proposed rules to clarify that scanning receivers that receive cellular transmissions . . . may continue to be manufactured for sale to [law enforcement].").

10. See CTIA REPLY COMMENTS, *supra* note 7, at 3 (describing some commenters' concerns that "the Commission's proposed rules are flawed because they will not effectively safeguard the privacy of cellular calls" because "millions of scanning receivers capable of tuning cellular frequencies are already in use, and [] such receivers will remain available for sale for another year."); SUMMARY OF TESTIMONY OF THOMAS E. WHEELER, CELLULAR TELECOMM. INDUS. ASS'N: H. COMMERCE COMM., SUBCOMM. ON TELECOMMS., TRADE & CONSUMER PROT., 105th Cong. (1997) [hereinafter SUMMARY OF WHEELER TESTIMONY] (statement of Thomas E. Wheeler, Member, Cellular Telecomms. Indus. Ass'n) ("[T]rying to ban a specific type of eavesdropping gear after it has already become widely available is difficult.").

11. See FCC REPORT AND ORDER, *supra* note 9, at 1.

12. The participants of the call — who included Republican Majority Leader Dick Armey, Republican Whip Tom Delay, New York Congressman Bill Paxon, and Ohio Congressman John Boehner — were discussing an investigation of Gingrich by the Congressional Ethics Committee. The Florida couple gave the recording to the ranking Democratic member of the Ethics Committee (and thus the leader of the Gingrich investigation). See *The Gingrich Cellular Phone Call*, PBS NEWSHOUR (Jan. 14, 1997), http://www.pbs.org/newshour/bb/politics/jan-june97/cellular_01-14.html.

13. This was not the only opportunity in 1997 for Congress to observe that cellular communications were still not secure. See H.R. REP. NO. 105-425, at 5 (1998), available at <http://www.gpo.gov/fdsys/pkg/CRPT-105hrpt425/pdf/CRPT-105hrpt425.pdf> ("The Subcommittee on Telecommunications, Trade, and Consumer Protection held a hearing on cellular privacy on February 5, 1997 . . . Prior to the witnesses' testimony, a technological demonstration was conducted to highlight the ease with which scanning equipment can be 'readily altered' to intercept cellular communications.").

phone technology to digital cellular phones — a decision motivated in part by the increase in cellular phone cloning fraud.¹⁴ Digital phone conversations were, at the time, far less likely to be intercepted because the necessary equipment was prohibitively expensive and thus available to fewer potential snoops.¹⁵

Governments with significant financial resources, however, have owned and used cellular phone surveillance equipment for quite some time.¹⁶ Indeed, for nearly two decades, U.S. federal, state, and local law enforcement agencies have employed sophisticated cellular surveillance equipment that exploits vulnerabilities in cellular networks.¹⁷ Once only accessible to a few global powers at six-figure prices, similar technology is now available to any government — including those with a history of spying in the United States — and to any other interested buyer from surveillance companies around the world, often for as little as a few thousand dollars per device.¹⁸ Moreover, hobbyists can now build less advanced but functional interception equipment for as little as \$100.¹⁹ The normal course of economics and innovation has destroyed the monopoly a select group of global powers once enjoyed over digital cellular surveillance technology, rendering surreptitious access to cellular communications as universally available as it once was in the analog world. Surveillance has, once again, become democratized, this time with a much more expansive set of capabilities.

During congressional testimony in 1997, current FCC Chairman Tom Wheeler, then the president of the Cellular Telecommunications Industry Association (“CTIA”), warned the Committee of this outcome: “Unless Congress takes a forward-looking approach, history will likely repeat itself as digital scanners and decoders, though expensive now, drop in price in the future.”²⁰ Mr. Wheeler’s prescient warning has come true. Although the technology has changed, we are

14. Cell phone cloning is a process by which one phone’s unique account number can be captured and programmed into another phone for purposes of billing one phone’s calls to another phone. See Jeri Clausing, *Congress Moving Quickly To Try To Curb Cell Phone Abuses*, N.Y. TIMES (Mar. 2, 1998), <http://www.nytimes.com/1998/03/02/business/congress-moving-quickly-to-try-to-curb-cell-phone-abuses.html>.

15. See David Wagner et al., *Cryptanalysis of the Cellular Message Encryption Algorithm*, in ADVANCES IN CRYPTOLOGY — CRYPTO ’97, at 526, 526 (1997), available at <http://www.schneier.com/paper-cmea.pdf> (“[T]he latest digital cellphones currently offer some weak protection against casual eavesdroppers because digital technology is so new that inexpensive digital scanners have not yet become widely available . . .”); H.R. REP. NO. 105-425, *supra* note 13, at 3–4 (“While digital cellular and PCS are not immune from eavesdropping, they are currently more secure than analog cellular because the equipment for intercepting digital calls is vastly more expensive and complex than existing, off-the-shelf scanners that intercept analog communications (e.g., \$200 vs. \$10,000–\$30,000).”).

16. See *infra* Part V.A.

17. See *infra* Part III.

18. See *infra* Part V.

19. *Id.*

20. See SUMMARY OF WHEELER TESTIMONY, *supra* note 10.

rapidly approaching a future of widespread interception that feels like the past, but with a much larger range of public and private actors with more diverse motives for snooping. Whoever employs this technology can obtain direct, unmediated access to information about and from a cellular phone without any aid from a wireless provider.²¹ In some cases, this technology can even intercept the contents of cellular phone calls, text messages, and other communications data transmitted to and from the phone.²²

In this Article, we will argue that policymakers did not learn the right lesson from the analog cellular interception vulnerabilities of the 90s: That is, the communications of Americans will only be secured through the use of privacy-enhancing technologies like encryption, not with regulations prohibiting the use or sale of surveillance technology.

Nearly two decades after Congress passed legislation to protect analog phones from interception by radio scanners,²³ the American public is poised, quite unknowingly, at the threshold of a new era of communications interception that will be unprecedented in its pervasiveness and variety. Foreign governments, criminals, the tabloid press, and curious individuals with innumerable private motives can now leverage longstanding security vulnerabilities in our domestic cellular communications networks that were previously only exploitable by a few global powers.

In spite of the security threat posed by foreign government and criminal use of cellular surveillance technology, U.S. government agencies continue to treat practically everything about the technology as a closely guarded “source and method,” shrouding the technical capabilities, limitations, and even the name of the equipment they use from public disclosure.²⁴ The source and method argument is invoked to protect law enforcement agencies’ own use of cellular surveillance technology by preventing criminal suspects from learning how to evade monitoring and detection.²⁵ This secrecy is of questionable efficacy for that purpose, however, and it comes at a high collateral cost: For twenty years, the American public has been kept in the dark about

21. See John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA TODAY (Dec. 8, 2013), <http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/> (“The Sting[Ray] can grab some data from cellphones in real time and without going through the wireless service providers involved.”); *Active GSM Interceptor: IBIS II—In-Between Interception System—2nd Generation*, ABILITY COMPUTERS & SOFTWARE INDUS. LTD., <http://www.interceptors.com/intercept-solutions/Active-GSM-Interceptor.html> (last visited Dec. 18, 2014) [hereinafter *IBIS II*] (“The IBIS II is a stand-alone solution for off the air interrogation / interception / monitoring / deception of tactical GSM [(Global System for Mobile)] communication, in a seamless way, *without any cooperation with the network provider.*”) (emphasis added).

22. See *infra* Part II.

23. See FCC REPORT AND ORDER, *supra* note 9.

24. See *infra* Part IV.

25. See *infra* Parts III.E, IV.

cellular network vulnerabilities and is thus generally unaware of the need to secure their private communications. Indeed, even though cybersecurity threats are a top congressional priority, it is only over the past year that a few policymakers have publicly acknowledged the exploitable vulnerabilities latent in our cellular networks, largely due to efforts by the press, privacy advocates, and researchers. Moreover, to date, there has been no corresponding serious policy debate about how to secure private communications from those threats.

If the United States and its close allies had a monopoly over this technology, the law enforcement community could credibly argue that certain national security interests furthered by the use of the technology — and thus the need to maintain the secrecy of all related information — trump the need to inform the American public about the vulnerability of cellular communications. This Article, however, dispels the myth that this technology is, in fact, secret at all. Indeed, it has been the subject of front page stories in leading newspapers,²⁶ has been featured in Hollywood movies²⁷ and television dramas,²⁸ and, more ominously, can be purchased over the Internet²⁹ from one of many non-U.S. based surveillance technology vendors or even built at home by hobbyists.³⁰ We therefore argue that the risks to the American public arising from the U.S. government's continued suppression of public discussion about vulnerabilities in our cellular communications networks that can be exploited to perform unmediated surveillance outweigh the now-illusory benefits of attempting to keep details of the technology secret. Congress should address these network vulnerabilities and the direct surveillance techniques they enable, as well as the necessity for responsive privacy-enhancing technologies like strong encryption,³¹ as part of the larger cybersecurity debate, to

26. See Ellen Nakashima, *Little-Known Surveillance Tool Raises Concerns by Judges, Privacy Activists*, WASH. POST (Mar. 27, 2013), http://www.washingtonpost.com/world/national-security/little-known-surveillance-tool-raises-concerns-by-judges-privacy-activists/2013/03/27/8b60e906-9712-11e2-97cd-3d8c1afe4f0f_story.html; Jennifer Valentino-DeVries, "Stingray" Phone Tracker Fuels Constitutional Clash, WALL ST. J. (Sept. 22, 2011), <http://online.wsj.com/article/SB1000142405311904194604576583112723197574.html>.

27. See ZERO DARK THIRTY at 00:80:38 (Sony Pictures 2012).

28. See *The Wire: Middle Ground* at 00:12:57 (HBO television broadcast Dec. 12, 2004) (dialogue between two characters) ("Remember those analog units we used to use to pull cell numbers out of the air? . . . We used to have to follow the guy around, stay close while he used the phone." "New digitals . . . bing, we just pull the number right off the cell towers.").

29. See Letter from Rep. Alan M. Grayson to Tom Wheeler, Chairman, FCC (July 2, 2014), available at http://grayson.house.gov/images/pdf/rep_grayson_letter_to_federal.communications_commission_chairman.pdf (making reference to a Chinese online merchant and stating that "IMSI catchers can apparently 'be bought openly' from online retailers for as little as \$1800").

30. See *infra* Part V.B.

31. See LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND

which they are all inextricably linked. To date, however, this policy debate is not occurring, which is not beneficial either to privacy or cellular network security.

Part II of this Article begins by naming this “secret” surveillance technology and describing its capabilities. Part III goes on to address the limited Department of Justice (“DOJ”) guidance and case law pertaining to this technology. Part IV discusses what appears to be a concerted effort by the U.S. government to prevent the public disclosure of information about this technology. Part V reveals, however, that the existence of the technology is both publicly known and acknowledged by governments in other countries. Part VI describes how foreign governments and criminals can and do use cellular surveillance equipment to exploit the vulnerabilities in phone networks, putting the privacy and security of Americans’ communications at risk. Part VII argues that the public is paying a high price for the U.S. government’s perpetuation of a fictional secrecy surrounding cell phone surveillance technology. Specifically, such fictional claims of secrecy prevent policymakers from publicly addressing the threats to the security of cellular communications. Part VIII argues that cellular network vulnerabilities should be addressed publicly in the larger cybersecurity policy process Congress is currently undertaking. Finally, Part IX examines possible technical avenues through which solutions could come.

II. AN INTRODUCTION TO CELL PHONE SURVEILLANCE TECHNOLOGY

Because cellular telephones send signals through the air, cellular communications are inherently vulnerable to interception by many more parties than communications carried over a copper wire or fiber optic cable into a home or business.³² This increased exposure to interception exists because anyone wishing to tap a traditional *wireline* telephone call must physically access the network infrastructure transporting that call — such as by attaching interception equipment to the telephone wires outside the home of the target or at the telephone company’s central office.³³ In contrast, intercepting a cellular

COMMUNICATIONS TECHNOLOGIES 22 (2013), available at <http://www.lawfareblog.com/wp-content/uploads/2013/12/Final-Report-RG.pdf> (advising the U.S. government to “support[] efforts to encourage the greater use of encryption technology for data in transit, at rest, in the cloud, and in storage.”).

32. See Timberg & Soltani, *supra* note 8 (“Cellphone conversations long have been much easier to intercept than ones conducted on traditional telephones because the signals are broadcast through the air, making for easy collection.”).

33. See *id.* Carrier-assisted wiretaps once required that the interception take place near the target, such as at a call-switching center. Today, telephone carriers have modern interception equipment that permits intercepts to be remotely initiated and controlled by a single dedicated surveillance team within the companies. See, e.g., UTIMACO, LAWFUL

telephone call only requires sufficient geographic proximity to the handset of one of the callers and the right kind of wireless interception equipment.

Cellular telephone calls can, of course, be intercepted by government agencies with the assistance of the wireless carriers via government-mandated interception capabilities these companies have built into their networks.³⁴ In fact, the vast majority of surveillance performed by law enforcement agencies in the United States is, almost certainly, carrier-assisted surveillance.³⁵ But cellular phone transmissions can also be captured without the assistance, or even the knowledge, of the carriers. The unmediated nature of this kind of interception, combined with the growing ease of access to cellular surveillance technology, makes the universe of private parties that can intercept a cellular call inestimably larger, and the range of their motives correspondingly broader, than the pool of potential law enforcement and national security actors who have both the legal capacity and technical capability to initiate a traditional wiretap of a wireline phone.

The technologies that enable the direct interception of cellular phone calls without the assistance of a wireless carrier generally fall into two categories: *passive* and *active*.³⁶ The former merely intercepts the signals sent between nearby phones and the wireless provider's network, while the latter transmits data to, and directly interacts with, the cellular phones under surveillance.

Passive interception technology functions in two stages. First, the signals exchanged between a cellular phone and the wireless carrier's network are intercepted as they are transmitted over the air. This pro-

INTERCEPTION OF TELECOMMUNICATION SERVICES, *available at* <https://www.wikileaks.org/spyfiles/docs/UTIMACO-LIMSLawfInte-en.pdf> (last visited Dec. 18, 2014) ("Utimaco's [Lawful Interception Management System] . . . automate[s] the administrative and operative tasks related to lawful interception. The system is based on a central management platform for the surveillance of communication services and implements electronic interfaces to various authorized law enforcement agencies and their monitoring centers."); ELAMAN, COMMUNICATIONS MONITORING SOLUTIONS, *available at* https://www.wikileaks.org/spyfiles/files/0/188_201106-ISS-ELAMAN3.pdf (last visited Dec. 18, 2014) ("Lawful Interception provides access to calls and call-related information (telephone numbers, date, time, etc.) within telecommunications networks, and delivers this data to a strategic Monitoring Center (MC) Such an MC gives access to an entire country's telecommunications network from one central place, but it needs the support of operators").

34. See The Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. §§ 1001–1010 (2012)) (requiring certain types of communications networks to contain built-in wiretapping capabilities).

35. See Eric Lichtblau, *Wireless Firms Are Flooded by Requests To Aid Surveillance*, N.Y. TIMES, July 9, 2012, at A1, *available at* <http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html> (describing the 1.3 million requests the wireless carriers received in 2011 from law enforcement agencies).

36. See Karsten Nohl & Chris Paget, *GSM — SRSLY?*, 26TH CHAOS COMM. CONG. (26C3) (Dec. 27, 2009), http://events.ccc.de/congress/2009/Fahrplan/attachments/1519_26C3.Karsten.Nohl.GSM.pdf.

cess does not disrupt the signals in transit. Second, once intercepted, if the communications are encrypted, they must be decrypted for analysis.³⁷ Not all communications are encrypted in transmission but, if they are, the ease of decryption varies based on the strength of the encryption algorithm chosen by the wireless carrier.³⁸ As described in greater detail in Part V of this Article, the major Global System for Mobile communications (“GSM”) network operators in the U.S., such as AT&T and T-Mobile, still use extremely weak encryption algorithms for their older, second generation (“2G”) networks which can be easily deciphered with widely available software or purpose-built hardware.³⁹ Moreover, although the competing code division multiple access (“CDMA”) cellular networks (operated by Verizon and Sprint) use different, incompatible cellular technology and encryption algorithms, surveillance companies offer products capable of intercepting and tracking CDMA phones too.⁴⁰

37. Encrypted cellular communications must be decrypted before they can be listened to. In some countries, like India, encryption between phones and the network base stations is disabled. In India, this is a result of legislation prohibiting the use of encryption, likely intended to make interception by the government easier. *See Nehaluddin Ahmad, Restrictions on Cryptography in India — A Case Study of Encryption and Privacy*, 25 COMPUTER L. & SEC. REV. 173, 175 (2009); Pranesh Prakash, *How Surveillance Works in India*, N.Y. TIMES (July 10, 2013), <http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/> (“[P]roviders in India have been known [to] use A5/0, that is, no encryption . . .”). In the United States, there is no law requiring wireless carriers to use encryption to protect calls. The choice is left entirely up to the carriers, which do use encryption in some cases, but not always. *See infra* Part V.B.3.

38. A number of encryption algorithms are supported by modern cellular telephone systems, but the specific algorithm used to encrypt communications between a telephone and the carriers’ network is chosen by the wireless carrier. In the United States, the A5/1 algorithm and A5/0 (the “NULL” encryption option) are still used by major GSM carriers, such as AT&T and T-Mobile, for their 2G networks. *See infra* Part V. The major CDMA carriers, Sprint and Verizon, use different encryption algorithms for their 2G and 3G networks. The Long Term Evolution (“LTE”) 4G cellular standard, which is the next generation technology adopted by all U.S. carriers, includes support for encryption algorithms that are much stronger. However, as with prior generations of cellular technology, wireless carriers can still choose to not use any encryption (the NULL option) with LTE. *See VERIZON, THE VERIZON WIRELESS 4G LTE NETWORK: TRANSFORMING BUSINESS WITH NEXT-GENERATION TECHNOLOGY* 16 (2012), available at http://business.verizonwireless.com/content/dam/b2b/resources/LTE_FutureMobileTech_WP.pdf (“The 128-bit AES algorithm is the preferred option in the Verizon Wireless 4G LTE network . . . AES is preferred because it has undergone more public scrutiny than other encryption options.”).

39. *See infra* Part V for a discussion of the software tools and commercial products now available to crack cellular encryption algorithms.

40. These include the Harris Corporation and Elaman. *See Letter from Lin Vinson, Major Account Manager of Wireless Prods. Grp., Harris Corp., to Raul Perez, City of Miami Police Dep’t* (Aug. 25, 2008), available at <http://egov.ci.miami.fl.us/Legistarweb/Attachments/48003.pdf> (“The Harris StingRay and KingFish systems are compatible with the CDMA standard . . .”); HARRIS CORPORATION, STINGRAY PRODUCT DESCRIPTION, available at http://files.cloudprivacy.net/Harris_Stingray_product_sheet.pdf (last visited Oct. 24, 2014) (describing one version of the Harris StingRay as a “Transportable CDMA Interrogation, Tracking and Location, and Signal Information Collection System”); ELAMAN, *supra* note 33, at 14 (“For operational field usage, off-air GSM monitoring systems are very powerful and essential . . . Systems for . . . CDMA are [also] available.”);

Active surveillance, performed with a device known as an *International Mobile Subscriber Identity (“IMSI”)* *catcher* or *cell site simulator*, works by impersonating a wireless base transceiver station (“BTS”) — the carrier-owned equipment installed at a cell tower to which cellular phones connect — and tricking the target’s phone into connecting to it.⁴¹ For some surveillance capabilities, such as intercepting communications content, the IMSI catcher can also impersonate the carrier’s network infrastructure, such that calls and text messages are transmitted through the IMSI catcher, once again without disrupting the communication and thus remaining imperceptible to the target.⁴² Depending on the particular features of the surveillance device and how they are configured by the operator, IMSI catchers can be used to identify⁴³ nearby phones, locate them with extraordinary precision,⁴⁴ intercept outgoing calls and text messages,⁴⁵ as well

Advanced CDMA Interception System. INTERCEPT MONITORING SYS., <http://en.intercept.ws/catalog/2197.html> (last visited Dec. 18, 2014).

41. See Daehyun Strobel, IMSI Catcher 13 (July 13, 2007) (unpublished seminar paper, Ruhr-Universität Bochum), available at http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf (“An IMSI Catcher exploits [GSM’s lack of authentication] and masquerades to a Mobile [Phone] as a Base Station.”).

42. See, e.g., ABILITY COMPUTERS & SOFTWARE INDUS. LTD., IBIS (IN-BETWEEN INTERCEPTION SYSTEM) PRODUCT DESCRIPTION 4, available at http://www.toplinkpac.com/pdf/IBIS_Brochure.pdf (last visited Oct. 24, 2014) (“IBIS can fully imitate target’s phone and talks with GSM network on its behalf Such a scheme makes possible *interception of incoming and outgoing calls*”) (emphasis added).

43. See, e.g., CELLXION LTD., UGX SERIES 330: TRANSPORTABLE DUAL GSM / TRIPLE UMTS FIREWALL AND ANALYSIS TOOL, available at <http://s3.documentcloud.org/documents/810703/202-cellxion-product-list-ugx-optima-platform.pdf> (last visited Oct. 24, 2014) (including as features, “[c]omprehensive identification of IMSI, IMEI and TMSI information” and “[s]imultaneous high speed acquisition of handsets (up to 1500 per minute), across up to five networks”); Septier IMSI Catcher, SEPTIER COMM'C'N LTD., <http://www.septier.com/146.html> (last visited Dec. 18, 2014) (“Septier IMSI Catcher allows its user to extract the IMSI and IMEI of GSM MS operating in its coverage area”).

44. See, e.g., Memorandum from Stephen W. Miko, Resource Manager, Anchorage Police Dep’t, to Bart Mauldin, Purchasing Officer, Anchorage Police Dep’t (June 24, 2009) [hereinafter Miko Memorandum], available at <http://files.cloudprivacy.net/anchorage-pd-harris-memo.pdf> (“[The] system allows law enforcement agencies . . . the ability to . . . [i]dentify location of an active cellular device to within 25 feet of actual location anywhere in the United States.”); HARRIS CORPORATION, AMBERJACK PRODUCT DESCRIPTION, available at <http://egov.ci.miami.fl.us/Lististarweb/Attachments/34769.pdf> (last visited Dec. 18, 2014) (“AmberJack is a phased array direction finding (DF) antenna system capable of tracking and locating mobile phone users. The DF antenna array is designed to operate with Harris’ Loggerhead and StingRay products”); PKI ELECTRONIC INTELLIGENCE GMBH GERMANY, GSM CELLULAR MONITORING SYSTEMS 12, http://www.pki-electronic.com/2012/wp-content/uploads/2012/08/PKI_Cellular_Monitoring_2010.pdf (last visited Dec. 18, 2014) (describing device’s ability to locate “a target mobile phone with an accuracy of 2 m[eters].”).

45. See, e.g., IBIS II, *supra* note 21 (noting the ability to intercept “incoming and outgoing [calls]”); VERINT, TACTICAL OFF-AIR INTELLIGENCE SOLUTIONS 15 (2013), available at <http://s3.documentcloud.org/documents/885760/1278-verint-product-list-engage-gi2-engage-pi2.pdf> (describing device’s ability to “[l]isten to, read, edit, and reroute incoming and outgoing calls and text messages”).

as block service, either to all devices in the area or to particular devices.⁴⁶

Cellular surveillance technology, by its very nature, tends to be invasive and over-broad in its collection of data.⁴⁷ Active surveillance devices send signals, often indiscriminately, through the walls of homes,⁴⁸ vehicles, purses, and pockets in order to probe and identify the phones located inside.⁴⁹ Both active and passive devices also pick up the signals of other phones used by innocent third parties, particularly when government agencies using them do not know the exact location of their target and thus must drive through cities and neighborhoods while deploying cellular surveillance equipment in order to locate her.⁵⁰

Both passive and active telephone surveillance technologies exploit security flaws in cellular telephones. Passive devices exploit the weak or, in some cases, lack of any encryption used to protect calls, text messages, and data transmitted between phones and the wireless carriers' base stations. Active surveillance devices, on the other hand, exploit the lack of authentication of the base station by cellular phones.⁵¹ As a result, phones have no way to differentiate between a legitimate base station owned or operated by the target's wireless carrier and a rogue device impersonating a carrier's base station.⁵²

46. See CELLXION LTD., *supra* note 43 (describing device's ability to "[d]isable all handsets except operationally friendly"); Miko Memorandum, *supra* note 44 ("[The] system allows law enforcement agencies . . . the ability to . . . [i]nterrupt service to active cellular connection [and] [p]revent connection to identified cellular device.").

47. In some cases, this may be a selling point. See VERINT, *supra* note 45, at 7 (describing product's ability to "collect mass GSM traffic over a wide area").

48. The devices send signals like those emitted by a carrier's own base stations. Those signals, of course, must "penetrate walls" to provide connectivity indoors. *What You Need to Know About Your Network*, AT&T, <http://www.att.com/gen/press-room?pid=14003> (last visited Dec. 18, 2014); E.H. Walker, *Penetration of Radio Signals into Buildings in the Cellular Radio Environment*, 62 BELL SYS. TECHNICAL J. 2719 (1983).

49. See Kelly, *supra* note 21 ("Typically used to hunt a single phone's location, the system intercepts data from all phones within a mile, or farther, depending on terrain and antennas.").

50. See Affidavit of Supervisory Special Agent Bradley S. Morrison at 5, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC) [hereinafter Morrison Affidavit 2012], available at <http://www.documentcloud.org/documents/1282619-11-10-17-2011-u-s-v-rigmaiden-cr08-814-phx-dgc.html> ("During a location operation, the electronic serial numbers (ESNs) (or their equivalent) from all wireless devices in the immediate area of the FBI device that subscribe to a particular provider may be incidentally recorded, including those of innocent, non-target devices.").

51. See Strobel, *supra* note 41, at 13.

52. More recent cellular phone systems, including so-called 3G and 4G networks, now include the capability for phones to authenticate the network base stations. See generally Muxiang Zhang & Yuguang Fang, *Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol*, 4 IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS 734, 734 (2005), available at <http://www.fang.ece.ufl.edu/mypaper/tw05zhang.pdf>. However, even the latest smartphones are backward compatible with older, vulnerable phone network technologies, which allows the phone to function if it is taken to a rural location or foreign country where the only service offered is 2G. As a result, modern phones remain vulnerable to active surveillance via a *protocol rollback attack* in which the nearby 3G and 4G network

Passive wireless surveillance devices do not transmit any signals.⁵³ These devices are thus far more covert in operation — indeed effectively invisible⁵⁴ — but they can only detect signals of nearby phones when those phones are actually transmitting data.⁵⁵ Active surveillance devices have the disadvantage of being relatively less covert because they produce telltale signals that are detectable using sophisticated, counter-surveillance equipment,⁵⁶ but their corresponding advantage is that they can rapidly identify and locate all nearby phones that are turned on, even if they are not transmitting any data.⁵⁷

A. An Approximate History of Cellular Phone Surveillance Technology⁵⁸

Rohde & Schwarz, a German manufacturer of radio equipment, is generally believed to have created the first purpose-built active device capable of performing surveillance on cellular telephones.⁵⁹ Their first model, introduced in 1996, identified nearby wireless telephones by

signals are first jammed. See Matthew Green, *On Cellular Encryption, A FEW THOUGHTS ON CRYPTOGRAPHIC ENGINEERING* (May 14, 2013), <http://blog.cryptographyengineering.com/2013/05/a-few-thoughts-on-cellular-encryption.html> (“The biggest . . . concern for 3G/LTE is that you may not be using it. Most phones are programmed to gracefully ‘fail over’ to GSM when a 3G/4G connection seems unavailable. Active attackers exploit this feature to implement a *rollback attack* — jamming 3G/4G connections, and thus reactivating all of the GSM attacks . . .”).

53. See *GTRoS — GSM Traffic Recording System*, ABILITY COMPUTERS & SOFTWARE INDUS. LTD., <http://www.interceptors.com/intercept-solutions/Passive-GSM-Interceptor.html> (last visited Dec. 18, 2014) (describing product as “a multi-band fully passive GSM interception system” which “is completely undetectable”).

54. See VERTINT, *supra* note 45, at 7 (describing product’s ability to “[o]perate undetected leaving no electromagnetic signature”).

55. Any phone that is connected to a cellular network will regularly transmit data to nearby base stations, even if it is not making calls, sending text messages, or using the Internet. Locating a phone that is not currently transmitting data with a passive interception device may, however, require waiting some time until the device “checks in” with the cellular network or otherwise communicates with a nearby base station.

56. See *infra* Part IV.C.

57. See CELLXION LTD., *supra* note 43.

58. As telephone interception technology is also used by intelligence agencies and the military, it is impossible to tell a totally accurate history of the development of wireless telephone interception technology. As with many surveillance technologies, the military and intelligence community are the first to use them, and, after time, they trickle down to law enforcement. Neither the manufacturers of this equipment nor their many intelligence and military clients advertise their use. This portion of our Article is an attempt to paint an approximate picture, but it is likely that there are many aspects to this story that are missing, due to the fact that they remain classified.

59. The earliest public document describing IMSI catchers and the Rohde & Schwarz products is an article in 1997 by Dirk Fox, a German security consultant. See Dirk Fox, *IMSI-Catcher*, 21 DATENSCHUTZ UND DATENSICHERHEIT 539, 539 (1997), available at <http://www.secervo.de/publikationen/imsi-catcher-fox-1997.pdf>. Five years later, Fox published an updated, more in-depth article about the same technology. See Dirk Fox, *Der IMSI-Catcher*, 26 DATENSCHUTZ UND DATENSICHERHEIT 212, 212 (2002), available at <http://www.secervo.de/publikationen/imsicatcher-fox-2002.pdf>.

forcing them to transmit their serial number, or IMSI.⁶⁰ Within a year, the company had introduced a more sophisticated product that could also intercept outgoing phone calls.⁶¹

U.S. government agencies have used both active and passive forms of cellular telephone surveillance technology since at least the early 1990s, if not earlier.⁶² Military and intelligence agencies were early adopters of this technology, with law enforcement agencies quickly following their lead.⁶³ Passive devices, often referred to as *digital analyzers*, were used by law enforcement agencies as early as 1991.⁶⁴ Active surveillance devices were also used by federal law enforcement agencies as early as 1995.⁶⁵ Initially, U.S. agencies used devices that were “general use” cell site simulators, which wireless carrier technicians operated to test cellular phones.⁶⁶ Later, cellular equipment manufacturers created and sold cell site simulators specifically designed for government surveillance.

Infamous computer hacker Kevin Mitnick was located in 1995 by FBI agents using a combination of an active cell site simulator and a passive *TriggerFish*, a digital analyzer manufactured by the Harris Corporation.⁶⁷ The active cell site simulator was able to page Mitnick’s phone without causing an audible ring,⁶⁸ after which the passive *TriggerFish* was used to locate the phone.⁶⁹

By 2003, Harris had introduced its more sophisticated *StingRay* product,⁷⁰ which performed active surveillance of digital cellular

60. See Strobel, *supra* note 41, at 13; MMI Research Ltd v. Cellxion Ltd & Ors, [2009] EWHC (Pat) 418, [130] (Eng.), available at <http://www.bailii.org/ew/cases/EWHC/Patents/2009/418.html> (describing a presentation of the Rohde & Schwarz GA-090 IMSI Catcher device to three German wireless carriers in December 1996).

61. See Strobel, *supra* note 41, at 13.

62. As U.S. law enforcement and intelligence agencies do not advertise their intelligence gathering sources and methods, there is no way to accurately determine when U.S. government agencies first started to use active or passive wireless phone surveillance technology.

63. See Kelly, *supra* note 21 (“Initially developed for military and spy agencies, the *Sting[R]ays* remain a guarded secret by law enforcement and the manufacturer, Harris Corp. of Melbourne, Fla.”).

64. See Glen L. Roberts, *Who’s on the Line? Cellular Phone Interception at Its Best, FULL DISCLOSURE* (1991), available at <http://blockyourid.com/~gbpprorg/2600/harris.txt> (describing the marketing by the Harris Corporation of *TriggerFish* passive surveillance devices to law enforcement agencies at the National Technical Investigators Association conference in 1991).

65. See Tsutomu Shimomura, *Catching Kevin*, WIRED, Feb. 1996, at 124, available at http://www.wired.com/wired/archive/4.02/catching_pr.html.

66. *Id.*

67. *Id.*

68. This capability is commonly referred to as a “silent SMS.” See generally Fabien Soyez, *Getting the Message? Police Track Phones with Silent SMS*, OWNLEU (Jan. 27, 2012), <http://owni.eu/2012/01/27/silent-sms-germany-france-surveillance-deveryware>.

69. Shimomura, *supra* note 65.

70. The U.S. Trademark office registration of *StingRay*, registered in 2003, described the device as a “multi-channel, software-defined, two-way electronic surveillance radio[] for authorized law enforcement and government agencies for interrogating, locating, tracking

telephones.⁷¹ The company now manufactures an extensive range of cellular telephone surveillance products,⁷² which can be mounted in vehicles, on airplanes and drones, or carried by a person.⁷³ Harris sells its products to local, state, and federal law enforcement agencies,⁷⁴ intelligence agencies, and the military.⁷⁵ The company dominates the U.S. law enforcement market, although several other companies also sell similar technology to U.S. military and intelligence agencies.⁷⁶

and gathering information from cellular telephones" STINGRAY, Registration No. 2,762,468.

71. See HARRIS CORPORATION, *supra* note 40 ("StingRay is Harris' latest offering in a long line of advanced wireless surveillance products. StingRay is a multichannel software defined radio that performs network base station surveys, Dialed Number and registration collection, mobile interrogation, and target tracking and location with Harris' AmberJackTM Direction-Finding Antenna.").

72. See Ryan Gallagher, *Meet the Machines that Steal Your Phone's Data*, ARS TECHNICA (Sept. 25, 2013), <http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/>.

73. See Jennifer Valentino-DeVries, *Judge Questions Tools that Grab Cellphone Data on Innocent People*, WALL ST. J. (Oct. 22, 2012), <http://blogs.wsj.com/digits/2012/10/22/judge-questions-tools-that-grab-cellphone-data-on-innocent-people/>; Freedom of Information Act Response from U.S. Immigration and Customs Enforcement to author (Sept. 19, 2012) [hereinafter Freedom of Information Act Response], available at <https://s3.amazonaws.com/s3.documentcloud.org/documents/479397/stingrayfoia.pdf> (describing the purchase of a "StingRay II Airborne Training" session and an "Airborne Flight Kit").

74. See Kelly, *supra* note 21 ("At least 25 police departments own a Sting[R]ay, a suitcase-size device that costs as much as \$400,000 and acts as a fake cell tower . . . In some states, the devices are available to any local police department via state surveillance units.").

75. See, e.g., Space and Naval Warfare Systems Command, *Harris Corp Blackfin Equipment*, FEDBIZOPPS.GOV (May 24, 2010), <https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=f34fc14f76e8744bf75d41e6d0242db>; U.S. Army Intelligence and Security Command, *Notice of Intent To Award a Sole Source Contract-Harris: KingFish Dual Mode System*, FEDBIZOPPS.GOV (Jan. 12, 2009), https://www.fbo.gov/index?s=opportunity&mode=form&id=fd03ebae781f3a3fdb7633699bc1e351&tab=core&_cview=1; *Customized Equipment Training (SET017)*, MARINE CORPS INTELLIGENCE SCHOOLS, <https://www.mcis.usmc.mil/ITEP/Lists/ITEP%20Course%20Catalogue/DispForm.aspx?ID=31> (last visited Dec. 18, 2014) (including "Harris Corporation: Gossamer, LongShip, BlackFin, BlackFin II, HawksBill, SpurDog, FishFinder, King-Fish, StingRay, StingRay II, GSM Interrogator, CDMA Interrogator, iDEN Interrogator, UMTS Interrogator, FishHawk, Porpoise, FireFish, Tarpon, AmberJack, Harpoon, Moray, LanternEye, RayFish, StoneCrab"); U.S. Marine Corps, *Interrogation, Tracking, Location and Signal Information Collection System Devices with Software and Training*, FEDBIZOPPS.GOV (Sept. 12, 2006), https://www.fbo.gov/index?s=opportunity&mode=form&id=6a5efbcc2b7bdf2f37448ad68d48e7e&tab=core&_cview=0; U.S. Special Operations Command, *FishHawk Software*, FEDBIZOPPS.GOV (Sept. 22, 2011), <https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=3176fb4a66f92793ac34e7670205e2c5> ("StingRay II — Special Equipment — Over-The-Air special signal software that is compatible with the Harris StingRay II System.").

76. Other manufacturers of cellular surveillance technology used by the U.S. military and intelligence agencies include Boeing, CellXion, and Martone Radio Technology. Comments of the Boeing Company, to the Nat'l Telecomm. & Info. Admin., U.S. Dep't of Commerce, Preventing Contraband Cell Phone Use in Prisons, 75 Fed. Reg. 26733 (May 12, 2010), available at <http://www.ntia.doc.gov/files/ntia/comments/100504212-0212-01/attachments/Boeing%20and%20DRT%20Comments%20on%20NTIA%20Contraband%20Cell%20Phone%20NOI%206%202011%2010.pdf> ("DRT [(a wholly owned subsidiary of Boeing)] manufactures a line of wireless location and management technologies that emulate a base

B. Uses of Direct Surveillance Technology

Law enforcement agencies perform most cellular surveillance with the assistance of telecommunications and Internet companies. This method of surveillance uses carrier-owned equipment or technology that enables surveillance — typically with the aid of dedicated electronic surveillance and compliance teams employed by these companies.⁷⁷ For more than one hundred years, the telephone companies have provided such assistance.⁷⁸ While carrier-performed or enabled surveillance is generally the easiest, most efficient, and most covert way to intercept communications, it is not the only way.⁷⁹

In spite of the user-friendly, often inexpensive surveillance capabilities provided to the government by wireless carriers,⁸⁰ there are certain situations where governments may need or prefer to engage in

station to detect and locate wireless handsets of interest in a limited geographic area."); FCC Application for New or Modified Radio Station by Phoenix Global Support (Mar. 21, 2011), *available at* https://apps.fcc.gov/oetcf/els/reports/442_Print.cfm?mode=current&application_seq=47486&license_seq=48001 (requesting a license to use transmitting devices made by Martone Radio Technology, Harris, and CellXion). Phoenix Global Support, the company that requested the license, is located less than fifteen miles from Fort Bragg, in Fayetteville, NC, the headquarters of the Joint Special Operations Command ("JSOC"). The company's website states that it "offers complete classes and curriculum for Signals Intelligence (SIGINT) and Electronic Warfare (E/W) spanning the spectrum of wireless communications." PHOENIX GLOBAL SUPPORT, www.pgsup.com (last visited Dec. 18, 2014).

77. See Letter from William B. Petersen, Gen. Counsel, Verizon Wireless, to Rep. Edward J. Markey (May 22, 2012), *available at* <http://web.archive.org/web/2012121711531/http://markey.house.gov/sites/markey.house.gov/files/documents/Verizon%20Wireless%20Response%20to%20Rep.%20Markey.pdf> ("Verizon Wireless has a dedicated team of approximately seventy that works . . . to respond to lawful demands for customer information . . ."); Letter from Timothy P. McKone, Exec. Vice President, Fed. Relations, AT&T, to Rep. Edward J. Markey (May 29, 2012), *available at* <http://web.archive.org/web/20121228183409/http://markey.house.gov/sites/markey.house.gov/files/documents/AT%26T%20Response%20to%20Rep.%20Markey.pdf> ("AT&T employs more than 100 full time workers . . . for the purpose of meeting law enforcement demands.").

78. By 1895, the New York Police Department had the ability to wiretap any telephone in the city. Wes Oliver, *Wiretapping and the Apex of Police Discretion* (Apr. 22, 2010) (Widener Law School Legal Studies Research Series, Paper No. 10-14), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1594282 (describing "the early years of police wiretapping," where "a police officer would simply go to the telephone company and request that the phone company assist them with a wiretap," which allowed the wiretap squad to "listen-in on any telephone call in the City of New York.").

79. In fact, since the earliest days of the telephone, the police have also directly performed wiretaps. See Meyer Berger, *Tapping the Wires*, THE NEW YORKER, June 18, 1938, at 41, *available at* http://www.spybusters.com/History_1938_Tapping_Wires.html ("In those days police wire-tappers just walked into the Telephone Company's offices, asked for the location of the wires they were interested in, and got the information without fuss. Lines were usually tapped right in the cellar of the house or at an outside wall box.").

80. See Christopher Soghoian, *ACLU Docs Reveal Real-Time Cell Phone Location Spying Is Easy and Cheap*, SLIGHT PARANOIA (Apr. 3, 2012), <http://paranoia.dubfire.net/2012/04/aclu-docs-reveal-real-time-cell-phone.html> (quoting Paul Taylor, Electronic Surveillance Manager, Sprint Nextel, as stating that Sprint's web-based GPS tracking tool is extremely popular with law enforcement, who "love that it is extremely inexpensive to operate and easy").

direct, unmediated surveillance of telephones themselves using an active or passive device. These situations include:

(1) Identifying unknown phones currently used by a known target. In situations where a surveillance target is believed to frequently switch phones (for example, by using so-called “burner” disposable phones⁸¹), investigators may wish to learn the serial number of the phone currently in use, which is necessary in order to initiate a carrier-assisted wiretap⁸² or Pen Register/Trap and Trace device (hereinafter Pen/Trap).⁸³ Law enforcement can determine the specific phone used by a particular surveillance target by deploying an IMSI catcher to collect data about nearby phones at multiple locations, such as the target’s home and place of business. This method ultimately narrows the search to only those phones that were present in all of the monitored locations.⁸⁴

(2) Locating devices that cannot be found by the wireless carriers. Federal E-911 regulations require that carriers be able accurately to determine the location of cellular phones.⁸⁵ As this technical obligation was mandated in the context of E-911,⁸⁶ it only applies to

81. See *The Wire: Hamsterdam* at 00:42:23 (HBO television broadcast Oct. 10, 2004) (dialogue between two characters) (“They make a few calls with a burner, throw it away. Go on to the next phone, do the same. There’s more of those things laying around the streets of West Baltimore than empty vials.” “Well, how the fuck you supposed to get a wire up on that?”).

82. See 18 U.S.C. §§ 2511–2520 (2012) (authorizing the interception of wire, oral, or electronic communications — including communications content — by law enforcement to investigate crimes enumerated in the statute upon satisfying various elements set out in the statute).

83. See 18 U.S.C. §§ 3121–3127 (2012) (authorizing law enforcement to install and use a pen register device to “record[] or decode[] [non-content] dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted” and to install and use a trap and trace device to “capture[] the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication . . .”).

84. See Complaint at 8 n.1, United States v. Chaparro, No. 12 CR 969, 2014 BL 216188 (N.D. Ill. Aug. 5, 2014), available at http://www.justice.gov/usao/iln/pr/chicago/2013/pr0222_01d.pdf (“[L]aw enforcement officers . . . used a digital analyzer device on three occasions in three different locations where Chaparro was observed to determine the IMSI associated with any cellular telephone being carried by Chaparro.”); *The Wire: Middle Ground* at 00:18:20 (dialogue between two characters) (“[I]f we know the approximate time of [the target’s] call we can start just by pulling calls off that tower, at that time.” “That could be thousands.” “Yeah, but that’s the baseline, but we get a second hit . . . and that list comes down to dozens. And after a third or fourth . . . then we’ve got his number.”).

85. See 47 C.F.R. § 20.18(h) (2014).

86. *Id.* Similarly, although CALEA only required the wireless carriers to turn over information about the cell sites used at the beginning and end of a call, *supra* note 34, federal law enforcement agencies subsequently asked the FCC to issue regulations requiring the carriers to be able to turn over higher-accuracy location E-911 location information at any time, without the knowledge of the subscriber. See FED. COMM’NS COMM’N, PETITION FOR EXPEDITED RULEMAKING, IN THE MATTER OF PETITION FOR EXPEDITED RULEMAKING TO ESTABLISH TECHNICAL REQUIREMENTS AND STANDARDS PURSUANT TO SECTION 107(B) OF

devices capable of making a telephone call to 911. As such, there is no affirmative obligation that wireless carriers be able to accurately locate data-only devices, such as tablet computers and mobile data-cards. When the government wishes to locate data-only devices that cannot be precisely located by the wireless carrier,⁸⁷ it is likely to turn to active cellular surveillance.

(3) **Selectively blocking devices or dialed numbers.** There are situations and environments where public safety officials may use a cell site simulator to selectively block the use of particular phones.⁸⁸ Some prisons, for example, have installed devices that permit access to registered phones, such as those used by guards and other staff, while blocking all unregistered phones, such as those smuggled into the facility, from making or receiving calls.⁸⁹ Law enforcement agencies may also, during high-security events like a hostage situation or a bomb threat, seek to redirect outgoing numbers dialed by particular phones or block incoming calls to all nearby phones.

(4) **Foreign intelligence and military operations.** Although U.S. government agencies can compel surveillance assistance from U.S. wireless carriers, this power does not extend to telephone companies in foreign countries. Moreover, even if some level of assistance is available from foreign governments, U.S. agencies may wish to keep their foreign surveillance activities covert, such as when the surveil-

THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT 27, 32, 37 (2007), available at http://askcalea.fbi.gov/lef/docs/20070823_JSTD025-BDeficiencyPetitionWappendices.pdf (stating that since the carriers now have E-911 mandated high-quality location data, they should be required to deliver it to law enforcement). The FCC never acted on this petition, but, perhaps under pressure from law enforcement, many major wireless carriers now provide law enforcement real-time E-911 GPS level accuracy location data. *See Soghoian, supra* note 80 (describing the real-time GPS tracking surveillance tools offered by several wireless carriers).

87. The FCC gave wireless carriers the choice of using *handset-based* or *network-based* technology to comply with the E-911 mandate. *See FED. COMM'NS COMM'N, THIRD REPORT AND ORDER, NO. 99-245, IN THE MATTER OF REVISION OF THE COMMISSION'S RULES TO ENSURE COMPATIBILITY WITH ENHANCED 911 EMERGENCY CALLING SYSTEMS* (1999), available at <http://transition.fcc.gov/Bureaus/Wireless/Orders/1999/fcc99245.pdf>. The handset-based solution involves the installation in telephone handsets of GPS chips that can be remotely queried. In contrast, the network-based solution requires the installation of specialized technology at the carriers' base stations, which can then locate any device connected to the carrier's network, including data-cards and tablet computers. As such, carriers such as AT&T and T-Mobile, which have deployed network-based E-911 technology, are able to locate data-devices, while Verizon and Sprint, which deployed handset-based E-911 technology, cannot. *See id.*

88. *See Miko Memorandum, supra* note 44 ("The KingFish Dual-Mode System . . . is a . . . cellular phone surveillance and tracking system . . . This system allows law enforcement agencies . . . to . . . [i]nterrupt service to active cellular connection [and] [p]revent connection to identified cellular device ('No Service').").

89. *See NAT'L TELECOMM. AND INFO. ADMIN., U.S. DEP'T OF COMMERCE, REP. ON CONTRABAND CELL PHONES IN PRISONS, POSSIBLE WIRELESS TECHNOLOGY SOLUTIONS* 19–25 (2010), available at http://www.ntia.doc.gov/files/ntia/publications/contrabandcellphonereport_december2010.pdf (describing "managed access" methods of preventing contraband cell phones from being used in prisons).

lance is aimed at a particular foreign government and its political leaders.⁹⁰ As a result, when conducting surveillance abroad — and in some cases, even domestically⁹¹ — direct surveillance technology may be the most effective surveillance (or even the only) tool available to U.S. intelligence agencies and military units for intercepting certain communications or tracking particular phones.⁹² The same logic, of course, applies to foreign governments conducting espionage in the United States.⁹³

III. “KNOWN KNOWNS”: CASE LAW AND DOJ GUIDANCE

U.S. law enforcement agencies have used cellular surveillance technology for more than two decades⁹⁴ and spent tens of millions of dollars acquiring these devices at federal, state, and local levels.⁹⁵

90. See Duncan Campbell et al., *Revealed: Britain’s “Secret Listening Post in the Heart of Berlin,”* INDEPENDENT (Nov. 5, 2013), <http://www.independent.co.uk/news/uk/home-news/revealed-britains-secret-listening-post-in-the-heart-of-berlin-8921548.html>; *How NSA Spied on Merkel Cell Phone from Berlin Embassy*, DER SPIEGEL (Oct. 27, 2013), <http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html> (“From the roof of the embassy, a special unit of the CIA and NSA can apparently monitor a large part of cellphone communication in the government quarter. And there is evidence that agents based at Pariser Platz recently targeted the cellphone that [German Chancellor Angela] Merkel uses the most.”).

91. When performing surveillance on sophisticated targets with counter-intelligence expertise, such as foreign embassies and foreign intelligence services operating from foreign embassies in the U.S., intelligence agents are likely to use passive cellular interception technology because it is far more difficult to detect. See Matthew M. Aid, *Spy Copters, Lasers, and Break-In Teams*, FOREIGN POLICY (Nov. 19, 2013), http://www.foreignpolicy.com/articles/2013/11/19/spy_copters_lasers_and_break_in_teams_fbi_spies_on_diplomats (describing FBI “vans, aircraft, and helicopters” that are “equipped with equipment capable of intercepting cell-phone calls and other electronic forms of communication” for the purpose of “intercept[ing] the communications of all diplomatic missions and international organizations located on American soil” (emphasis added)).

92. See Jeremy Scahill & Glenn Greenwald, *The NSA’s Secret Role in the U.S. Assassination Program*, INTERCEPT (Feb. 10, 2014), <https://firstlook.org/theintercept/article/2014/02/10/the-nasas-secret-role/> (describing NSA drones equipped with “virtual base-tower transceivers . . . that can force a targeted person’s device to lock onto the NSA’s receiver” and allow “the military to track the cell phone to within 30 feet of its actual location, feeding the real-time data to teams of drone operators who conduct missile strikes or facilitate night raids.”).

93. See *infra* Part VI.

94. See *supra* Part II.A (discussing the fact that law enforcement has used passive devices since at least 1991 and active devices since at least 1995).

95. See Freedom of Information Act Response, *supra* note 73 (“ICE has invested \$5,000,000.00 towards the investment of equipment and training in Harris Corporation services.”); Kelly, *supra* note 21 (“The federal government funds most of the [StingRay] purchases, via anti-terror grants.”); Marisa Kendall & John Kelly, *Cell Tower Dumps Not Used Locally*, NEWS-PRESS, Dec. 8, 2013, at A, available at https://www.aclu.org/sites/default/files/assets/news-press_article_131208.pdf (“[The Florida Department of Law Enforcement] has spent more than \$3 million buying a fleet of Sting[R]ays, records show.”); Carl Prine, *FBI Closely Guards Details of Spy Gear Technology*, PITT. TRIB.-REV. (Feb. 16, 2014), <http://triblive.com/news/allegheny/5548583-74/fbi-technology-projects> (stating that public records revealed that Harris “secured 68 FBI contracts worth at least \$23.7 million.

Notwithstanding this history, there is scant case law addressing its use in investigations. Indeed, when compared with traditional, carrier-assisted cellular phone tracking,⁹⁶ there is limited case law and publicly available internal agency guidance describing: (1) statutory authorities that may permit or preclude law enforcement use and how the DOJ interprets such authorities to permit or limit law enforcement use (to include any Fourth Amendment constraints); (2) the frequency or regularity with which such technology is used by federal, state, and local law enforcement; (3) the types of investigations or actual factual scenarios where law enforcement agencies have used the technology; and (4) any related prosecution-based and policy-driven considerations for the retention of data collected by an IMSI catcher. This Part will present and analyze the limited publicly available case law and DOJ guidance in an attempt to describe the policies and rules governing federal law enforcement agencies' use of this technology.

A. The 1995 Digital Analyzer Magistrate Opinion⁹⁷

Despite their use since at least 1991,⁹⁸ it was not until 1995 that a federal magistrate judge in California published the first decision analyzing a government application to use a digital analyzer.⁹⁹ In this matter, the government wanted court authorization to use a passive surveillance device to "analyze signals emitting from any cellular phone used by any one of five named subjects of a criminal investigation."¹⁰⁰ The agents likely needed to use this technology because they did not know the particular phone numbers that the targets were using, and thus could not seek surveillance assistance from the targets' wire-

Purchases included Harris devices such as the StingRay, Amberjack, Kingfish and Gossamer trackers, plus spare parts and classroom instruction.").

96. For a discussion of the statutory authorities used by law enforcement to acquire cellular phone location data and an analysis of multiple court opinions addressing law enforcement access to location data, see generally Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 27 BERKELEY TECH. L.J. 117 (2012). For information about the frequency or regularity with which federal, state, and local law enforcement agencies make requests for location data from carriers, see generally the collection of documents posted at http://www.markey.senate.gov/documents/2013-10-03_ATT_re_Carrier.pdf and http://www.markey.senate.gov/documents/2013-12-09_VZ_CarrierResponse.pdf (describing carrier disclosure of real-time and historical location data to law enforcement agencies).

97. Our analysis of this magistrate opinion draws from our previous article, Stephanie K. Pell & Christopher Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J.L. & TECH 134, 157–60 (2013).

98. See Roberts, *supra* note 64.

99. In the Matter of the Application of the United States of America for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer, 885 F. Supp. 197 (1995). The government submitted an *ex parte* application for an order permitting agents of the Orange County Regional Narcotics Suppression Program ("RNSP") to use a digital analyzer. *Id.* at 198–99.

100. *Id.* at 199.

less carriers.¹⁰¹ It also appears that the agents wanted to determine with whom the targets were communicating, information they could obtain in real time by intercepting signals as calls took place.¹⁰²

Following what was likely DOJ policy at the time,¹⁰³ the government sought a pen register order authorizing the surveillance. Magistrate Judge Edwards denied the government's application without prejudice, explaining that a Pen/Trap court order was not required because the Pen/Trap statute limits its application "to a device 'which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line *to which such device is attached.*'"¹⁰⁴ Judge Edwards noted that, because the digital analyzer was not intended to be — and could not be — physically attached to the cellular phone, the Pen/Trap statute was not applicable to its use.¹⁰⁵

101. The opinion notes that agents could not identify the particular cellular telephones they wished to analyze. *Id.*

102. *Id.* Information about whom targets are communicating with is often relevant to identifying the scope of the alleged criminal activity to discover the identities of additional criminal targets that may not be known to law enforcement. It would not, however, be necessary for the agents to continue to use a digital analyzer to determine the phone numbers the target phone was calling and was called by once the target phone was identified through its unique identifying number. Rather, agents could subpoena historical telephone toll records from the relevant cell phone provider(s) or obtain a Pen/Trap order to collect real-time records from the provider(s) reflecting this information. Indeed, once target phones are appropriately identified through their unique numbers, more traditional forms of carrier-assisted surveillance can proceed.

103. See discussion *infra* Part III.B.

104. See *In the Matter of the Application of the United States of America for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer*, 885 F. Supp. at 200.

105. *Id.* The court further explained its reasoning:

The statutory definition of a "trap and trace device" does not include the limitation in the definition of a pen register described above, limiting the devices to those that are attached to a telephone line. *See* 18 U.S.C. § 3127(4). Nonetheless, it appears from the construction of related sections of the statutes governing trap and trace devices that they include only devices that are attached to a telephone line. Specifically, 18 U.S.C. § 3123(b) requires that an order for use of both pen registers and trap and trace devices include "the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached . . .".

This limitation on the proscription against pen registers and trap and trace devices to prohibit only devices that are "attached" to a telephone line cannot be assumed to be inadvertent. In other statutes relating to interceptions of telephone communications, Congress encompassed, generally, any types of interceptions of wire, oral, or electronic communications — regardless of whether the intercepting device was "attached" to a telephone line. *See, e.g.*, 18 U.S.C. § 2511. That Congress did not impose equally comprehensive restrictions on lesser interceptions that do not raise 4th Amendment issues, such as those made with pen registers and trap and trace devices, is neither surprising nor inconsistent.

In any event, it must be remembered that the prohibition against the use of pen registers and trap and trace devices without court order is found in a criminal statute. *See* 18 U.S.C. § 3121(d).

Judge Edwards also found, pursuant to the third party doctrine as articulated in *Smith v. Maryland*,¹⁰⁶ that the government's use of a digital analyzer raised no Fourth Amendment concerns.¹⁰⁷ The court noted that “[n]umbers dialed by a telephone are not the subject of a reasonable expectation of privacy” and “[n]o logical distinction is seen between telephone numbers called and a party’s own telephone number (or [device serial] number), all of which are regularly voluntarily exposed and known to others.”¹⁰⁸

Although Judge Edwards ruled that the Pen/Trap statute did not regulate the passive surveillance technology the government sought to use — that is, it neither authorized nor prohibited its use — he expressed serious reservations about its use by law enforcement.¹⁰⁹ Specifically, he expressed concern about both the privacy of innocent third parties in range of the device and a lack of adequate congressional oversight.¹¹⁰ If the court were to authorize the government's use of a digital analyzer to identify the particular phones used by known targets, Judge Edwards acknowledged that such an order would essentially permit agents to intercept signals emitted from *all* phones in the target's area.¹¹¹ Thus, in addition to the unique serial numbers identifying the targets' phones, the digital analyzer would also identify the serial numbers of phones used by innocent third parties.¹¹² Judge Edwards recognized that “depending upon the effective range of the digital analyzer, telephone numbers and calls made by others than the subjects of the investigation could be inadvertently intercepted.”¹¹³

Under well-settled principles, the statute should be strictly construed, and any ambiguity in its scope must be construed narrowly.

Id.

106. 442 U.S. 735 (1979).

107. In the Matter of the Application of the United States of America for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer, 885 F. Supp. at 199.

108. *Id.*

109. *Id.* at 201–02.

110. *Id.*

111. *Id.*

112. *Id.*

113. *Id.* at 201. The court also noted that, although the agents were not seeking to intercept communications content, the digital analyzer they used could be programmed for that purpose. *Id.* at 199; *see also* STAFF OF THE ELEC. SURVEILLANCE UNIT, OFFICE OF ENFORCEMENT OPERATIONS — ITS ROLE IN THE AREA OF ELECTRONIC SURVEILLANCE 14 (1997) [hereinafter 1997 DOJ GUIDANCE] (published in the U.S. Attorneys' Bulletin), available at http://www.justice.gov/usao/eousa/foia_reading_room/usab4505.pdf (describing a digital analyzer as being “programmed so it will not intercept cellular conversations or dialed numbers when it is used for the limited purpose of seizing ESNs and/or the cellular telephone’s number,” although the analyzer is capable of such interceptions); ELEC. SURVEILLANCE UNIT, U.S. DEP’T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL: PROCEDURES AND CASE LAW FORMS 41 (2005) [hereinafter 2005 ELECTRONIC SURVEILLANCE MANUAL], available at <http://www.justice.gov/criminal/foia/docs/elec-surveillance-manual.pdf> (“Digital analyzers/cell site simulators/triggerfish and similar devices may be capable of intercepting the contents of communications and, therefore, such devices must be

The court also expressed concern that an order, if granted, would permit the government to collect data about large numbers of phones without any record-keeping or reporting requirements, thus preventing effective congressional oversight of the surveillance tool. Specifically, the court contrasted the “lack of record production” with the statutory reporting requirements in the Pen/Trap statute, such as “the use of court orders that identified particular telephones and the investigative agency” and “periodic reports to Congress stating the numbers of such orders.”¹¹⁴ Noting these differences and others,¹¹⁵ the court found that the government’s application “would not insure sufficient accountability.”¹¹⁶

Although clearly troubled by the surveillance capabilities of this technology, the court could not restrain its use by law enforcement.¹¹⁷ Moreover, the court’s determination that neither the Fourth Amendment nor the Pen/Trap statute authorized, restricted, or otherwise regulated law enforcement use of the technology likely reinforced the DOJ’s view that it did not *need* court authorization for use of a digital analyzer, even if it advised prosecutors to seek court authorization out of an abundance of caution or as a matter of policy.¹¹⁸ The DOJ later articulated this position in a 1997 internal document.

B. The 1997 DOJ Guidance

A document published by the DOJ in 1997, initially distributed nationally to prosecutors¹¹⁹ and later published on the DOJ’s website, is the earliest publicly available DOJ document that describes the capabilities of passive and active wireless phone surveillance technology.¹²⁰ The document also discusses, again for the first time, the legal

configured to disable the interception function, unless interceptions have been authorized by a Title III order.”).

114. *See In re the Application of the United States of America for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer*, 885 F. Supp. at 201–02.

115. *Id.* (citing 18 U.S.C. §§ 3123(b), 3126).

116. *Id.* at 201.

117. The court denied the government’s application because it found that the Pen/Trap statute was not applicable to a digital analyzer. *Id.* at 200. The court noted that the government was seeking the application only “out of an abundance of caution.” *Id.*

118. The court’s reasoning appears to illustrate its concern that, if it granted such an order — even “out of an abundance of caution” — pursuant to a statute whose definitional elements did not conform to the surveillance technique at issue, the court risked giving: (1) a potentially incorrect interpretation of a statute, or worse (2) judicial approval of a surveillance technique that Congress appeared neither explicitly to authorize nor prohibit.

119. *See* 1997 DOJ GUIDANCE, *supra* note 113. USA Bulletins are published by the Executive Office of United States Attorneys (“EOUSA”) and distributed to United States Attorneys’ Offices across the country. They cover a range of topics and issues of interest to federal prosecutors (such as law enforcement surveillance methods), including new case law, law enforcement tools and practices, statutory authorities, and internal DOJ guidance.

120. *Id.* at 13–14 (describing the types of information that digital analyzers and cell site simulators acquire).

policies governing the technology's use by federal law enforcement agents.¹²¹

In this document, the DOJ took the position that, as long as (1) law enforcement agents were not intercepting communications content and (2) the acquisition of the non-content data did not involve the assistance of carriers, "it does not appear that there are constitutional or statutory constraints on the warrantless use of [an active or passive surveillance] device . . .".¹²² In other words, the DOJ appears to have recognized no need for a warrant or other judicial process for

121. *Id.* at 13–15.

122. *Id.* at 14. Specifically, the DOJ reasoned that

Title III's provisions (18 U.S.C. §§ 2510–2522) would not apply to the use of a digital analyzer or a CSS when they are used to capture call processing information (MIN, ESN, cell site location, status of call, etc.) because they do not intercept the contents of any wire, oral, or electronic communication as the term "contents" is defined by Title III. Currently, Section 2510(8) states, "contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that information." ESNs/MINs and other automatic call processing information that are technologically necessary for the service provider to process cellular calls are not the types of transmissions Congress included within Section 2510(8)'s definition of "contents" when it was amended in 1986. [See S. Rep. No. 541 at 13 (1986)].

Id. (bracketed citation in original). Moreover, the DOJ asserts:

[T]here is no "electronic communication" [as defined by 18 U.S.C. § 2510(12)] unless the MIN or ESN is "transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic, or photo optical system that affects interstate or foreign commerce." A transmission normally contemplates a sender and a receiver. The ECPA legislative history regarding the definition of wire communication warns against an improper mechanical reading of the phrase "in whole or in part . . . by the aid of wire . . ." and states that the phrase "is intended to refer to wire that carries the communication to a significant extent from the point of origin to the point of reception, even in the same building. It does not refer to wire that is found inside the terminal equipment at either end of the communication." [S. Rep. No. 99-541, 12.] Thus, it does not appear that MINs and ESNs "forced" from the cellular telephone by the CSS or obtained by a digital analyzer are "electronic communications" within the contemplation of 18 U.S.C. § 2510(12).

Id. (bracketed citations in original). The DOJ further excludes collection of cell site information from a digital analyzer or cell site simulator from Stored Communications Act ("SCA") statutory requirements:

If cell site information is treated as a subscriber record or other information rather than a contemporaneous electronic communication covered by Title III, then 18 U.S.C. § 2703 (regarding stored electronic communications) might apply. It should be noted, however, that Section 2703 controls disclosures by service providers to Government entities and does not prohibit the Government from obtaining such information on its own without involving the service provider. Additionally, because CSSs and digital analyzers do not access communications in electronic storage in a facility with electronic communication service, Section 2703 does not apply.

Id. at 14–15.

law enforcement's use of digital analyzers and cell site simulators when they are only employed to intercept non-content data (including location data and real-time numbers sent and received) without the assistance of carriers, whether in relation to specific targets or innocent third parties.

Although concluding that law enforcement use of these direct, unmediated surveillance devices did not *require* any legal process, the 1997 DOJ Guidance, as a matter of *policy*, advises that "to the extent [cell site simulators] and digital analyzers are used as pen registers or trap and trace devices, they should only be used pursuant to a court order issued pursuant to these statutes."¹²³ When law enforcement wants to determine in real time the calls made and received by a particular phone, the government can obtain a court order compelling a service provider to install a pen register or trap and trace device.¹²⁴ This disclosure of information involving carrier assistance is regulated by statute, whereas the digital analyzer and cell site simulator technology enables government agents to obtain the same information directly from cell phones *without* any statutory process requirement. Perhaps in an effort to reconcile this disparity in regulation, arguably as early as 1995¹²⁵ but certainly by 1997, the DOJ advised prosecutors and agents to seek Pen/Trap court process when using a digital analyzer/cell site simulator as a Pen/Trap device.¹²⁶

The 1997 DOJ Guidance also recognized that digital analyzers and similar technologies could capture cell site location data (to include cell site data for target phones as well as innocent third-party phones).¹²⁷ While the capability to acquire location data directly may not have raised significant constitutional or policy-related "red flags" to the DOJ in 1994¹²⁸ or 1997, determining and fixing the proper legal

123. *Id.* at 14 (noting that the guidance to seek a Pen/Trap order is "[d]epartment[] policy").

124. See 18 U.S.C. §§ 3121–3127 (2012).

125. The DOJ sought a Pen/Trap order from Judge Edwards "out of an abundance of caution." *See supra* note 117.

126. 1997 DOJ GUIDANCE, *supra* note 113, does not, however, give any similar guidance with respect to direct (non-carrier assisted) collection of cell phone location data. In other words, it does not advise agents and prosecutors to obtain the same legal process used to compel location data from carriers.

127. *Id.* at 14. Digital analyzers and cell site simulators "can capture the cell site codes identifying the cell location and geographical sub-sector from which the cellular telephone is transmitting; the call's incoming or outgoing status; the telephone numbers dialed (pen register order required); and the date, time, and duration of the call." *Id.*

128. In 1994, the Office of Enforcement Operations ("OEO") opined that "investigators did not need to obtain any legal process in order to use cell phone tracking devices so long as they did not capture the numbers dialed or other information 'traditionally' collected using a pen/trap device." 2005 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 113, at 45. Back in 1994, the OEO concluded that the "'signaling information' automatically transmitted between a cell phone and the provider's tower does not implicate either the Fourth Amendment or the wiretap statute because it does not constitute the 'contents' of a communication." *Id.* Moreover, the 1994 analysis reasoned that "the pen/trap statute did not

standard(s) for authorizing law enforcement access to location data has become the subject of considerable debate for both the courts and Congress.¹²⁹

C. The 2001 USA PATRIOT Act Amendments to Pen/Trap Statute and Guidance in the 2005 Electronic Surveillance Manual

While the PATRIOT Act is generally not thought of as privacy-enhancing legislation, it did bring law enforcement use of passive and active cellular surveillance technology under some limited degree of judicial supervision and congressional oversight through specific definitional changes to the Pen/Trap statute.

Whereas the pre-2001 pen register definition only applied to “numbers dialed or otherwise transmitted,” the PATRIOT Act added the term “signaling information.”¹³⁰ The 2005 edition of the DOJ’s Electronic Surveillance Manual explains that “[s]ignaling information” is a broader term that encompasses other kinds of non-content information used by a communication system to process communications.¹³¹ Indeed, the DOJ instructed prosecutors that the new pen register definition “appears to encompass *all* of the non-content between a cell phone and a provider’s tower.”¹³²

apply to the collection of such information because of the narrow definitions of ‘pen register’ and ‘trap and trace device.’” *Id.* Therefore, “since neither the [C]onstitution nor any statute regulated their use, such devices did not require any legal authorization to operate.” *Id.*

129. See generally Pell & Soghoian, *supra* note 96 (describing the current congressional debates over proper legal standard(s) and analyzing various magistrate opinions requiring different legal standards for law enforcement access to location data).

130. See 18 U.S.C. § 3127(3) (2012) (defining pen register as “a device or process which records or decodes dialing, routing, addressing, and signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted”).

131. 2005 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 113, at 45

132. *Id.* (emphasis added). Similarly, the definition of “trap and trace” device, which originally included only “the originating number of an instrument or device” expanded to include “the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication . . .” 18 U.S.C. § 3127(4). Like the expanded definition of pen register, the DOJ instructs that the new trap and trace definition now “appears to include such information as the transmission of a MIN [or other type of unique identifying number], which identifies the source of a communication.” 2005 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 113, at 46. The DOJ’s conclusion that Pen/Trap now encompasses all non-content data between a cell phone and a cell tower was based, in part, on its analysis of the relevant but “scant” legislative history which suggested that the new definitions were intended to “apply to all communications media, instead of focusing solely on traditional telephone calls.” *Id.* Examining, for example, House language referencing “a packet requesting a telnet session — a piece of information passing between machines in order to establish a communication session for the human user,” the DOJ suggests that the term “provides a close analogy to the information passing between a cell phone and a tower in the initial stages of a cell phone call.” *Id.* at 47. Moreover, in contrast to earlier Pen/Trap definitions that referenced the attachment of a Pen/Trap device to a phone line, the House Report recognized that Pen/Trap devices “could . . . collect information remotely.” *Id.*

These expanded Pen/Trap definitions had implications for law enforcement's direct collection of mobile device serial numbers, real-time monitoring of numbers called and received, and acquisition of location information. Specifically, post-PATRIOT Act, the DOJ took the position that *all* forms of non-content data collected directly required prosecutors to obtain a Pen/Trap court order.¹³³

D. 2012 Cell Site Simulator ("StingRay") Magistrate Opinion¹³⁴

With the passage of the PATRIOT Act in 2001, the DOJ took the position that a Pen/Trap order was necessary to authorize law enforcement use of direct surveillance technology, like a StingRay, to intercept non-content data. It would take more than a decade, however, for a federal magistrate judge to publish an opinion evaluating an

It should be noted, however, that the DOJ drew a distinction between standards authorizing "off air" collection of cell phone location data via digital analyzers and IMSI catchers and the collection of these data through *compelled disclosures* from carriers. Indeed, in 1994, the CALEA instructed that "any information that may disclose the physical location of [a telephone service] subscriber" may *not* be acquired "solely pursuant to the authority for pen registers and trap and trace devices . . ." 47 U.S.C. § 1002(a)(2) (2012). The DOJ opined that, "[b]y its very terms, this prohibition applies only to information collected by a provider and not to information collected directly by law enforcement authorities. Thus, CALEA does not bar the use of pen/trap orders to authorize the use of cell phone tracking devices used to locate targeted cell phones." 2005 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 113, at 46–47.

As applied to compelled disclosures of prospective location information from carriers, the CALEA dictate meant that the DOJ had to find another authority to pair with or replace Pen/Trap authority. Since at least 2005, the DOJ has been advising prosecutors to obtain both a Pen/Trap order and an 18 U.S.C. § 2703(d) order ("D Order"). *See* Pell & Soghoian, *supra* note 96, at 135–37. Moreover, some magistrate judges have required "probable cause" search warrants before issuing orders authorizing law enforcement to compel a provider to track a cell phone in real time. *Id.* at 137–39. As referenced earlier, the appropriate standard(s) for law enforcement-compelled disclosures of historical and prospective location data remains an unresolved issue for the courts and Congress. *See supra* note 96. For purposes of this discussion, however, it is sufficient to note that both a D Order and a "probable cause" warrant standard are more stringent than Pen/Trap. To obtain a Pen/Trap order, the government need merely certify that the information sought "is relevant to an ongoing criminal investigation . . ." 18 U.S.C. § 3122(b)(2) (2012). Such "certification" does not require any fact finding by a magistrate judge. *See* Pell & Soghoian, *supra* note 97, at 155–56. In contrast, to obtain a D Order, the government must assert and a judge must find "specific and articulable facts" that the location information sought is "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). The requirement for a search warrant is even more stringent, as the government must show, and a magistrate must find, that there is probable cause to believe that the location information would be "evidence of a crime." *See* FED. R. CRIM. P. 41(c)(1). Notwithstanding that compelling location data from a carrier would require a more stringent standard than that found in the Pen/Trap statute, the DOJ's 2005 Guidance took both the legal and policy position that a Pen/Trap order was sufficient for direct collection of cell phone location data by law enforcement. 2005 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 113, at 47 ("CALEA does not bar the use of pen/trap orders to authorize the use of cell phone tracking devices used to locate targeted cell phones.").

133. *Id.* at 45–48.

134. Our analysis of this magistrate opinion draws from our previous article. Pell & Soghoian, *supra* note 97.

application for law enforcement use of a direct, active surveillance device.¹³⁵

In 2012, a federal magistrate judge from Texas issued an order denying an application submitted by agents from the Drug Enforcement Agency for the use of a StingRay.¹³⁶ The government sought a Pen/Trap order “to detect radio signals emitted from wireless cellular telephones in the vicinity of the [Subject] that identify the telephones . . .”¹³⁷ The agents submitted their application pursuant to 18 U.S.C. §§ 3122(a)(1), 3127(5) (the Pen/Trap statute) and 2703(c)(1) (a provision of the Stored Communications Act).¹³⁸ The government informed Magistrate Judge Owsley that the application was “based on a standard application model and proposed order approved by the [DOJ].”¹³⁹

Since the subject was known to law enforcement (whereas the subject’s phone was unknown), the agents planned to identify the phone by capturing device identification data “at various locations in which the [subject’s] [t]elephone [was] reasonably believed to be operating . . .”¹⁴⁰ After reviewing the application, Judge Owsley conducted an *ex parte* hearing and ultimately denied the government’s application.¹⁴¹ Judge Owsley expressed concern that the application did not explain adequately either the technology itself, “how many distinct surveillance sites [the agents] intend[ed] to use, or how long

135. One likely reason for this time gap is the default sealing of all pen register applications and orders with no corresponding requirement that they be unsealed outside of the prosecution’s discovery obligations to indicted criminal defendants as part of the criminal discovery process. See generally Stephen Wm. Smith, *Gagged, Sealed and Delivered: Reforming ECPA’s Secret Docket*, 6 HARV. L. & POL’Y REV. 313, 314 (2012) (“Through a potent mix of indefinite sealing, nondisclosure (i.e., gagging), and delayed-notice provisions, ECPA [Electronic Communications Privacy Act] surveillance orders all but vanish into a legal void.”). The Pen/Tap statute is Title III of ECPA. See Pub. L. No. 99-508, tit. III, 100 Stat. 1848, 1868–73 (codified as amended at 18 U.S.C. §§ 3121–3127 (2012)).

136. In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747, 748 (S.D. Tex. 2012). A target had switched from using a phone known to agents to an unknown phone. *Id.* The agent leading the investigation indicated that the “equipment designed to capture [the] cell phone numbers was known as a ‘[S]ting[R]ay.’” *Id.*

137. *Id.*

138. It is not clear from the 2012 magistrate opinion what purpose this citation to ECPA’s Stored Communications Act served in terms of providing additional authority of unmediated, direct collection of non-content data in this investigation. The 2005 Guidance indicated that only a Pen/Trap order was required for use of devices to collect non-content data directly. 2005 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 113, at 47–48. The DOJ, however, might have provided updated guidance reflecting a different or more nuanced legal position. As of the writing of this Article, this new guidance, if it exists, is not publicly available.

139. In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d at 749.

140. *Id.* at 748.

141. *Id.* at 748, 752.

they intend[ed] to operate the [S]ting[R]ay equipment to gather all telephone numbers in the immediate area.”¹⁴² Moreover, the court noted that no explanation was given, either in writing or verbally, as to what would be done with the innocent information collected from the phones of uninvolved individuals who just happened to be in the area under surveillance.¹⁴³ Finally, the court expressed concern that neither the prosecutor nor the Drug Enforcement Administration agent appeared to understand the technology at issue and “seemed to have some discomfort in trying to explain it.”¹⁴⁴

Notwithstanding these concerns, the court’s decision to deny the application appears to stem from a definitional problem the court identified in the Pen/Trap statute that the government did not adequately address during the application or *ex parte* hearing process. While recognizing that the PATRIOT Act broadened the Pen/Trap definitions, “amplif[ying] the various types of information that are available such as routing and signaling information,”¹⁴⁵ Judge Owsley interpreted § 3123(b)(1) of the pen register statute as “straightforward in that a telephone number or similar identifier is *necessary* for a pen register.”¹⁴⁶ Accordingly, the judge found that the language in the statute “mandates that this Court have a telephone number or some similar identifier before issuing an order authorizing a pen register.”¹⁴⁷ Because the government did not provide any support to the contrary in case law or any other authority suggesting that the statute authorized collection of non-content data from *unidentified* devices, the judge denied the application without prejudice.¹⁴⁸

E. The Rigmaiden Federal Prosecution

In 2011, a decade after the Harris Corporation introduced the StingRay,¹⁴⁹ the FBI’s use of the device finally surfaced during the pre-trial stages of a criminal case.¹⁵⁰ The government prosecuted Daniel David Rigmaiden (“Rigmaiden”) for his role in a scheme through which he obtained fraudulent tax refunds for hundreds of deceased

142. *Id.* at 749.

143. *Id.*

144. *Id.*

145. *Id.* at 751.

146. *Id.* (emphasis added).

147. *Id.*

148. *Id.* at 751–52.

149. See discussion *supra* Part II.

150. United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012); see also Valentino-DeVries, *supra* note 26 (“A [S]ting[R]ay’s role in nabbing the alleged ‘Hacker’ — Daniel David Rigmaiden —is shaping up as a possible test of the legal standards for using these devices in investigations.”).

persons and other third parties.¹⁵¹ After a lengthy investigation, federal agents located Rigmaiden, in part by tracking the location of “[a wireless data-card] connected to a laptop computer” in his apartment.¹⁵² The government did not know Rigmaiden’s actual identity until agents arrested him.¹⁵³ Indeed, the government’s only solid lead was an IP address associated with the prepaid Verizon data-card that Rigmaiden used to transmit fraudulent tax returns to the IRS.¹⁵⁴ To narrow down the location of the data-card, the government obtained historical cell-site records from Verizon. Those records determined that the data card’s location was within an approximately one-quarter square-mile area. As Verizon did not have the technical capability to provide higher-accuracy location information,¹⁵⁵ the government used a StingRay to locate the data-card, leading the agents to Rigmaiden’s apartment.¹⁵⁶

Prior to locating the data-card, the government obtained a search warrant pursuant to Fed. R. Crim. P. 41(b) authorizing the use of a cell site simulator.¹⁵⁷ After his arrest, Rigmaiden filed a motion to suppress, arguing that the government had repeatedly violated the Fourth Amendment in its efforts to locate him.¹⁵⁸ Ultimately, the gov-

151. The government indicted Rigmaiden in a superseding indictment on seventy-four counts of wire fraud, aggravated identify theft, mail fraud, and conspiracy to commit these offenses. *United States v. Rigmaiden*, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *1 (D. Ariz. May 8, 2013). In April 2014, Rigmaiden pleaded guilty to four felony counts of mail fraud, wire fraud, and conspiracy to commit these offenses. See Dennis Wagner, *Tax Scammer Rigmaiden Pleads Guilty, Gets Time Served*, AZCENTRAL (Apr. 8, 2014), <http://www.azcentral.com/story/news/politics/2014/04/07/rigmaiden-tax-scammer-pleads-guilty/7448151>. He was sentenced to time served, which amounted to the sixty-eight months he spent awaiting trial. *Id.*

152. *United States v. Rigmaiden*, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *1 (D. Ariz. May 8, 2013).

153. *Id.* at 1–6.

154. *Id.* at 1–4.

155. See *supra* Part II.B.2 and note 86 (explaining how E-911 regulations do not require carriers to be able to locate data-only devices in real-time).

156. Investigative Details Report at 7, *United States v. Rigmaiden*, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC), available at <https://ia600707.us.archive.org/33/items/gov.uscourts.azd.396130.gov.uscourts.azd.396130.484.6.pdf> (U.S. Postal Inspection Services Inspector James L. Wilson states in the report that “[o]n 7/16/08, we were informed that they were able to track a signal and were using a ‘Sting[R]ay’ to pinpoint the location of the aircard.”).

157. *United States v. Rigmaiden*, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *14 (D. Ariz. May 8, 2013) (noting that Judge Seeborg found that the warrant application “established ‘probable cause to believe that the use and monitoring of a mobile tracking device’ would ‘lead to evidence of’ several specific crimes, including conspiracy to defraud the government, fraud relating to identity information, aggravated identity theft, and wire fraud,” and the identification of those who committed the offenses).

158. Rigmaiden’s motion to suppress divides the government’s investigative actions into twenty-one different searches. *Id.* at 6. In its Order addressing Rigmaiden’s Motion to Suppress, the District Court grouped the alleged searches, the defendant’s challenges, and the government’s responses into the following categories:

whether Defendant had a legitimate expectation of privacy in the location of the aircard; the government’s collection of historical cell-

ernment conceded *arguendo* that its efforts to locate Rigmaiden's data-card constituted a Fourth Amendment search and seizure.¹⁵⁹

A key question to consider is why the government chose to make this concession when the DOJ's 2005 Guidance did not advise that digital analyzers and cell site simulators raised any Fourth Amendment issues that would necessitate securing a warrant. Is there a more nuanced DOJ position directing or advising prosecutors to obtain a warrant when the use of a cell site simulator may reveal the location of a device to be inside a home or other protected space?¹⁶⁰

site information, destination IP addresses, and data from the Domicilio apartment's alarm company; the search for the aircard using the mobile tracking device; the searches of Defendant's apartment and computer; and whether the Fourth Amendment's good faith exception applies.

Id. at 6–7.

159. *Id.*; Government's Memorandum Re Motion for Discovery at 1, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC); *see also* United States v. Rigmaiden, 844 F. Supp. 2d 982, 996–97 (D. Ariz. 2012). In an order addressing the defendant's motion to suppress, the District Court isolated certain facts related to the use of the cell site simulator, some of which were stipulated to by the government, including: (1) signals sent by the mobile tracking device to the aircard are signals that would not have been sent to the aircard in the normal course of Verizon's operation of its cell towers, (2) the tracking operation was a Fourth Amendment search and seizure, and (3) the mobile tracking device located the aircard precisely within Defendant's apartment. *Id.* at 14.

160. *See* Reporter's Transcript of Proceedings: Motion Hearing at 61, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC). During questioning by the judge, prosecutors explained:

We generally recommend [the] use [of] a search warrant at a point where we think that we're going to reasonably be interrogating a device within an area where there's a reasonable expectation of privacy, because we're — in going into that area where there's a reasonable expectation of privacy, we want to ensure a neutral and detached magistrate has made a finding of probable cause at that point.

However, it's the same type of data that we're getting in both missions, because based upon the transmissions back and forth to the cell tower is what we would use to direction-find the cellular device.

With a pen register order, we — because the pen register order doesn't include a finding of probable cause by a magistrate, we will generally restrict our use there to where we're not knowingly going into an area where there's a reasonable expectation of privacy . . .

. . . . It's not the nature of the data; it's the nature of the interest. And the — the nature of the — the legal interests, the Fourth Amendment — you know, where you have an expectation of privacy is where we would recommend using the search warrant as opposed to just a pen register order.

Id. (statement by Mr. Mazel). Indeed, the prosecutors recognized that *Kyllo v. United States*, 533 U.S. 27, 40 (2001), where the Supreme Court held that “[g]overnment use[] [of] a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion . . . is a ‘search’ and is presumptively unreasonable without a warrant,” would likely apply to the government's use of a StingRay to send a signal through walls of an apartment complex to locate Rigmaiden's data-card. *See*

If the DOJ anticipated *actual* Fourth Amendment issues with its use of a cell site simulator to locate Rigmaiden, obtaining a warrant was a reasonable, prudent precaution. The government's *arguendo* concession, however, is limited to the defendant's motion to suppress in the instant case. In other words, the DOJ did not take the position, *arguendo* or otherwise, that law enforcement use of a StingRay in any other criminal investigation would constitute a Fourth Amendment search. Moreover, the government seems to shift positions on whether it believes the Fourth Amendment was implicated during some part of the tracking operation to locate Rigmaiden: At first, it suggested that (notwithstanding the *arguendo* concession) the tracking operation, "as a factual matter . . . did not involve a search or seizure under the Fourth Amendment."¹⁶¹ Later during direct questioning from the court, however, the government explained that it seeks a warrant when a cell site simulator would locate an individual in a protected space.¹⁶² Ultimately, the 2011 Rigmaiden prosecution provides no clarity about the government's view on when or if the use of a Sting-Ray requires an agent to obtain a warrant.

Indeed, in late 2014, the Wall Street Journal revealed that the U.S. Marshals Service has equipped airplanes with IMSI catchers, which, since 2007, the agency has flown over cities to locate targets.¹⁶³ The IMSI catchers used in these tracking operations interact with and collect data from a vast number of innocent people's phones.¹⁶⁴ Moreover, such surveillance necessarily involves sending signals through the walls of homes and apartment buildings or penetrating briefcases, purses, and pockets in order to identify the phones contained within. While the Rigmaiden case presented a situation where law enforcement agents canvassed a neighborhood (and thus penetrated with electronic signals many of the homes within that neighborhood),¹⁶⁵ the U.S. Marshals' airplane-assisted surveillance operations involve surveillance on a much larger scale. Indeed, they send signals into huge numbers of Fourth Amendment protected spaces — potentially into every home, purse, and pocket in a city. Such dragnet surveillance operations therefore raise serious legal questions, even if authorized by a court.¹⁶⁶

Reporter's Transcript of Proceedings: Motion Hearing at 63, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC).

161. Government's Memorandum Re Motion for Discovery at 1 n.1, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC).

162. See Reporter's Transcript of Proceedings: Motion Hearing, *supra* note 160.

163. Devlin Barrett, *Americans' Cell Phones Targeted in Secret U.S. Spy Program*, WALL ST. J. (Nov. 13, 2014), <http://online.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533>.

164. *Id.*

165. See *supra* note 156 and accompanying discussion in main text.

166. See, e.g., [Proposed] Brief Amici Curiae in Support of Daniel Rigmaiden's Motion to Suppress at 17, United States v. Rigmaiden, 844 F. Supp. 2d 982, 989 (D. Ariz. 2012)

While it is impossible to discern all elements behind the DOJ's concession in Rigmaiden's case, one aspect of the rationale emerges in the discovery, pre-trial motion practice, and related hearings: The government considers cell site simulator technology to be a sensitive source and method that it believes will be rendered less effective if its capabilities were revealed publicly, as future targets of surveillance would learn how to thwart the surveillance method. Accordingly, prosecutors appear to have made strategic choices to limit the StingRay's exposure in the case, including an effort to protect the device's name.¹⁶⁷ In response to certain Rigmaiden discovery requests, for example, the government argued that the technology used to locate the Defendant's data-card and the manner in which the technology was employed was "sensitive law enforcement information"¹⁶⁸ subject to the qualified privilege recognized in *Roviaro* and *Van Horn*.¹⁶⁹ These cases essentially hold that the government can shield information about sensitive investigative techniques when a court determines that such disclosure would not be relevant or helpful to the defense or otherwise "essential to a fair determination of a cause . . .".¹⁷⁰

Hence, while Rigmaiden filed discovery motions to compel the government to disclose more information about the cell site simulator,¹⁷¹ the government's concession that the tracking operation was a Fourth Amendment search presumably foreclosed the relevance of at least some details about the StingRay and its use by law enforcement (thereby preventing their public disclosure).¹⁷² That the government

(No. 2:08-CR-008814-DGC) ECF No. 904-3, available at https://www.aclu.org/files/assets/rgmaiden_amicus.pdf ("That [S]ting[R]ays obtain information about third parties 'creates a serious risk that every warrant for [a StingRay] will become, in effect, a general warrant,' to search persons as to whom there is no probable cause.").

167. See Morrison Affidavit 2012, *supra* note 50, at 1 ("The actual make and model of the equipment used in any particular operation by the FBI is law enforcement sensitive, and pursuant to FBI policy, cannot be released to the general public.").

168. United States v. Rigmaiden, 844 F. Supp. 2d 982, 989 (D. Ariz. 2012).

169. *Id.* at 2 (citing *Roviaro v. United States*, 353 U.S. 53 (1957) and *United States v. Van Horn*, 789 F.2d 1492 (11th Cir. 1986)).

170. *Roviaro*, 353 U.S. at 60–61. With respect to government surveillance equipment, the defendant-target of electronic surveillance is not entitled to learn the location and type of equipment used by the government unless he can show sufficient need for such information. *Van Horn*, 789 F.2d 1492.

171. See Motion for Additional Discovery Due to Government Ignoring Defendant's Recent Discovery Requests, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC).

172. See Government's Memorandum Re Motion for Discovery at 2 n.3, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC) ("[T]o avoid disclosure of privileged information and simplify the Fourth Amendment analysis, the United States will concede, for purposes of any forthcoming motion to suppress, that the FBI located the aircard within Unit 1122 of the Domocilio Apartments."). With the "search" concession, the defendant is not harmed by any lack of disclosure — Rigmaiden gets to start from the position that the government's actions constituted a Fourth Amendment search and seizure and can then make all arguments that flow from that position, while the government can protect details that it believes could assist potential targets in evading detection by the technology in the future. See United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013

seeks to protect its use of cell site simulators as a sensitive source and method — to the extent that it will not even acknowledge the name of the specific equipment it uses¹⁷³ — is, however, consistent with a larger effort to prevent public disclosure of the technology and its capabilities. We address that effort next.

IV. THE GOVERNMENT'S SECRET STRINGRAY

Based on the recent public disclosure of an affidavit by Agent Bradley S. Morrison, the head of the FBI team responsible for the agency's use of StingRay and other cellular tracking technologies, we now know that the Rigmaiden prosecutors' efforts to shield details about the StingRay were part of a coordinated effort across federal, state, and local agencies to keep law enforcement use of this equipment secret.¹⁷⁴ Specifically, Agent Morrison asserts that "disclosure of what appears to be innocuous information about the use of cell site simulators would provide adversaries with critical information . . . necessary to develop defensive technology, modify their behaviors, and otherwise take countermeasures designed to thwart the use of this technology."¹⁷⁵ Agent Morrison warns that disclosure "could result in the FBI's inability to protect the public from terrorism and other criminal activity because, through public disclosures, this technology has been rendered essentially useless for future investigations."¹⁷⁶ Similar arguments have been made by a number of other local law enforcement agencies across the country.¹⁷⁷

In order to ensure the continued effectiveness of cellular surveillance equipment, the FBI, for the past ten years, has taken significant

WL 1932800, at *4 (D. Ariz. May 8, 2013) (finding "that Defendant was fully able to make his Fourth Amendment arguments in light of the extensive disclosures provided by the government, detailed stipulations of fact agreed to by the government, and information Defendant was able to obtain through his own investigations" and that "Defendant has been placed at no disadvantage by the government's withholding of sensitive law enforcement information"). Moreover, because law enforcement can generally switch to carrier-assisted surveillance once a cell site simulator is used to identify a target, it is feasible to exclude the use of IMSI catcher technology from the government's case-in-chief trial evidence. In other words, because an IMSI catcher may only be initially necessary to identify or locate a target (which may not be relevant proof of the charges at trial), additional tracking of a target, when needed, can be performed with carrier-assisted surveillance, which can be used as evidence at trial without fear of exposing a sensitive source or method. Indeed, in the Rigmaiden prosecution, the court noted that "the government ha[d] never suggested that it intend[ed] to present evidence about its location of the aircard [i.e., data-card] at trial." *United States v. Rigmaiden*, 844 F. Supp. 2d 982, 989 (D. Ariz. 2012).

173. See Morrison Affidavit 2012, *supra* note 50, at 1.

174. Affidavit of FBI Supervisory Special Agent Bradley S. Morrison, Chief, Tracking Technology Unit, Operation Technology Division in Quantico Division, at 2, Apr. 11, 2014, attachment to City's Verified Answer, *Hodai v. City of Tucson*, No. C20141225 (Ariz. Supr. Ct. Apr. 14, 2014) [hereinafter Morrison Affidavit 2014].

175. *Id.* at 1–2.

176. *Id.* at 2.

177. See discussion *infra* Part IV.C.

steps to prevent the disclosure of information about the specific electronic equipment and techniques used by law enforcement.¹⁷⁸ These steps include what might be characterized as a purposeful lack of disclosure to magistrate judges when seeking approval to use a cell site simulator in a criminal investigation, strict non-disclosure agreements with state and local law enforcement, and essentially across-the-board refusals to turn over documents relating to cell site simulators in response to Freedom of Information Act (“FOIA”) and public records requests. This Part describes the growth (one might even say the metastasis) of a discourse of secrecy regarding the StingRay’s use across various channels and levels of government.

A. Lack of Disclosure to the Courts

Despite the fact that U.S. government agencies have used cellular surveillance devices for more than twenty years, the 2012 Judge Owsley opinion is one of only two known published magistrate opinions to address law enforcement use of this technology. There are several possible reasons for this dearth of judicial analysis,¹⁷⁹ but one of the most troubling possibilities may be a lack of knowledge on the part of magistrate judges about the specific surveillance technique(s) they are authorizing, due to a lack of candidly presented explanatory information in the government’s applications. In one set of DOJ emails obtained by the American Civil Liberties Union (“ACLU”) through a Freedom of Information Act request, for example, a federal prosecutor in Northern California noted that “many agents are still using [cellular surveillance technology with a] pen register application [that] does not make [the use of that technology] explicit.”¹⁸⁰ Similarly, at a conference at Yale Law School in 2013, Judge Owsley indicated that federal agents may frequently obfuscate the planned use of a StingRay in authorization requests:

“I may have seen them before and not realized what it was, because what they do is present an application that looks essentially like a pen register application . . . So any magistrate judge that is typically looking at a lot of pen register applications and not

^{178.} *Id.*

^{179.} For a broader discussion of the reasons underlying the lack of judicial review of law enforcement use of the StingRay, see Pell & Soghoian, *supra* note 97.

^{180.} E-mail from Miranda Kane, Chief, Criminal Div., U.S. Attorneys Office Northern District Cal., to USACAN-Attorneys-Criminal, U.S. Dep’t of Justice (May 23, 2011, 11:55 PST), available at https://www.aclu.org/files/assets/doj_emails_on_stingray_requests.pdf.

paying a lot of attention to the details may be signing an application that is authorizing a Sting[R]ay.”¹⁸¹

In Tacoma, Washington, the local police have used StingRay surveillance devices since 2009 and insist that they only do so with approval from a judge.¹⁸² When asked about the police department’s statements in 2014, however, the presiding judge of the local Superior Court told a reporter that the StingRay equipment had not been mentioned in any warrant applications that he has seen. He also revealed that other judges in his court were similarly surprised to hear that the Tacoma police were using the technology, stating that “[the judges] had never heard of it.”¹⁸³

That prosecutors have not made this information clear to judges often appears to be an intentional action. In the Rigmaiden case, for example, prosecutors conceded that the government had not made a “full disclosure to the magistrate judge [who issued the original order authorizing the surveillance] with respect to the nature and operation of the [StingRay] device [used to locate Rigmaiden].”¹⁸⁴ The reason for that lack of candor, the DOJ later told the court, was “because of the sensitive nature of the device in terms of concerns out of the disclosure to third parties.”¹⁸⁵

Likewise, two notable events in Florida suggest an intentional effort by local law enforcement in that state to protect details about the use and functions of cellular surveillance technology. In a 2008 state case, police in Tallahassee used a StingRay to locate a victim’s stolen phone in the defendant’s apartment.¹⁸⁶ The police later revealed that they “did not want to obtain a search warrant because they did not

181. Ryan Gallagher, *Feds Accused of Hiding Information from Judges About Covert Cellphone Tracking Tool*, SLATE (Mar. 28, 2013), http://www.slate.com/blogs/future_tense/2013/03/28/stingray_surveillance_technology_used_without_proper_approval_report.html (quoting Judge Owsley); see also Jennifer Valentino-DeVries, *supra* note 26 (reporting that when prosecutor was asked by the judge how a court order or warrant could be obtained without telling the judge what technology was being used, the prosecutor responded “[i]t was standard practice, your honor”).

182. See Kate Martin, *Tacoma Police Admit to Cellphone Surveillance, Say They Don’t Keep Data*, NEWS TRIB. (Aug. 27, 2014), <http://www.thenewstribune.com/2014/08/27/3349396/tpd-responds-to-cell-phone-surveillance.html>.

183. *See id.*

184. Transcript of Motion To Suppress at 81, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC).

185. *Id.* at 81–82. The DOJ prosecutor also told the court, “Obviously, if the magistrate judge had had questions, he would have been entitled to answers, as any magistrate judge.” But when the court noted that it was “not the magistrate’s burden to ferret that [information] out while he’s got the agents in his office,” the prosecutor conceded that it was not. *Id.*

186. See Thomas v. Florida, 127 So. 3d 658, 660 n.2 (Fla. Dist. Ct. App. 2013); Nathan Freed Wessler, *VICTORY: Judge Releases Information About Police Use of Stingray Cell Phone Trackers*, ACLU FREE FUTURE BLOG (June 3, 2014), <https://www.aclu.org/blog-national-security-technology-and-liberty/victory-judge-releases-information-about-police-use> (a transcript from the trial, unsealed at the ACLU’s request, confirms that the police used a StingRay in the case).

want to reveal information about the technology they used to track the cell phone signal.”¹⁸⁷ In addition, an investigator with the technical operations unit of the Tallahassee Police Department testified: “[W]e prefer that alternate legal methods be used, so that we do not have to rely upon the equipment to establish probable cause, [in order to avoid] reveal[ing] the nature [of the surveillance] and methods [used].”¹⁸⁸

In Sarasota, police have enacted a policy of describing StingRay-derived intelligence in depositions and reports as “information from a confidential source regarding the location of the suspect . . .”¹⁸⁹ According to emails obtained by the ACLU, this policy, which was requested by the U.S. Marshals, is intended to shield information about the StingRay “so that [law enforcement] may continue to utilize this technology without the knowledge of the criminal element.”¹⁹⁰ Even if the aim of this policy is to keep the general public in the dark, by including misleading information in court documents, the police are also preventing the courts from having a true understanding of the electronic surveillance that is being conducted under their watch.

B. Secrecy via Regulatory Restrictions and Non-Disclosure Agreements

The Harris Corporation, which manufactures the StingRay, has submitted to the FCC applications for equipment-authorization licenses for each of its cellular-surveillance products.¹⁹¹ These applications include language provided by the FBI,¹⁹² which requests that the FCC impose specific conditions as part of regulatory agency’s authorization of Harris’ surveillance equipment:

187. *Thomas*, 127 So. 3d at 660.

188. *Id.*

189. See Joe Palazzolo, *Suspects in Florida Tracked by Cellphone “Stingray” Tool*, WALL ST. J. (June 20, 2014), <http://online.wsj.com/articles/suspects-in-florida-tracked-by-cellphone-stingray-tool-1403302294>.

190. See Kim Zetter, *Emails Show Feds Asking Florida Cops to Deceive Judges*, WIRED (June 19, 2014), <http://www.wired.com/2014/06/feds-told-cops-to-deceive-courts-about-stingray/>.

191. See Letter from Tania W. Hanna, Vice President of Legislative Affairs & Pub. Policy, Harris Corp., and Evan S. Morris, Counsel on Gov’t Relations, Harris Corp., to Marlene H. Dortch, Sec’y, FCC (Apr. 28, 2011), available at <http://files.cloudprivacy.net/Harris-FCC-confidential-request-1.pdf>; Letter from Tania W. Hanna, Vice President of Legislative Affairs & Pub. Policy, Harris Corp., and Evan S. Morris, Counsel on Gov’t Relations, Harris Corp., to Marlene H. Dortch, Sec’y, FCC (Mar. 21, 2011), available at <http://files.cloudprivacy.net/Harris-FCC-confidential-request-2.pdf>.

192. See E-mail from [redacted] to [redacted] (June 28, 2010, 10:56 EST), available at https://www.aclu.org/sites/default/files/assets/fcc_foia_harris_emails.pdf (“Harris has agreed with the [FBI] to request that the Commission condition its equipment authorization for the StingRay® product in order to address concerns over the proliferation of surreptitious law enforcement surveillance equipment.”).

(1) The marketing and sale of these devices shall be limited to federal/state/local public safety and law enforcement officials only; and

(2) State and local law enforcement agencies must [in] advance coordinate with the FBI the acquisition and use of the equipment authorized under this authorization.¹⁹³

The FCC submissions filed by Harris go on to explain that the purpose of the requested license restrictions is to ensure that use of the product be “limited to its intended use, operated only by federal, state, and local public safety officials” and to “address concerns regarding the proliferation of the equipment to unauthorized users.”¹⁹⁴

The FBI and DOJ are indeed coordinating the use of this technology, particularly through non-disclosure agreements, to limit disclosure to the public of information about cellular interception equipment. The FBI has entered into non-disclosure agreements with state and local enforcement partners.¹⁹⁵ The FBI argues that information shared by the federal government with states “concerning cell site simulator technology is considered homeland security information under the Homeland Security Act.”¹⁹⁶ The result of this classification is that cell site simulator information “remain[s] under the control of the [FBI] . . . ”¹⁹⁷

193. See Letter from Tania W. Hanna to Marlene H. Dortch (Apr. 28, 2011), *supra* note 191, at 2 (emphasis removed).

194. *Id.*

195. Morrison Affidavit 2014, *supra* note 174, at 2; see also Letter from Laura M. Laughlin, Special Agent in Charge, Seattle Div., Fed. Bureau of Investigation, to Donald Ramsdell, Chief of Police, Tacoma Police Dep’t (Dec. 19, 2012), available at http://s3.documentcloud.org/documents/1303020/nda_redacted.pdf (“Consistent with the conditions on the equipment authorization granted to Harris Corporation by the [FCC], state and local law enforcement agencies must coordinate with the [FBI] to complete this non-disclosure agreement prior to the acquisition and use of the equipment/technology authorized by the FCC authorization.”); Jennifer Portman, *FDLE Signed Stingray Non-Disclosure Deal*, TALLAHASSEE DEMOCRAT (Mar. 30, 2014), <http://www.tallahassee.com/article/20140330/NEWS01/303300011/FDLE-signed-Stingray-non-disclosure-deal> (“[The Florida Department of Law Enforcement] Commissioner Gerald Bailey said his agency had a non-disclosure agreement with the FBI to not reveal information about the technology . . . ”).

196. See Morrison Affidavit 2014, *supra* note 174, at 3 (explaining that 6 U.S.C. §§ 482(f)(1)(B)–(D) “defines homeland security information as information that relates to the ability to prevent, interdict, or disrupt terrorist activity; information that would improve the identification or investigation of a suspected terrorist or terrorist organization; or information that would improve the response to a terrorist act,” and asserting that “[c]ell site simulator technology meets all three criteria”).

197. *Id.* (relying on 6 U.S.C. § 482(e), which states that homeland security information “obtained by a State or local government from a Federal agency under this section shall remain under the control of the Federal agency, and a State or law authorizing or requiring such a government to disclose information shall not apply to such information”).

Local law enforcement agencies that have purchased Harris cellular interception technology have also signed non-disclosure agreements with the manufacturer of the equipment. The Harris non-disclosure agreement, which has been obtained by activists through Open Records Act requests,¹⁹⁸ specifically prohibits the disclosure of any information about the use of the company's products, including operations, missions, and investigative results that would be deemed a "release of technical data"¹⁹⁹

C. Federal FOIA and State Public Records Act Responses

Over the past few years, privacy advocates and journalists have submitted numerous open records requests to federal and state law enforcement agencies seeking any documents pertaining to StingRays and related surveillance technologies.²⁰⁰ The FBI, DOJ, and Department of Homeland Security ("DHS") have, collectively, located more than 24,000 pages of relevant documents, but have either withheld them in their entirety or released them in such a heavily redacted form that they reveal little to no useful information.²⁰¹

To justify their limited disclosure, the FBI, DOJ, and DHS claim a number of FOIA exemptions, including arguments that the production of documents would: (1) reveal classified information;

198. See Kim Zetter, *Police Contract with Spy Tool Maker Prohibits Talking About Device's Use*, WIRED (Mar. 4, 2014), <http://www.wired.com/2014/03/harris-stingray-nda/>.

199. See Complaint for Statutory Special Action & Injunctive Relief & Application for Order to Show Cause at Ex. B, Hodai v. City of Tucson, No. 14-1225 (Ariz. Super. Ct. Mar. 3, 2014), available at http://www.wired.com/images_blogs/threatlevel/2014/03/ACLU-Stingray-Complaint-Hodai-v-TPD.pdf.

200. See EPIC v. FBI — Stingray / Cell Site Simulator, ELEC. PRIVACY INFO. CTR., <https://epic.org/foia/fbi/stingray/> (last visited Dec. 18, 2014) (collecting documents released by DOJ relating to FBI's use of cell site simulators); Nathan Freed Wessler, *Police Hide Use of Cell Phone Tracker from Courts Because Manufacturer Asked*, ACLU FREE FUTURE BLOG (Mar. 3, 2014), <https://www.aclu.org/blog/national-security-technology-and-liberty/police-hide-use-cell-phone-tracker-courts-because> (reporting that "the ACLU and ACLU of Florida have teamed up . . . submitting public records requests to nearly 30 police and sheriffs' departments across Florida seeking information about their acquisition and use of [S]ting[R]ays").

201. See Letter from Kenneth Counter, Acting Chief, FOIA/PA Unit, Criminal Div., U.S. Dep't of Justice, to author, at 1 (July 17, 2013), available at <http://files.cloudprivacy.net/DOJ-Stingray-FOIA-5th-reply.pdf> ("As to the portion of your request for information concerning cell site simulators, digital analyzers, and similar mobile phone surveillance technology generally, the Criminal Division processed an additional five hundred and sixty-seven pages of responsive records, and has determined that these records are exempt from disclosure"); Letter from Tony R. Tucker, FOIA Officer, Office of Intelligence and Analysis, U.S. Dep't of Homeland Sec., to author, at 2 (Feb. 17, 2012), available at <http://files.cloudprivacy.net/DHS-OIA-Stingray-FOIA-reply.pdf> ("[T]he Office of Intelligence and Analysis located 1085 pages. Of these total pages, 1046 must be withheld in their entirety"); Fourth Decl. of David M. Hardy at 9, EPIC v. FBI, No. 12-0667 (D.D.C. Oct. 1, 2013), available at <https://epic.org/foia/fbi/stingray/Fourth-Hardy-Declaration.pdf> ("The FBI reviewed and processed a total of 22,982 pages of responsive material, of which, 4,377 pages were released in full or in part, and 18,605 were withheld in full.").

(2) disclose techniques and procedures for law enforcement investigation; and (3) reasonably be expected to risk circumvention of the law.²⁰²

Consistent with the government's FOIA positions, the prosecutor in the Rigmaiden case stated that "the sensitive nature of the equipment [used to locate the defendant] goes beyond issues of law enforcement to matters of national security," as "some of this equipment is not only used in the law enforcement realm, it's used in the national security realm."²⁰³

Local law enforcement agencies have similarly been evasive. In response to queries from journalists working with USA Today, thirty-six police agencies refused to confirm whether or not they have even used cellular surveillance equipment.²⁰⁴ Several state and local law enforcement agencies have also refused to disclose records related to the use of this technology, arguing that "criminals or terrorists could use the information to thwart important crime-fighting and surveillance techniques."²⁰⁵ In sum, these federal and state responses, while perhaps lawful responses to FOIA and Public Records Act requests, illustrate a much larger secrecy policy and narrative: Law enforcement agencies believe that the existence, capabilities, and limitations of this cellular interception technology are secret and that the secrecy must persist in order for the technology to continue to be an effective law enforcement surveillance tool.²⁰⁶

V. A SECRET NO MORE

While U.S. government agencies shroud cellular surveillance technology in secrecy, in several other countries this same technology is subject to legislative oversight, judicial review, and, thus, public discourse. In still other countries, the unregulated nature of this technology has led to a chaotic situation where thousands of untracked

202. See Letter from Kenneth Courier to author, *supra* note 201, at 2; Letter from Tony R. Tucker to author, *supra* 201, at 1; Decl. of Hardy, *supra* note 201, at 12.

203. Status Conference, Reporter's Partial Tr. of Proceedings at 14, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC).

204. See Kelly, *supra* note 21.

205. *Id.*

206. See Taylor Killough, *State Police Acknowledge Use of Cell Phone Tracking Device*, IND. PUB. MEDIA (Dec. 12, 2013), <http://indianapublicmedia.org/news/state-police-respond-investigation-tracking-device-59918/> ("Indiana State Police Captain Dave Bursten said in a statement the department is working well within the bounds of the law Bursten won't say exactly how the [StingRay] technology is used, because he says it would be 'like a football team giving up their playbook.'"); Nathan Freed Wessler, *Local Police in Florida Acting Like They're the CIA (But They're Not)*, ACLU FREE FUTURE BLOG (Mar. 25, 2014), <https://www.aclu.org/blog/national-security-technology-and-liberty/local-police-florida-acting-theyre-cia-theyre-not> (describing a "Glomar" response from the Sunrise, Florida Police Department, neither confirming nor denying the existence of documents related to the purchase of Harris cellular surveillance technology).

interception devices are in use, many by non-governmental actors. Moreover, skilled hobbyists using readily available off-the-shelf components can now build homemade cellular interception devices for a tiny fraction of the cost law enforcement and security agencies pay for Harris' StingRay. In detailing the existence of an open, global market for cellular interception technology, this Part dispels any rational notion that cellular interception technology is or can be kept secret.

A. The Globalization of Cellular Interception Technology

The first generation of cellular interception technology was introduced during the early-1990s.²⁰⁷ Generally, it was expensive and sold by a few defense contractors only to major global powers. Today, however, both passive and active surveillance devices are much cheaper and available on the open market from surveillance vendors in the Middle East, South America, and Asia.²⁰⁸ The major powers thus no longer enjoy a monopoly over cellular phone surveillance. It has become, for better or for worse, irreversibly globalized.

Defense contractors sold the first phone interception devices to world powers such as Germany,²⁰⁹ the United Kingdom,²¹⁰ the United States,²¹¹ and most likely, Russia and Israel.²¹² Over the past three decades, the market for this technology has steadily expanded and the price of the technology has, consequently, dropped.²¹³ Manufacturers

207. See *supra* Part II.A.

208. See *infra* notes 214–221.

209. Cf. *supra* notes 59–60.

210. Cf. MMI Research Ltd v. Cellxion Ltd & Ors. [2009] EWHC (Pat) 418, [78] (Eng.), available at <http://www.bailii.org/ew/cases/EWHC/Patents/2009/418.html> (describing the demonstration of the GSM-X interception device to potential government clients in 1999 by MMI Research Ltd, a British surveillance equipment manufacturer).

211. See *supra* Part II.A.

212. Given the active, sophisticated espionage efforts of the Russian and Israeli intelligence agencies, it is almost certainly the case that companies in these countries were early manufacturers of this technology too. Today, there are many large companies in Israel and Russia that actively export cellular surveillance equipment around the world. For Israel, see *Cellular Interception*, ABILITY COMPUTERS & SOFTWARE INDUS. LTD., <http://www.interceptors.com/intercept-solutions/Cellular-Interception.html> (last visited Dec. 18, 2014); *Septier Guardian Tactical Systems*, SEPTIER COMM'C'N LTD., <http://www.septier.com/93.html> (last visited Dec. 18, 2014) (describing several cellular surveillance products). For Russia, see Andrei Soldatov & Irina Borogan, *5 Russian-Made Surveillance Technologies Used in the West*, WIRED: DANGER ROOM (May 10, 2013), <http://www.wired.com/dangerroom/2013/05/russian-surveillance-technologies> (The Discovery Telecom Technologies system “masquerades as a cell phone tower, sucking in nearby signals and allowing the device’s operator to surreptitiously listen and record. Established in Moscow, the firm . . . boasts on its Russian website about including the Kremlin and the FSB among its clients.”).

213. Compare Kelly, *supra* note 21 (“The cell-tracking systems [purchased by U.S. law enforcement agencies] cost as much as \$400,000, depending on when they were bought and what add-ons they have. The latest upgrade, code-named ‘Hailstorm,’ is spurring a wave of upgrade requests.”), with Letter from Alan M. Grayson to Tom Wheeler, *supra* note 29

and resellers now include firms in Argentina,²¹⁴ Bangladesh,²¹⁵ Canada,²¹⁶ China²¹⁷, India,²¹⁸ Malaysia,²¹⁹ the Netherlands,²²⁰ Pakistan,²²¹ Switzerland,²²² Taiwan,²²³ and Turkey,²²⁴ who, in addition to selling devices to their own governments, actively seek out other government (and, perhaps, non-government) customers as part of the five-billion dollar global market for commercial surveillance technology.²²⁵ Indeed, cellular interception devices are reportedly among the “bestselling items” exhibited at surveillance industry trade shows.²²⁶

Although several governments have employed phone interception technology, the extent to which it has been used responsibly and disclosed to the public varies considerably by country. Germany is perhaps the most open and transparent country regarding its use of active interception technology. The use of such devices by German govern-

(citing one online merchant in China, “IMSI catchers can apparently ‘be bought openly’ from online retailers for as little as \$1800”).

214. See *Products*, SOLUCIONES-PARA-GOBIERNO.COM, <http://solucionesparagobierno.com/english/productos.html> (last visited Dec. 18, 2014).

215. *Passive GSM (Dual Band) / CDMA Monitoring System*, ALIBABA.COM, http://www.alibaba.com/product-detail/Passive-GSM-Dual-Band-CDMA-Monitoring_103809673.html (last visited Oct. 7, 2014).

216. *GSS Pro-A GSM Interceptor*, GLOBAL SEC. SOLUTIONS, <http://www.global-security-solutions.com/ProAInterceptor.html> (last visited Dec. 18, 2014).

217. See Letter from Alan M. Grayson to Tom Wheeler, *supra* note 29.

218. See *Cellular Monitoring*, SHOGHI COMM'S LTD., <http://www.shoghicom.com/cellular-monitoring.php> (last visited Dec. 18, 2014) (describing the cellular intercept products available for sale); *IMSI Catcher*, TRADEIM.COM, <http://www.tradeim.com/company.html?method=product&productCode=8693695> (last visited Dec. 18, 2014).

219. See *GSM Interceptor*, INFRALANGIT, <http://infralangit.com/gsm-interceptor/> (last visited Oct. 7, 2014).

220. See *GSM Interception System*, PI PRODUCTS, <http://www.pi-products.nl/pi-products/PDF/Communication%20Monitoring/Monitoring%20GSM%20networks/gsm%20interception%20system.pdf> (last visited Dec. 18, 2014).

221. See *GSM Interceptor Scanner*, WEIKU.COM, http://www.weiku.com/products/18444632/GSM_interceptor_Scanner.html (last visited Dec. 18, 2014).

222. See *Catalogue*, NEOSOFT AG, <https://www.documentcloud.org/documents/810502-945-neosoft-catalogue.html> (last visited Dec. 18, 2014).

223. See *IMSI Catcher*, ALIBABA.COM, http://www.alibaba.com/product-detail/IMSI-catcher_135958750.html (last visited Dec. 18, 2014) (listing the PKI 1640 for \$1800 per unit, which can “catch all active UMTS mobile phones in your proximity” and capture and store data “such as IMSI, IMEI, TMSI”).

224. See *Interceptor GSM A5-1 A5-2 ve 3*, ALIBABA.COM, http://www.alibaba.com/product-free/126383443/interceptor_gsm_A5_1_A5_2.html (last visited Dec. 18, 2014).

225. See Nicole Perlroth, *Software Meant To Fight Crime Is Used To Spy on Dissidents*, N.Y. TIMES (Aug. 30, 2012), <http://www.nytimes.com/2012/08/31/technology/finspy-software-is-tracking-political-dissidents.html> (“The market for such technologies has grown to \$5 billion a year from ‘nothing 10 years ago,’ said Jerry Lucas, president of TeleStrategies, the company behind ISS World, an annual surveillance show . . .”).

226. See Stefan Kreml, *28C3: New Attacks on GSM Mobiles and Security Measures Shown*, H OPEN (Dec. 28, 2011), <http://www.h-online.com/open/news/item/28C3-New-attacks-on-GSM-mobiles-and-security-measures-shown-1401668.html> (noting that Karsten Nohl of Security Research Labs reported, after a trip to the ISS trade fair, “that the bestselling items in the espionage community at present are devices for monitoring mobile phones, such as IMSI catchers”).

ment agencies is specifically regulated by several statutes,²²⁷ which mandate, among other things, that statistical data describing their use be aggregated and published by the German Parliament.²²⁸ Moreover, there have been several formal parliamentary answers to questions submitted by the public regarding the use of IMSI catchers,²²⁹ as well as a decision from the German Constitutional Court permitting their use.²³⁰

The way cellular interception devices are regulated in Norway is also noteworthy because of the degree to which the legislation permitting their use explicitly acknowledges the dragnet nature of the technology. The relevant law permits temporary mass monitoring of all calls in a specific area during which police listen to all phone calls in the suspect's community, regardless of whether the intercepted parties have any connection with the case under investigation.²³¹

It is in India, however, where cell phone interception technology has had the most high profile and politically destabilizing impact. Beginning in 2005, agencies in the Indian national government imported passive cellular interception systems.²³² In 2010, audio recordings and

227. See Bundesverfassungsschutzgesetz [BVerfSchG] [Federal Constitution Protection Act], Dec. 20, 1990, as amended, BGBl. I at 2499, § 9, para. 4 (Ger.), available at http://www.gesetze-im-internet.de/bverfschg/_9.html. See generally MARKUS RAU, TERRORISM AS A CHALLENGE FOR NATIONAL AND INTERNATIONAL SECURITY: SECURITY VS. LIBERTY? 311 (Christian Walter et al. eds., 2004).

228. See DEUTSCHER BUNDESTAG DRUCKSACHEN, Bericht, Mar. 14, 2013, BT 17/12774 (Ger.) (2011 data), available at <http://dip21.bundestag.de/dip21/btd/17/127/1712774.pdf>; DEUTSCHER BUNDESTAG DRUCKSACHEN, Bericht, Feb. 10, 2012, BT 17/8638 (Ger.) (2010 data), available at <http://dipbt.bundestag.de/dip21/btd/17/086/1708638.pdf>.

229. See DEUTSCHER BUNDESTAG DRUCKSACHEN, Antwort, Sep. 10, 2001, BT 14/6885 (Ger.) (2001 response), available at <http://dip21.bundestag.de/dip21/btd/14/068/1406885.pdf>; DEUTSCHER BUNDESTAG DRUCKSACHEN, Antwort, Nov. 9, 2011, BT 17/7652 (Ger.) (2011 response), available at <http://dipbt.bundestag.de/dip21/btd/17/076/1707652.pdf>.

230. See Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Aug. 22, 2006, ENTSCHEIDUNGEN DES BUNDESVERFASSUNGSGERICHTS [BVERFG] 2 BVR 1345/03 (Ger.), available at http://www.bundesverfassungsgericht.de/entscheidungen/rk20060822_2bvr134503.html; EURO. COMMISSION ANN. REP. OF ART. 29 WORKING PARTY ON DATA PROTECTION at 45–46 (2006), available at http://www.akvorrat.at/sites/default/files/VDS_Materialien/Art%2029%20WP%2010th_annual_report_en.pdf (English language summary of the ruling by the Federal Constitutional Court on 22 August 2006 on the use of the IMSI-catchers in criminal proceedings).

231. See Justis- og beredskapsdepartementet, *Om lov om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet)* [On Amendments to the Criminal Procedure Act and the Police Act (covert audio surveillance and the use of coercive measures to prevent serious crime)], Ot.prp. nr. 60 (2004–2005) (Nor.), available at [232. Saikat Datta, *A Fox on a Fishing Expedition*, OUTLOOK INDIA \(May 3, 2010\), <http://www.outlookindia.com/article.aspx?265192> \(“India began purchasing the off-the-air](https://www.regjeringen.no/nb/dokumenter/otprp-nr-60-2004-2005-/id398192/?docId=OTP200420050060000DDDEPIS&q=&navchap=1&ch=8#KAP8-5-3; Per Anders Johansen, Politiet og Forsvaret kan ta kontroll over mobilnettet [The Police and the Military to Take Control of Cellular], AFTENPOSTEN (Sept. 21, 2014), http://www.aftenposten.no/nyheter/riks/Politiet-og-Forsvaret-kan-ta-kontroll-over-mobilnettet-7713131.html.</p>
</div>
<div data-bbox=)

written transcripts of politicians' calls that were intercepted with these devices were leaked to the press, leading to a huge scandal.²³³ Media reports revealed that, just two years after the devices were first purchased by the national intelligence agency, they were used to monitor the phone calls of senior politicians, including opposition leaders.²³⁴

An anonymous intelligence official told one Indian newspaper that cellular interception technology enabled them to "dig into everyone's life . . . be it political and corporate leaders, journalists, social activists or bureaucrats. We can track anyone we choose."²³⁵ Another anonymous official stressed that the principal strategic advantage of the technology is that it:

"works on deniability . . . It can be deployed anywhere. We don't need to show any [formal legal] authorisation [sic] since we're not tapping a phone number at the [wireless carrier's office] but intercepting signals between the phone and the cellphone tower . . . [W]e can [always] . . . erase the conversation. No one gets to know."²³⁶

In addition to the high-profile use of the devices against politicians, news reports also reveal that the equipment has been used to spy on business leaders, journalists, and families of politicians.²³⁷ One intelligence official stated that "the [surveillance] machine intercepted calls of the wives of [members of parliament] discussing personal and sensitive matters, corporate leaders seeking private liaisons in hotels . . . Most of the corporate calls at night are for sex."²³⁸ Given the

GSM/CDMA monitoring systems around 2005–06, and the first interception of a mobile phone conversation using the system was carried out by the NTRO on January 7, 2006, in New Delhi."); Harish Gupta & Nivedita Mookerji, *Private Hand in Phone Tapping Worries Manmohan Singh; Probe Ordered*, DNA INDIA (Dec. 14, 2010), <http://www.dnaindia.com/india/1481036/report-private-hand-in-phone-tapping-worries-manmohan-singh-probe-ordered> ("These machines were first introduced in the NTRO, a top government technical surveillance agency directly under the PM, sometime in 2005.").

233. See Saikat Datta, *Bootleg Tapes: The Rulers Who Listen*, OUTLOOK INDIA (May 10, 2010), <http://www.outlookindia.com/story.aspx?sid=4&aid=265272> (describing various conversations recorded using the surveillance technology and provided to the press).

234. Saikat Datta, *We, The Eavesdropped*, OUTLOOK INDIA (May 3, 2010), <http://www.outlookindia.com/article.aspx?265191> (describing NTRO's interception of conversations of various politicians).

235. Datta, *supra* note 232 (internal quotation marks omitted).

236. Datta, *supra* note 234.

237. See "Give Us Legal Immunity, We'd Be Happy To Provide Proof of Illegal Tapping," OUTLOOK INDIA (May 10, 2012), <http://www.outlookindia.com/article/Give-Us-Legal-Immunity-Wed-Be-Happy-To-Provide-Proof-Of-Illegal-Tapping/265273> (interview with several anonymous senior intelligence officials confirming that "the machine records lots and lots of calls of ministers, MPs, bureaucrats, lobbyists, arms dealers, editors and journalists").

238. *Id.*

sensitive nature of the communications intercepted using these devices, another official described the problem in economic terms: “When an officer on a salary of [130 dollars] a month has pretty much unrestricted access to this kind of technology . . . things will go wrong, and have gone wrong.”²³⁹

A subsequent official investigation revealed that lax customs rules permitted unregulated importation and purchase of the interception technology. Government officials later acknowledged that over forty different makes and models of cellular interception technology had been imported from over a dozen vendors.²⁴⁰ The devices had been purchased by numerous national governmental agencies, state governments,²⁴¹ and the military.²⁴² Officials estimate that thousands of cellular interception devices have been imported,²⁴³ and that hundreds are in the possession of private parties, such as corporations and detective agencies.²⁴⁴

By late 2010, senior Indian government officials acknowledged that legal prohibitions on the private purchase and use of cellular in-

239. Praveen Swami, *The Government’s Listening to Us*, HINDU (Dec. 1, 2011), <http://www.thehindu.com/news/national/the-governments-listening-to-us/article2678501.ece> (internal quotation marks omitted).

240. Sudhi Ranjan Sen, *Phone-Tapping: Telecom Firms Under Scanner for Eavesdropping?*, NDTV (Sept. 25, 2012), <http://www.ndtv.com/article/india/phone-tapping-telecom-firms-under-scanner-for-eavesdropping-271661> (“But the bad news is, of the 45-odd suspected machines identified, the government doesn’t have the address of importers of as many as 24 machines.”); Sanjay Singh, *Government Hunts for Elusive Bug: DoT Wants Snooping and Listening Devices Within Private Sector Surrendered*, DAILY MAIL (Nov. 27, 2012), <http://www.dailymail.co.uk/indiahome/indianews/article-2239422/Government-hunts-elusive-bug-DoT-wants-snooping-listening-devices-private-sector-surrendered.html> (“Despite the ban on the free import of phone interceptors, these gadgets manufactured in Israel, the UK, France and China continue to be smuggled into the country through Nepal and Bangladesh. It is believed that there [are] as many as 45 different variants of these machines . . . floating around in India.”).

241. See Hitender Rao, *“Off-Air” Tapping: MHA Wants States To Surrender Devices*, HINDUSTAN TIMES (June 29, 2011), <http://www.hindustantimes.com/Punjab/Chandigarh/Off-air-tapping-MHA-wants-states-to-surrender-devices/Article1-715297.aspx> (describing their use by Haryana state government).

242. Ritu Sarin, *MHA Poses Fresh Queries About Army Interceptors*, INDIAN EXPRESS (Nov. 4, 2012), <http://www.indianexpress.com/news/mha-poses-fresh-queries-about-army-interceptors/1026444/> (describing the home ministry’s audit of army’s deployment of off-air interception equipment).

243. *“Invisible” Phone Taps: Is the Govt Worried?*, NDTV (Mar. 2, 2012), <http://www.ndtv.com/article/india/invisible-phone-taps-is-the-govt-worried-181763> (“My inquiries with the government authorities have revealed that during the last three years, 1100 GSM monitoring interceptors were imported’”); Ritu Sarin, *States Begin To Surrender Off-Air Phone Snooping Equipment*, FIN. EXPRESS (June 5, 2012), <http://www.financialexpress.com/news/states-begin-to-surrender-offair-phone-snooping-equipment/957859> (stating that as many as 73,000 dual-use devices had been imported, and some could be employed for innocuous purposes).

244. Singh, *supra* note 240 (estimating that, between the government and private sector, 2000 off-air surveillance devices imported in 2000); *“Invisible” Phone Taps*, *supra* note 243 (“Sources in the Telecom Department and Home Ministry suspect that among the buyers are large corporate houses, politically-aligned detective agencies and even government agencies who are not authorised to carry out cellphone taps.”).

terception technology would not protect the privacy of citizens' communications. India's prime minister stressed the need to "look for solutions through technology to prevent access of telephone conversations . . ."²⁴⁵ Another senior government official acknowledged that the secrecy of government communications was threatened by the private use of interception technology.²⁴⁶

B. The Democratization of Cellular Interception Technology

The effective monopoly over cellular interception technology long enjoyed by governments was largely due to the cost.²⁴⁷ Devices retail for as much as \$400,000,²⁴⁸ depending on the features — far too expensive for the average person, but a relatively small sum for the military, intelligence community, and even many law enforcement agencies. Part of the high price reflected the difficulty and significant capital investment required to design and manufacture the StingRay's sophisticated radio equipment. As a result, hobbyists and researchers without large budgets were simply unable to develop cellular communications technology. This cost barrier no longer exists. Moreover, a set of free software tools has been developed by a community of researchers and hobbyists that has lowered the skill level necessary to tinker with cellular communication technology. Consequently, as the cost and ease of developing cellular interception technology has declined, the longstanding nation-state monopoly has vanished. Surveillance has become democratized and, correspondingly, the motives for surveillance have multiplied. The next elements of this Part will describe briefly how innovations in radio technology have enabled researchers and hobbyists without large budgets to develop their own cellular interception devices.

245. Manoj Mitta, *Off-the-Air Taps a Bigger Worry: PM*, TIMES OF INDIA (Dec. 15, 2010), http://articles.timesofindia.indiatimes.com/2010-12-15/india/28230420_1_cabinet-secretary-telephone-interception-national-technical-research-organization (internal quotation marks omitted).

246. Singh, *supra* 240 ("A[n] [anonymous] top government official . . . said a large number of corporate houses have small offices in and around central Delhi areas in the proximity of important government buildings. 'Officials working in key positions under various ministries and sensitive departments are, therefore, vulnerable to phone tapping . . .'"').

247. See Ralf-Philipp Weinmann, *Baseband Attacks: Remote Exploitation of Memory Corruptions in Cellular Protocol Stacks*, 6TH USENIX WORKSHOP ON OFFENSIVE TECHNOLOGIES (Aug. 6, 2012), <https://www.usenix.org/system/files/conference/woot12/woot12-final24.pdf> ("In the past, spoofing a GSM network required a significant investment, which limited the set of possible attackers . . . Open-source solutions such as OpenBTS allow anyone to run their own GSM network at a fraction of the cost of carrier-grade equipment, using a simple and cheap software-defined radio.").

248. Kelly, *supra* note 21 ("The cell-tracking systems cost as much as \$400,000, depending on when they were bought and what add-ons they have. The latest upgrade, code-named 'Hailstorm,' is spurring a wave of upgrade requests.").

1. Low Cost Software-Defined Radio-Based Active Interception

Hobbyists can now build their own active surveillance devices with readily available electronic components currently costing approximately \$700.²⁴⁹ The ability to create such low-cost cellular interception devices is due to technological innovations that have lowered both the costs and skill-level necessary to develop radio technology. Specifically, a revolution in *software-defined radio* technology during the past decade has eliminated the longstanding technical barriers that prevented researchers and hobbyists from being able to experiment freely with large swaths of the radio spectrum. Software-defined radios are flexible hardware platforms that, when combined with specific software, “can change the frequency range, modulation type or output power of a radio device without making changes to hardware components.”²⁵⁰ Instead of having to create expensive new microchips (i.e., *hardware*) for each new radio technology — such as GPS navigation, Bluetooth, and High Definition TV — a low cost software-defined radio, combined with specific software for a particular application, can now be used instead.

The development of software-defined radio has reduced earlier barriers of access to radio technology, thus enabling tinkering by researchers of varied skill-levels. This access has allowed developers to create, for example, free software capable of operating a cellular network. Indeed, OpenBTS is a popular open source, cellular base station software suite,²⁵¹ which is designed to work with low cost (currently around \$700) software-defined radios.²⁵² The existence of OpenBTS and similar software has thus significantly reduced the cost of creating and running a cellular network and brought it within the reach of non-profit organizations, rural communities, and hobbyists.²⁵³

249. Taylor Killian, *SDR Showdown: HackRF vs. bladeRF vs. USRP*, TAYLOR KILLIAN (Aug. 7, 2013), <http://www.taylorkillian.com/2013/08/sdr-showdown-hackrf-vs-bladerf-vs-usrp.html> (describing a specifications for a number of hobby radios ranging in price from \$300 to \$1100).

250. See Press Release, Federal Commc’n, FCC Approves First Software Defined Radio (Nov. 19, 2004), available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-254463A1.pdf.

251. See *id.*; Harvind Samra, *The OpenBTS Project — An Open-Source GSM Base Station*, LWN.NET (Sept. 4, 2008), <http://lwn.net/Articles/296949/>.

252. See generally Killian, *supra* note 249 (comparing various software-defined radios).

253. Volunteers using OpenBTS have operated free cellular networks at Burning Man, a popular festival held in the Nevada desert, as well as at several computer security conferences. See Davis Burgess, *Burning Man 2011 — Yes We Were There.*, OPENBTS CHRONICLES (Sept. 6, 2011), <http://openbts.blogspot.com/2011/09/burning-man-2011-yes-we-were-there.html>; Dan Goodin, *At DEFCON, Hackers Get Their Own Private Cell Network: Ninja Tel*, ARS TECHNICA (July 28, 2012), <http://arstechnica.com/security/2012/07/ninja-tel-hacker-phone-network/>. Non-profit organizations have also used OpenBTS to provide cellular service to remote communities in developing countries. See Stephen Lawson, *Cell System Used in Antarctica May Help To Cover the Plains*, COMPUTERWORLD (Mar. 26, 2013), <http://www.computerworld.com.au/article/457350/>

Once hobbyists and researchers were able to build and operate their own cellular networks with open source software, it was only a matter of time before the software was modified such that it could masquerade as a legitimate wireless carrier's network with the capacity to intercept calls.²⁵⁴ Indeed, a security researcher did just that in 2010—in front of an audience at the DEF CON security conference—using a laptop running OpenBTS that had been configured to masquerade as AT&T's network, thereby allowing the researcher to intercept outgoing calls from the phones of audience members.²⁵⁵ Although the hardware and software necessary to build an OpenBTS-based cellular interception device is readily available, doing so still takes a significant amount of technical expertise. As is often the case with difficult-to-exploit security vulnerabilities, however, the usability barriers eventually shrink with the development of easy-to-use software.²⁵⁶ Once these usability barriers are removed, low-cost interception tools will be available to anyone with a motive or interest in listening to the calls of others.²⁵⁷

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 48 of 76

cell_system_used_antarctica_may_help_cover_plains/ ("One [OpenBTS] network[] serves a remote village in Papua, Indonesia, that can only reach the outside world via satellite. Residents of the village can now call and text each other and exchange text messages with the rest of the world using an OpenBTS network linked to a satellite transceiver."); Jacqueline Mpala & Gertjan van Stam, *Open BTS, a GSM Experiment in Rural Zambia*, AFRICOMM 2012: FOURTH INTERNATIONAL IEEE EAI CONFERENCE ON E-INFRASTRUCTURE AND E-SERVICES FOR DEVELOPING COUNTRIES (Nov. 2012), http://www.academia.edu/2122498/Open_BTS_a_GSM_experiment_in_rural_Zambia.

254. David Burgess, the co-creator of OpenBTS who has previously written software for commercial IMSI catchers has observed, "Nearly any BTS or BTS simulator can be used as the basis of an IMSI-catcher." David Burgess, *Some Comments on IMSI-Catchers*, OPENBTS CHRONICLES (May 6, 2009), <http://openbts.blogspot.com/2009/04/some-comments-on-imsi-catchers.html>.

255. DEFCONConference, *DEF CON 18 — Chris Paget — Practical Cellphone Spying* at 23:36, YOUTUBE (Nov. 8, 2013), <https://www.youtube.com/watch?v=fQSu9cBaojc> (recording of Chris Paget's talk at DEF CON 18 on July 31, 2010).

256. See Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. 1327, 1399 (2008) ("[S]ometimes Superusers empower ordinary users with easy-to-use [hacking] software."); Kate Murphy, *New Hacking Tools Pose Bigger Threats to Wi-Fi Users*, N.Y. TIMES, Feb. 17, 2011, at B8, available at <http://www.nytimes.com/2011/02/17/technology/personaltech/17basics.html> ("Until recently, only determined and knowledgeable hackers . . . could spy while you used your laptop or smartphone at Wi-Fi hot spots. But a free program called Firesheep . . . has made it simple to see what other users of an unsecured Wi-Fi network are doing and then [impersonate] them [on] sites they visited.").

257. For example, one German graduate student created a more usable IMSI catcher based on OpenBTS for his master's thesis. See Dennis Wehrle, *Open Source IMSI-Catcher* (Oct. 28, 2009) (unpublished Masters thesis, University of Freiburg), available at https://github.com/tom-mayer/imsi-catcher-detection/blob/master/Papers/Thesis%20KS/Ausarbeitung-Dennis_Wehrle.pdf.

2. Lower Cost Active Interception with Femtocells

Technically skilled hobbyists and researchers can create even cheaper, more organic active interception technology using a “femtocell,” a device that extends the carrier’s own network. Wireless providers have augmented their networks with devices known as microcells, picocells, and femtocells to provide better cellular service to their customers and to fill in “dead spots” where there is poor reception.²⁵⁸ These small cellular base stations, which customers can install in their homes or offices, provide cellular connectivity to nearby phones within tens or hundreds of meters.²⁵⁹ Indeed, these devices are already widely deployed in the U.S.—Sprint and AT&T each have distributed more than 1 million femtocells.²⁶⁰

From the perspective of a cellular phone, a femtocell is a normal cellular base station, indistinguishable from a carrier’s base station installed at a cell tower. Because they must be installed in consumers’ homes, the devices, unlike traditional cell towers, are small, easy to use, and inexpensive. They are typically sold for less than \$100²⁶¹ and often given away for free to consumers who complain about poor service.²⁶² The femtocell was, therefore, a naturally attractive target for security researchers.²⁶³ The devices are widely available, affordable,

258. Microcells, picocells, and femtocells all employ the same underlying technology. The difference between these products is their effective range. Microcells, picocells, and femtocells provide service to areas of 200m–2km, 4m–200m, and 10m, respectively. See Dimitris Mavrakis, *Do We Really Need Femto Cells?*, VISIONMOBILE (Dec. 1, 2007), <http://www.visionmobile.com/blog/2007/12/do-we-really-need-femto-cells/>.

259. *See id.*

260. INFORMA TELECOMS & MEDIA, SMALL CELL MARKET STATUS 3 (Feb. 2013) (“Sprint’s deployment reached 1 million units as of October 2012 and analysts estimate that AT&T’s deployment has reached similar numbers.”); Sue Marek, *Sprint’s Femtocell Tally Tops 1M*, FIERCEWIRELESS (Oct. 24, 2012), <http://www.fiercewireless.com/story/sprints-femtocell-tally-tops-1m/2012-10-24>.

261. *See* Roger Cheng, *A Cell Tower of Your Very Own*, WALL ST. J. (July 8, 2010), <http://online.wsj.com/article/SB10001424052748703636404575353153350315146.html> (“AT&T has been rolling out the 3G Microcell, which provides a full signal to a surrounding area of up to 5,000 square feet, as an answer for customers in areas with poor reception. The price is \$149.99. Verizon Wireless’s femtocell, the ‘Network Extender,’ is priced at \$99.99 . . . ”).

262. *See* Eric Savitz, *Sprint Giving Femtocells to Some Customers; Will VZ, T Follow?*, BARRON’S (Sept. 15, 2010), <http://blogs.barrons.com/techtraderdaily/2010/09/15/sprint-giving-femtocells-to-some-customers-will-vz-t-follow/>.

263. *See generally* Ravishankar Borgaonkar, Kevin Redon & Jean-Pierre Seifert, *Security Analysis of a Femtocell Device*, in PROCEEDINGS OF THE 4TH INTERNATIONAL CONFERENCE ON SECURITY OF INFORMATION AND NETWORKS 95–102 (Nov. 14–19, 2011); Nico Golde, Kevin Redon & Ravishankar Borgaonkar, *Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunication*, in PROCEEDINGS OF THE 19TH ANNUAL NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM (Feb. 2012); David Malone, Darren F. Kavanagh & Niall R. Murphy, *Rogue Femtocell Owners: How Mallory Can Monitor My Devices*, 5TH IEEE INTERNATIONAL TRAFFIC MONITORING AND ANALYSIS WORKSHOP (Apr. 19, 2013); *The Vodafone Access Gateway / UMTS FemtoCell / Vodafone Sure Signal*, THE HACKER’S CHOICE WIKI (July 13, 2011), <http://wiki.thc.org/vodafone>.

and fully functional as cellular base stations with the capability to deliver (and intercept) calls, text messages, and data connections. Moreover, the femtocells — like any computer — have security flaws that researchers have been able to exploit to gain administrative access. Indeed, researchers have then been able to modify the devices, turning the femtocells into hundred dollar surveillance devices capable of intercepting communications to and from nearby phones.²⁶⁴ While the degree of technical skill necessary to turn a femtocell into an interception device is high,²⁶⁵ their low cost and small size makes them an ideal choice for a technically sophisticated criminal.

3. Advances in Passive Interception

Just as the software-defined radio revolution and the availability of open source cellular radio software have lowered the cost of active interception, they have also enabled researchers and hobbyists to create low-cost, passive interception devices. Such capacity to receive the signals transmitted over the air between phones and cellular networks should not automatically enable interception of the contents of telephone calls. After all, modern cellular networks generally use encryption technologies to protect communications.²⁶⁶ The wireless industry, however, continues to use insecure encryption algorithms, many of which were created behind closed doors, without review by independent cryptography experts.²⁶⁷ Moreover, some developers of

264. Golde, Redon & Borgaonkar, *supra* note 263, at 7 (“This allows an attacker to impersonate any operator by utilizing a rogue femtocell as an inexpensive 3G IMSI-Catcher and wiretap device. Consequently, adversaries can intercept mobile communication by installing the device in the radio range of a victim.”); Erica Fink & Laurie Segall, *Femtocell Hack Reveals Mobile Phones’ Calls, Texts and Photos*, CNNMONEY (July 15, 2013), <http://money.cnn.com/2013/07/15/technology/security/femtocell-phone-hack/index.html> (“In a demonstration . . . researchers . . . covertly recorded one of our phone conversations and played it back for us. They were also able to record our browsing history, text messages, and even view pictures we sent from one smartphone to another by hacking the network extender.”).

265. It is possible, and in fact, likely, that sophisticated users will in time automate much of the difficult work required to modify the software running on femtocells, thus lowering the technical barriers that currently prevent less-sophisticated users from using femtocells to intercept calls. Cf. *supra* note 256.

266. This is not always the case. See *supra* note 37 (describing countries where encryption is not used for voice communications). Moreover, even when voice communications are encrypted, text messages may not be. See Magnus Glendrange et al., Decoding GSM 141 (unpublished Masters thesis, Norwegian University of Science and Technology) (June 2010), available at <http://www.diva-portal.org/smash/get/diva2:355716/FULLTEXT01.pdf> (“When the authors of this thesis asked the various operators, [the Norwegian cellular carrier] Telenor was the only company to admit that they were *not* encrypted It seems to be optional for the operator to encrypt SMS, because we have reports of it being encrypted in Germany.”).

267. See Orr Dunkelman, Nathan Keller & Adi Shamir, *A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony*, IACR EPRINT ARCHIVE (2010), <http://eprint.iacr.org/2010/013.pdf> (“GSM cellular telephony is protected by the A5 family of cryptosystems. The first two members of this family, A5/1 . . . and A5/2 . . . were

these standards have alleged that they were weakened at the request of Western intelligence services.²⁶⁸

Predictably, cryptography researchers have repeatedly discovered critical security flaws in the encryption algorithms designed and deployed by the cellular industry.²⁶⁹ Such flaws can be exploited to decipher the encrypted cellular signals captured with passive monitoring equipment. Moreover, even after researchers demonstrated that these encryption algorithms are vulnerable to interception, the cellular industry — including major U.S. wireless carriers — continues to use them,²⁷⁰ perhaps because of the significant cost of upgrading to newer, more secure technology.²⁷¹

designed in the late 1980s in an opaque process and were kept secret until they were reverse engineered in 1999 from actual handsets.”).

268. See John Perry Barlow, *Decrypting the Puzzle Palace*, COMM’NS OF THE ACM (July 1992), http://groups.csail.mit.edu/mac/classes/6.805/articles/digital-telephony/Barlow_decrypting_puzzle_palace.html (describing the adoption by the U.S. cellular industry of intentionally vulnerable encryption algorithms known to be “pitifully easy to break” as a result of pressure by the NSA); Arild Færaas, *Sources: We Were Pressured To Weaken the Mobile Security in the 80’s*, AFTENPOSTEN (Jan. 9, 2014), <http://www.aftenposten.no/nyheter/uriks/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s-7413285.html> (interviewing several experts involved with the creation of the original GSM A5/1 standard who claim that it was intentionally weakened as a result of pressure from the British government); John Markoff, *Researchers Crack Code in Cell Phones*, N.Y. TIMES (Apr. 14, 1998), <http://www.nytimes.com/1998/04/14/business/researchers-crack-code-in-cell-phones.html> (“[A] digital key used by G.S.M. may have been intentionally weakened during the design process to permit Government agencies to eavesdrop on cellular telephone conversations.”); Posting of Ross Anderson, rja14@cl.cam.ac.uk to UK.Telcom Google Group, <https://groups.google.com/forum/#!forum/uk.telecom> (June 17, 1994), <https://groups.google.com/forum/#!msg/uk.telecom/TkdCaytoeU4/Mroy719hdroJ> (“[T]here was a terrific row between the NATO signals agencies in the mid 1980’s [sic] over whether GSM encryption should be strong or not. The Germans said it should be, as they shared a long border with the Evil Empire; but the other countries didn’t feel this way.”).

269. For example, the COMP128 cellular authentication algorithm was broken in two hours by Ian Goldberg and David Wagner, then graduate students at UC Berkeley. See Posting of Marc Briceno, marc@scard.org, to ukcrypto@maillist.ox.ac.uk (Oct. 21, 1999) [hereinafter Posting of Briceno], available at <http://cryptome.org/jya/gsm-weak.htm> (revealing that he reverse-engineered the COMP128 and A5/2 algorithms “during evenings and on weekends over the course of a few months on a budget of well below \$100,” and that Ian Goldberg and David Wagner then cryptanalyzed and promptly broke the algorithms in 2 hours for COMP128 and 2 days for A5/2); David Wagner, Ian Goldberg & Marc Briceno, *GSM Cloning*, ISSAC ARCHIVE (Apr. 13, 1998), <http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html>.

270. See *infra* note 281.

271. As Steve Babbage, the Chairman of ETSI SAGE observed in 2007, the cost to the wireless carriers of replacing old cellular network equipment with newer, more secure technology is likely a major reason for the carriers’ decade long delay in replacing algorithms known to be significantly flawed. See Steve Babbage, *An Update from ETSI SAGE, SECURITY ALGORITHMS GROUP OF EXPERTS 3 n.3* (2007), available at http://www.etsi.org/images/files/securityworkshop2007/Security2007S7_4_Steve_Babbage.pdf (“GSM encryption is performed in the base station — and there are an awful lot of base stations in an operator network. Introducing substantially different algorithms typically requires a hardware upgrade, not just a software change. So upgrading a network to support a new GSM algorithm is very expensive.”).

One of the most widely used cellular telephone encryption algorithms, A5/1, was created by the wireless industry in 1988.²⁷² A weakened version intended for use by non-Western countries, known as A5/2, was developed five years later.²⁷³ The industry did not publish these algorithms, but in 1999 they were reverse engineered and finally subjected to review by independent security experts.²⁷⁴ A team of graduate students broke the weakened,²⁷⁵ “export-grade” A5/2 algorithm in only a few hours after it was published.²⁷⁶ Several months later, a team of cryptographers discovered a critical flaw in the stronger A5/1 algorithm, opening the door to practical, real-time decryption of A5/1 protected communications.²⁷⁷

Even though the cryptography community considered A5/2 broken in 1999, the cellular industry did not phase out its use until 2007,²⁷⁸ and then only because new research demonstrated that the

272. See SECURITY ALGORITHMS GROUP OF EXPERTS (SAGE), REPORT ON THE SPECIFICATION AND EVALUATION OF THE GSM CIPHER ALGORITHM A5/2, ETSI TECHNICAL REPORT 278 (Mar. 1996), available at http://www.etsi.org/deliver/etsi_etr/200_299/278/01_60/etr_278e01p.pdf.

273. See *id.* (“SAGE started work on A5/2 in November 1992 and delivered the final specification and test data to the MoU Security Rapporteur on the 31 March 1993.”).

274. See Dunkelman, Keller & Shamir, *supra* note 267.

275. The design goal of A5/2 was to “protect traffic on the GSM radio path so that such traffic is no more vulnerable to eavesdropping than on a Public Switched Telephone Network (PSTN) telephone line” The algorithm apparently passed this low bar, and “all members of SAGE stated [prior to the algorithm’s release] that they were satisfied that the algorithm was suitable to protect against eavesdropping on the GSM radio path” See SECURITY ALGORITHMS GROUP OF EXPERTS (SAGE), *supra* note 272, at 9, 11. However, by 2007, after academic researchers had demonstrated significant security flaws in the algorithm, even the Chairman of the SAGE group acknowledged that the “A5/2 encryption algorithm for GSM is extremely weak — it provides no protection at all against eavesdropping.” See Babbage, *supra* note 271, at 2.

276. See Posting of Briceno, *supra* note 269; E-mail from David Wagner to author (Mar. 17, 2014, 01:04 AM EDT) (“It took us about 5 hours to devise a break of A5/2.”) (on file with author); Ian Goldberg et al., *The (Real-Time) Cryptanalysis of A5/2*, CRYPTO ‘99 (Aug. 26, 1999), available at <http://www.cs.berkeley.edu/~daw/tmp/a52-slides.ps>.

277. See Alex Biryukov et al., *Real Time Cryptanalysis of A5/1 on a PC*, FAST SOFTWARE ENCRYPTION WORKSHOP (2000), available at <http://cryptome.org/a51-bsw.htm> (updating a paper published in LECTURE NOTES IN COMPUTER SCIENCE 1978, at 1–18 (1999)). During the decade that followed the A5/1 research by Biryukov and Shamir, several other research teams improved on this work, to make it more efficient to break. See, e.g., Eli Biham & Orr Dunkelman, *Cryptanalysis of the A5/1 GSM Stream Cipher*, in PROGRESS IN CRYPTOLOGY, PROCEEDINGS OF INDOCRYPT ‘00, LECTURE NOTES IN COMPUTER SCIENCE 1977 43 (2000); Alexander Maximov et al., *An Improved Correlation Attack on A5/1*, in PROCEEDINGS OF THE 11TH INTERNATIONAL CONFERENCE ON SELECTED AREAS IN CRYPTOGRAPHY (SAC’04), LECTURE NOTES IN COMPUTER SCIENCE 3357 1 (2005); Karsten Nohl, *Attacking Phone Privacy*, SECURITY RESEARCH LABS, at 6 (July 28, 2010), https://srlabs.de/blog/wp-content/uploads/2010/07/Attacking.Phone_Privacy_Karsten.Nohl_1.pdf.

278. See *Withdrawal of A5/2 Algorithm [sic] Support*, OSMOCOM SECURITY, http://security.osmocom.org/trac/wiki/A52_Withdrawal (Nov. 12, 2010). See generally Harald Welte, *A Brief History on the Withdrawal of the A5/2 Ciphering Algorithm in GSM*, HARALD WELTE’S BLOG (last modified Nov. 12, 2010), www.advogato.org/person/LaForge/diary.html?start=137.

methods used to attack A5/2 could be used to attack the security of Western A5/1 networks as well.²⁷⁹ Today, the A5/1 algorithm, created in 1988 and thoroughly broken a decade ago, remains the most widely deployed cellular encryption algorithm in the world.²⁸⁰ Indeed, wireless carriers AT&T and T-Mobile still use the A5/1 algorithm for their older “2G” networks in the United States.²⁸¹

Information about the strength of the encryption algorithms chosen by carriers, or whether encryption is used at all, is not readily made available to consumers, who reasonably might be alarmed to learn that the wireless carriers are not using the most secure encryption available (or in some cases, any at all) to protect their communications. Indeed, the GSM standard requires that phones be capable of displaying a warning when no encryption is in use.²⁸² However, the standard also permits wireless carriers to disable the encryption indicator, something that most do.²⁸³ Likely due to the fact that it was generally disabled and thus not displayed to consumers, many phone manufacturers, including some of the largest phone manufacturers such as Apple, Samsung, and Huawei, do not support the encryption warning feature in their phones.²⁸⁴ As such, there is generally no easy way for consumers to determine when their calls are unencrypted or only protected with weak encryption algorithms.

Although the academic research community has long documented the flaws in the encryption algorithms used by wireless carriers, these

279. The primary motivation for the cellular industry to withdraw A5/2 was not concern for the privacy of users in countries where the weak A5/2 algorithm was used, but rather, because the availability of A5/2 support in handsets threatened the security of phone calls in countries where the more-secure A5/1 algorithm was used. See Welte, *supra* note 278 (“Since they [sic] key generation for A5/1 and A5/2 is the same, a semi-active downgrade attack can be used to retroactively break previously-recorded, encrypted A5/1 calls. The only solution to this problem is to remove A5/2 from all equipment, to make sure the downgrade is not possible anymore.”).

280. See Timberg & Soltani, *supra* note 8 (“More than 80 percent of cellphones worldwide use weak or no encryption for at least some of their calls . . .”).

281. See *GSM Security Country Report: USA*, SECURITY RESEARCH LABS, at 4 (Aug. 2013), available at http://gsmmap.org/assets/pdfs/gsmmap.org-country_report-United_States_of_America-2013-08.pdf; E-mail from Karsten Nohl to author (Apr. 6, 2014, 11:19 PM PDT) (on file with author) (describing the continued use of A5/1 “by AT&T and T-Mobile, but only for 2G voice and SMS” while 3G “uses a much improved cipher, that currently nobody knows how to crack” and A5/0 is used in the United States “only for less important transaction[s] such as regular [network] updates, but not for calls or SMS”).

282. See Iosif Androulidakis et al., *Ciphering Indicator Approaches and User Awareness*, 2012 MAEJO INT'L J. SCI. & TECH. 514, 516, available at <http://www.mijst.mju.ac.th/vol6/514-527.pdf>.

283. See DEFCONConference, *supra* note 255, at 07:10 (“So, every sim card that I have ever seen in my entire life, and I've seen a few, from various networks around the world, every single one of them has [the warning disabled], every single operator that I've ever seen disables that warning message.”).

284. Androulidakis et al., *supra* note 282, at 519 (“Nine different manufacturers in the considered dataset (Sharp, Samsung, Qtek, HTC, Motorola, LG, Huawei, Chinabuye and Apple) did not employ a Ciphering Indicator, although this is required by the standards . . .”).

vulnerabilities could only be exploited by those with the resources to buy or build interception and decryption equipment. But just as software-defined radio technology has lowered the cost of active interception, so too has it provided researchers and hobbyists with the means to receive cellular signals that can then be deciphered using open source software that implements decade-old academic cryptographic research.²⁸⁵ Passive interception technology that once cost tens of thousands of dollars can now be built at home for as little as \$15.²⁸⁶ Similarly, whereas cellular interception was once a black art practiced by those in the intelligence community, today, professors assign the task of decrypting cellular communications to their computer science students.²⁸⁷

The widespread availability of low-cost radio hardware, fast personal computers, and free open source cellular interception and cryptanalysis software has made passive interception possible for any interested tech-savvy person, including criminals, enabling them to access conversations and other data previously only available to governments.²⁸⁸ These security threats are discussed next.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 54 of 76

285. See Glendrange et al., *supra* note 266, at 2 (stating that, due to its expense and complexity “[a]nalyzing and capturing GSM traffic was up until recently an unexplored area” but anticipating that soon “anyone with [an] interest in GSM security [will be enabled] to investigate the theoretical security principles through practical approach”); *A5/1 Decryption*, SECURITY RESEARCH LABS, <https://opensource.srlabs.de/projects/a51-decrypt> (last visited Dec. 18, 2014) (the website for the Kraken tool, which “allows the ‘cracking’ of A5/1 keys used to secure GSM 2G calls and SMS.”).

286. See Jon Borland, *\$15 Phone, 3 Minutes All That’s Needed To Eavesdrop on GSM Call*, ARS TECHNICA (Dec. 29, 2010), <http://arstechnica.com/gadgets/2010/12/15-phone-3-minutes-all-thats-needed-to-eavesdrop-on-gsm-call/>; Posting of Lucky Green, [email unavailable], to cryptography@c2.net (Dec. 5, 1999), <http://www.mail-archive.com/cryptography@c2.net/msg02532.html> (“I know how to build a GSM interception station using off-the-shelf hardware and [an Intel Pentium II processor] running Linux for a total cost of well below USD 10k.”).

287. See Gerhard Schneider, Konrad Meier & Dennis Wehrle, *Practical Exercise on the GSM Encryption A5/1* (Feb. 23, 2011), https://web.archive.org/web/20131228091106/http://www.data.ks.uni-freiburg.de/download/misc/practical_exercise_a51.pdf (accessed through the Internet Archive Index).

288. It should be noted that the research team that has in recent years lead the way in demonstrating significant, practical flaws in the A5/1 algorithm has intentionally not published step-by-step instructions to decrypt calls. See Posting of Karsten Nohl, nohl@virginia.edu, to A51@lists.srlabs.de (Aug. 11, 2013), <https://lists.srlabs.de/pipermail/a51/2013-August/001268.html> (“We are not publishing attack tutorials. The line we are walking — between warning about possible abuse and enabling it — is already very fine.”). However, it is almost certain that others will fill this void by documenting the process.

VI. OUR VULNERABLE CELLULAR NETWORKS CAN BE AND ARE EXPLOITED BY OTHERS

The U.S. and other select global powers no longer enjoy a domestic monopoly over the use of cellular interception technology.²⁸⁹ Accordingly, a much larger number of hostile foreign intelligence services can and, almost certainly, are using the technology in this country for espionage. Similarly, if cellular interception technology is not already in use by criminals, the paparazzi, and tech-savvy creepy neighbors, it is only a matter of time before they acquire and use it too. This Part discusses these current and possible future threats.

A. Foreign Governments

Cellular interception technology can be a critical tool in intelligence operations.²⁹⁰ In contrast to law enforcement surveillance, for example, where the assistance of a wireless carrier is often available, intelligence agencies operating without the knowledge or assistance of local governments cannot obtain information from wireless carriers.²⁹¹ As such, cellular interception devices are often the only way for intelligence agencies to monitor the communications of targets.

Indeed, as a result of the disclosures to the media by Edward Snowden, it is now clear (and not surprising) that the U.S. National Security Agency (“NSA”) uses both active and passive cellular interception technology. The NSA’s Special Collection Service reportedly uses passive cellular interception devices installed at U.S. embassies and consulates around the world to spy on the telephone calls of foreign leaders.²⁹² More specifically, an internal NSA surveillance product catalog describes active cellular interception devices that are available for use by agents conducting intelligence operations.²⁹³

Just as U.S. intelligence agencies use cellular interception technology to perform surveillance in foreign countries, so too do foreign

289. See *supra* Part V.

290. See Morrison Affidavit 2012, *supra* note 50; *supra* Part II.B.

291. See *supra* Part II.B.

292. See *DRTBOX and the DRT Surveillance Systems*, TOP LEVEL TELECOMM’S (Nov. 27, 2013), <http://electrospace.blogspot.com/2013/11/drtbox-and-drt-surveillance-systems.html> (describing the DRT family of cellular surveillance products manufactured by Boeing and analyzing their likely use by the NSA, based on references to “DRTBox” in NSA documents leaked by Edward Snowden); *supra* note 90.

293. See *CANDYGRAM — GSM Telephone Tripwire*, <http://leaksource.files.wordpress.com/2013/12/nsa-ant-candygram.jpg> (last visited Dec. 18, 2014) (“Mimics GSM cell tower of a target network Typical use scenarios are asset validation, target tracking and identification as well as identifying hostile surveillance units with GSM handsets.”); Jacob Appelbaum, Judith Horchert & Christian Stöcker, *Shopping for Spy Gear: Catalog Advertises NSA Toolbox*, SPIEGEL ONLINE (Dec. 29, 2013), <http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html>.

intelligence agencies operating in Washington D.C.²⁹⁴ In a 2012 book, national security reporters Marc Ambinder and D.B. Grady hinted at the existence of cellular surveillance activities by foreign governments, revealing that “[t]he FBI has quietly removed from several Washington, D.C.-area cell phone towers, transmitters that fed all data to . . . foreign embassies.”²⁹⁵ When asked about the claim by the Washington Post, the FBI declined to comment.²⁹⁶ However, a former FBI deputy director told Newsweek in the summer of 2014 that “[t]his type of technology has been used in the past by foreign intelligence agencies here and abroad to target Americans, both [in the] U.S. government and corporations There’s no doubt in my mind that they’re using it.”²⁹⁷

As President Obama has noted, “We know that the intelligence services of other countries . . . are constantly probing our government and private sector networks and accelerating programs to listen to our conversations”²⁹⁸ It is for that reason, he added, that “BlackBerrys and iPhones are not allowed in the White House Situation Room.”²⁹⁹ The importance of those security rules was proven after a team of technical experts revealed in the fall of 2014 that they had detected, with sophisticated anti-surveillance equipment, tell-tale signs of IMSI catchers in eighteen locations in the Washington D.C. area, including near the White House, Congress, and several foreign embassies.³⁰⁰

Although the NSA takes steps to protect the communications of the President and other senior national security officials from foreign

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 56 of 76

294. See Matthew M. Aid, *The Spies Next Door*, FOREIGN POL’Y (Sept. 21, 2012), http://www.foreignpolicy.com/articles/2012/09/21/the_spies_next_door (“Almost half of the 200,000 men and women who belong to the U.S. intelligence community work in Washington, as do several thousand foreign intelligence officers who operate openly from dozens of embassies and international organizations in the U.S. capital, trawling the landscape for secrets.”) (emphasis added).

295. See MARC AMBINDER & D.B. GRADY, DEEP STATE: INSIDE THE GOVERNMENT SECRECY INDUSTRY 245 (2013).

296. Timberg & Soltani, *supra* note 8.

297. Jeff Stein, *New Eavesdropping Equipment Sucks All Data off Your Phone*, NEWSWEEK (June 22, 2014), <http://www.newsweek.com/2014/07/04/your-phone-just-got-sucked-255790.html>.

298. See Barack Obama, President of the United States, Speech on NSA Reforms (Jan. 17, 2014), *in Transcript of President Obama’s Jan. 17 Speech on NSA Reforms*, WASH. POST (Jan. 17, 2014), http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bc8d84_story.html.

299. *Id.*

300. See Ashkan Soltani & Craig Timberg, *Tech Firm Tries To Pull back Curtain on Surveillance Efforts in Washington*, WASH. POST (Sept. 17, 2014), http://www.washingtonpost.com/world/national-security/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/f8c1f590-3e81-11e4-b03f-de718edeb92f_story.html.

intelligence agencies, they are the exception, not the norm.³⁰¹ It is likely that many Members of Congress and their staff do not receive special assistance or protection from surveillance in the United States.³⁰² Similarly, there are many other people who participate, directly or indirectly, in this country's policy process — including journalists, lawyers, lobbyists, researchers, and activists — whose communications are intelligence-rich, vulnerable, and likely targeted by foreign intelligence agencies.

Moreover, cellular interception equipment is equally useful for non-political espionage conducted by foreign governments. Specifically, this technology can be used in business centers like New York or Silicon Valley for industrial espionage or to gain insider knowledge by monitoring the communications of business executives, financiers, and entrepreneurs.³⁰³

B. Non-Government Use of Cellular Surveillance Technology

If cellular interception technology were still prohibitively expensive and exclusively available to governments engaged in foreign and domestic surveillance, the communications of the average law-abiding American would rarely be targeted.³⁰⁴ After all, intercepting telephone calls on U.S. soil will presumably focus their efforts on the tiny percentage of Americans whose communications have some significant strategic or intelligence value.

301. See Michael S. Schmidt & Eric Schmitt, *Obama's Portable Zone of Secrecy (Some Assembly Required)*, N.Y. TIMES, Nov. 10, 2013, at A1, available at <http://www.nytimes.com/2013/11/10/us/politics/obamas-portable-zone-of-secrecy-some-assembly-required.html> ("Countermeasures are taken on American soil as well. When cabinet secretaries and top national security officials take up their new jobs, the government retrofits their homes with special secure rooms for top-secret conversations and computer use.").

302. See Letter from Tom Wheeler, Chairman, FCC, to Rep. Alan M. Grayson (Aug. 1, 2014), available at http://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db0822/DOC-328995A1.pdf (responding to inquiry by Rep. Grayson as to how Congress can protect their cellular communications from interception by encouraging Rep. Grayson and his colleagues in Congress to "utilize resources the Commission has made available to educate and inform regarding communications goods and services," including "several consumer publications aimed at increasing consumer awareness of [interception] risks").

303. See James Clark, *French Spies Listen in to British Calls*, SUNDAY TIMES (U.K.), Jan. 23, 2000, available at Factiva, Doc. No. st00000020010817dw1n000f ("French intelligence is intercepting British businessmen's calls Eavesdroppers can 'pluck' GSM digital mobile phone signals from the air by targeting individual numbers or sweeping sets of numbers. Targets have included executives at British Aerospace, British Petroleum and British Airways").

304. The strategic targeting practices of foreign governments do not, however, completely insulate innocent, law-abiding Americans from having their communications monitored incidentally by the United States and foreign government agencies. As described in Part II, this surveillance technology is by its very nature overbroad in its operation, capturing data about many other phones in the vicinity of the area where it is used.

With respect to the average American's exposure to private communications interception, however, history appears to be repeating itself. Just as the radio scanners of the 1990s enabled nearly anyone to intercept a neighbor's analog phone communications, modern cellular interception devices are now available for purchase over the Internet from surveillance technology resellers around the world for a few thousand dollars each.³⁰⁵ Moreover, they are far easier to use than the homemade models built by researchers,³⁰⁶ making them an attractive tool for criminals, private investigators, and paparazzi.³⁰⁷

In the Czech Republic, for example, law enforcement and intelligence officials have voiced concerns about the threat posed by cellular interception technology. In 2012, the head of the Czech Criminal Police unit for wiretapping told the national public radio service that his team had detected non-police active interception devices in use around the country.³⁰⁸ Similarly, the ex-head of the Czech Military Intelligence Agency expressed fears about potential widespread availability and sale of such technology, stating that "if their use will not be in any way regulated, and access to these devices will not be in any way controlled, then a regular citizen can do absolutely nothing [to safeguard their communications]."³⁰⁹ He speculated that the most likely private users of the devices were security firms and rival businesses engaged in industrial espionage.³¹⁰

In China, cellular interception devices are perhaps more widely available than in any other country in the world. In the spring of 2014, Chinese police shut down twenty-four different factories manufacturing illegal IMSI catchers.³¹¹ These devices are in widespread use by criminal gangs, apparently not for surveillance or espionage, but rather, to send spam and fraudulent text messages that lure unwitting victims to phishing sites.³¹² Specifically, using these devices, fraudsters send tens of millions of messages per day to unsuspecting consumers with spoofed origin phone numbers normally used by online

305. See *supra* Part V.

306. See *supra* Part V.B.1.

307. We are not suggesting that it would be legal for private parties to intercept the conversations of others. The chance of being discovered intercepting calls, however, is extremely low, even more so when passive surveillance technology is used.

308. See Masha Volynsky, *Spy Games Turn Real as Eavesdropping Technology Spreads*, RADIO PRAGUE (Aug. 16, 2012), <http://www.radio.cz/en/section/curraffrs/spy-games-turn-real-as-eavesdropping-technology-spreads>.

309. *Id.*

310. *Id.*

311. See *Chinese Police Bust Major Telecom Fraud Ring*, XINHUA, available at http://www.chinadaily.com.cn/china/2014-04/29/content_17474783.htm (last updated Apr. 29, 2014).

312. See Russel Brandom, *Phony Cell Towers Are the Next Big Security Risk*, VERGE (Sept. 18, 2014), <http://www.theverge.com/2014/9/18/6394391/phony-cell-towers-are-the-next-big-security-risk>.

banks and other trusted parties.³¹³ According to one Chinese mobile security expert, “It’s very lucrative to have a [fake] tower device right now. People will pay big money for it”³¹⁴

While commercial cellular interception technology is, for now, probably too expensive for the average stalker or garden variety criminal, the cost of these devices will, like all technology, decrease over time.³¹⁵ At just a few thousand dollars each, however, commercial cellular interception devices are already affordable for sophisticated domestic or multi-national criminal organizations, companies engaging in industrial espionage, private investigators, and paparazzi. And for the technically skilled criminal, no matter the scale of his operations, cellular surveillance technology is already affordable.³¹⁶

Although cellular surveillance devices are not *yet* in widespread private use in the United States,³¹⁷ they are certainly no longer a secret. To suggest otherwise is to embrace and propagate a fiction; these technologies have been globalized and democratized, and the vulnerabilities they exploit now threaten the privacy of hundreds of millions of Americans who use cellular telephones to communicate. Indeed, the use of cellular interception devices in India and the Czech Republic paints a worrisome picture of the potential threat. Even so, U.S. government agencies continue to treat cellular surveillance equipment as a closely guarded secret, even protecting the name of the equipment they use.³¹⁸ As discussed next, the consequence of embracing this erroneous, tendentious narrative, which grants surveillance priority over the security of communication networks, is that the American public remains vulnerable to cellular surveillance by a variety of non-U.S. government actors.

VII. A HIGH PRICE TO PAY FOR THE FICTION OF SECRECY

The analog-phone vulnerabilities of the 1990s were no secret. The technology required to intercept calls was widely available and several high-profile abuses led to front-page scandals involving the com-

313. *Id.*

314. *Id.*

315. See generally Douglas McCormick, *Wright's Law Edges out Moore's Law in Predicting Technology Development*, IEEE SPECTRUM (July 25, 2012), <http://spectrum.ieee.org/tech-talk/at-work/test-and-measurement/wrights-law-edges-out-moores-law-in-predicting-technology-development> (describing a research paper that compares various models, including Moore's Law, all of which attempt to predict the decrease in the price of technologies over time).

316. See *supra* Part V.B.1.

317. This does not mean they have not been used at all. According to national security journalist Marc Ambinder, “The Secret Service has caught people using Sting[R]ays to collect personal data for use in financial fraud cases.” See E-mail from Marc Ambinder to author (May 13, 2013, 11:30 PM PDT) (on file with author).

318. See *supra* Part IV.

munications of the rich and powerful. In response, Congress held hearings, the cellular industry weighed in, and, ultimately, the FCC promulgated regulations intended to limit the ease with which interception technology could be obtained.³¹⁹ Although the approach adopted by policy makers and regulators — seeking to prohibit the sale of interception equipment, rather than mandating technical solutions capable of securing communications from interception — was ineffective, Congress and the FCC at least acknowledged the problem and did *something* to try to address it.

The Congress of the 1990s held public hearings focused on cellular interception vulnerabilities;³²⁰ the Congress of the 2010s has not. The FCC of the 1990s adopted regulations intended to protect cellular communications from interception,³²¹ the FCC of the 2010s perpetuates the fiction that cellular interception is a secret capability available only to government agencies by shielding information about cellular interception equipment from public disclosure.³²² Whereas the cellular vulnerabilities of the 1990s were treated as a threat to the nation's cellular network, today, DHS, whose stated mission includes protecting critical infrastructure and information networks,³²³ also appears to have embraced the sensitive source and method narrative.³²⁴

In 2013, acting FCC Chairwoman Mignon Clyburn stated, “Protecting consumer privacy is a key component of [the FCC’s] mission to serve the public interest.”³²⁵ Her predecessor, former FCC Chairman Julius Genachowski, similarly acknowledged that Congress had directed the Commission to “protect the privacy of consumers who rely on our Nation’s communications infrastructure.”³²⁶ Over the past two decades, however, the FCC appears to have done little other than accommodate and perpetuate the fictional secrecy narrative authored

319. See *supra* Part I.

320. *Id.*

321. *Id.*

322. See Letter from Julius P. Knapp, Chief, Office of Eng’g & Tech., FCC, to author (Feb. 29, 2012), available at <http://files.cloudprivacy.net/FOIA/FCC/fcc-stingray-reply.pdf> (“[W]e are withholding certain intra-agency and interagency e-mails and documents because they are classified or because taken together with other information they could endanger national and homeland security.”).

323. *Mission*, U.S. DEP’T OF HOMELAND SEC., <http://www.dhs.gov/mission> (last modified Aug. 8, 2012) (“[DHS] works with industry and state, local, tribal and territorial governments to secure critical infrastructure and information systems.”).

324. See *supra* Part III.

325. Statement of Mignon Clyburn, Acting Chairwoman, FCC, Re: Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information, CC Docket No. 96-115 (June 27, 2013), available at http://transition.fcc.gov/Daily_Releases/Daily_Business/2013/db0627/FCC-13-89A2.pdf.

326. *Consumer Online Privacy: Hearing Before the S. Comm. on Commerce, Sci. and Transp.*, 111th Cong. 3 (2010) (statement of Julius Genachowski, Chairman, FCC), available at <http://www.gpo.gov/fdsys/pkg/CHRG-111shrg67686/html/CHRG-111shrg67686.htm>.

by law enforcement agencies and cellular surveillance equipment manufacturers.³²⁷ Indeed, the agency continues to grant equipment authorizations (and requested protections from public disclosure) for each new cellular surveillance product the Harris Corporation seeks to market to law enforcement agencies.³²⁸

Together with the FCC, DHS shares the responsibility of protecting the security of America's civilian telephone networks. DHS is also a law enforcement agency, with component agencies that have spent millions of dollars on StingRays and other cellular interception equipment.³²⁹ Moreover, DHS funds the acquisition of cellular surveillance equipment by state and local law enforcement agencies.³³⁰ Likewise, as the primary regulator of the wireless and wireline carriers, the FCC has repeatedly used its regulatory powers to force telecommunications companies to facilitate surveillance by law enforcement and intelligence agencies.³³¹ These two agencies thus

327. See *supra* Part IV.B.

328. See *supra* note 191.

329. See Kelly, *supra* note 21.

330. See STAFF OF PERMANENT SUBCOMM. ON INVESTIGATIONS OF THE S. COMM. ON HOMELAND SEC. AND GOVERNMENT AFFAIRS, 112TH CONG., REP. ON FEDERAL SUPPORT FOR AND INVOLVEMENT IN STATE AND LOCAL FUSION CENTERS 81 (Oct. 3, 2012), available at <http://www.hsgac.senate.gov/download/?id=49139e81-1dd7-4788-a3bb-d6e7d97dde04> (describing the use of a FEMA grant to purchase "sophisticated cell phone tracking devices" by the Washington D.C. Homeland Security and Emergency Management Agency); CITY OF TACOMA, WA, CITY COUNCIL MINUTES (Mar. 19, 2013), available at <http://cms.cityoftacoma.org/cityclerk/Files/CityCouncil/Minutes/2013/CCMin20130319.pdf> ("Authorizing the execution of a grant agreement with the U.S. Department of Homeland Security Port Security Grant Program in the amount of \$188,814.31 . . . [to purchase from the] Harris Corporation . . . technical support equipment to assist in the prevention, detection, response, and recovery of improvised explosive devices."); Michael Bott & Thom Jensen, *Cellphone Spying Technology Being Used Throughout Northern California*, NEWS 10 (Mar. 6, 2014), <http://www.news10.net/story/news/investigations/watchdog/2014/03/06/cellphone-spying-technology-used-throughout-northern-california/6144949/> ("StingRays are being paid for mostly by Homeland Security grant money distributed by the California Emergency Management Agency, under programs such as the Urban Areas Security Initiative (UASI) or the State Homeland Security Program (SHSP).").

331. The FCC has repeatedly used the license granting process to extract surveillance enabling concessions from service providers that are not required by law. *Fourth Amendment and the Internet: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 106th Cong. 135 (2000) (statement of Stewart Baker, Partner, Steptoe & Johnson LLP), available at http://commdocs.house.gov/committees/judiciary/hju66503.000/hju66503_0f.htm (noting that "[t]he FBI and the Justice Department have intervened repeatedly at the FCC to try to deny licenses to companies that have not been fully cooperative" and citing specific examples of such practice); Craig Timberg & Ellen Nakashima, *Agreements with Private Companies Protect U.S. Access to Cables' Data for Surveillance*, WASH. POST (July 6, 2013), http://www.washingtonpost.com/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html ("In deals involving a foreign company, say people familiar with the process, the FCC has held up approval for many months while the squadron of lawyers dubbed Team Telecom developed security agreements that went beyond what's required by the laws governing electronic eavesdropping."). Responding to a specific request by the DOJ, the FCC has also required telephone companies to retain telephone call records. Douglas Cox, *More Misleading Information from ODNI on NSA Telephone Metadata Collection*, DOCUMENT EXPLOITATION (July 24, 2013), <http://www.docexblog.com/2013/07/more-misleading-information-from-odni-on-nsa-telephone-metadata-collection/>.

attempt to satisfy two, sometimes competing, jurisdictional mandates:³³² enabling or engaging in surveillance on the one hand, while seeking to ensure the security of communications networks, on the other. These dual roles and objectives come into conflict, in theory and practice, when choices must be made to privilege either surveillance or security.

With respect to the dual surveillance and security responsibilities under the jurisdiction of these federal agencies, an uncritical adoption of the law enforcement narrative can suppress an equally compelling counter-narrative: Americans' cellular communications are vulnerable to interception by foreign governments and criminals. We don't know if or to what extent officials at the FCC or DHS have made an actual policy choice to privilege cellular interception over the security of cellular networks. Are officials, by withholding information about cellular interception technology, uncritically perpetuating the sensitive source and method narrative or, much worse, are they participating in a strategic choice to embrace this fiction?

By viewing cellular interception equipment completely from a law enforcement agency perspective, policymakers and regulators are unlikely to address the underlying vulnerabilities in American cellular networks. To date, the government has made little effort publicly to address the cellular network vulnerabilities or to warn users about them. Meanwhile, the FCC and DHS have actively enabled the ongoing exploitation of these vulnerabilities by U.S. government agencies.

In response to a letter from Congressman Alan Grayson that cited an early online draft of this Article,³³³ FCC Chairman Tom Wheeler announced that the Commission has formed a task force to investigate "illicit uses" of cellular surveillance technology.³³⁴ Congressman Grayson's letter and Chairman Wheeler's announcement are the first direct, public statements by current U.S. government officials acknowledging the privacy and national security threats posed by cellular interception technology.

misleading-information-from-odni.html (noting that, in addition to implementing the policy requested by the DOJ, the FCC also "extended the legal retention period for as long as the DOJ said was necessary").

332. These are not the only agencies that have conflicting missions. The NSA has been criticized for prioritizing its offensive mission over defense. Bruce Schneier, *It's Time to Break up the NSA*, CNN OPINION (Feb. 20, 2014), <http://www.cnn.com/2014/02/20/opinion/schneier-nsa-too-big/index.html> ("[The NSA] is an agency that prioritizes intelligence gathering over security, and that's increasingly putting us all at risk.").

333. Letter from Alan M. Grayson to Tom Wheeler, *supra* note 29 (citing a draft of this Article as well as a Newsweek article that describes a demonstration of IMSI catchers for congressional staff organized by one of this Article's authors).

334. Letter from Tom Wheeler to Alan M. Grayson, *supra* note 302 ("I have recently established a task force to initiate immediate steps to combat the illicit and unauthorized use of IMSI catchers. The mission of this task force is to develop concrete solutions to protect the cellular network systemically from similar unlawful intrusions and interceptions.").

While the FCC's task force is perhaps a positive first step, to the extent that it focuses only on the illicit uses of the surveillance technology without addressing the underlying network vulnerabilities exploited by IMSI catchers, it will do little to address the real cybersecurity threat.³³⁵ To address these network vulnerabilities, however, because all parties' surveillance technology exploit the same network vulnerabilities, policymakers will have to grapple with the tension inherent in facilitating "lawful" IMSI catcher use by law enforcement and prohibiting unlawful use by a host of bad actors. That is, there is no way to allow law enforcement to use cellular surveillance devices without also leaving networks vulnerable to criminals and foreign governments.

If the existence and knowledge of these vulnerabilities were truly a secret, and the technology that exploits them were only available to U.S. government agencies, privileging law enforcement equities might be a reasonable policy choice. Such a choice would only be warranted, however, if law enforcement surveillance capabilities could be protected without placing the American public at risk. But as this Article has illustrated, this scenario does not describe reality.

IMSI catcher secrecy is a fairytale, while the long-term impact of the technology may lead to a privacy and security nightmare. Indeed, many of the security flaws exploited by cellular surveillance devices were publicly documented by academic security researchers a decade ago.³³⁶ In the years since, numerous foreign governments have acquired surveillance devices that exploit those same vulnerabilities.³³⁷ Moreover, they are readily available to technologically sophisticated criminals, private investigators, and the paparazzi. Meanwhile, law-abiding citizens and businesses remain in a government-willed darkness on the matter, exposed to a myriad of interception risks.

If policymakers understood cellular network vulnerabilities and treated them as part of the existing debate about cybersecurity, informed public discourse about the balance of risks and rights could begin. The cybersecurity debate and the rightful place of cellular network security in that discourse are addressed next.

VIII. FOCUSING ON CYBERSECURITY

The United States faces a serious cybersecurity threat.³³⁸ Foreign governments, such as China, have repeatedly hacked into the comput-

335. See Stephanie Pell, *We Must Secure America's Cell Networks — From Criminals and Cops*, WIRED (Aug. 27, 2014), <http://www.wired.com/2014/08/we-must-secure-americas-cell-networks-from-criminals-and-cops-alike/>; *infra* Part VIII.

336. *See supra* Part V.B.

337. *See supra* Part V.A.

338. Mitchell S. Kominsky, *The Current Landscape of Cybersecurity Policy: Legislative Issues in the 113th Congress*, HARVARD NAT'L SEC. J. (Feb. 6, 2014), <http://harvardnsj.org/>

er systems of government agencies and major U.S. companies, including technology firms and defense contractors, to steal intellectual property and classified information.³³⁹ James Clapper, the Director of National Intelligence, and James Comey, the Director of the FBI, have both told Congress that cyber attacks are the most serious national security threat faced by the United States.³⁴⁰

In response to these cybersecurity threats and the warnings of senior government and industry officials, Congress has held numerous hearings and proposed legislation.³⁴¹ The White House has appointed a cybersecurity “czar,”³⁴² agencies’ cybersecurity practices are regularly evaluated as part of the oversight process (often revealing serious problems),³⁴³ and the government spends billions of dollar every year on cybersecurity.³⁴⁴

2014/02/the-current-landscape-of-cybersecurity-policy-legislative-issues-in-the-113th-congress/ (“Cybersecurity represents one of the most serious national security threats and economic challenges confronting our country. Cybercrime costs the United States approximately \$100 billion annually . . . [T]he cyber threat is quickly becoming the top priority for our national defense apparatus and private enterprise.”).

339. E.g., Jim Finkle, *Hacker Group in China Linked to Big Cyber Attacks: Symantec*, REUTERS (Sept. 17, 2013), <http://www.reuters.com/article/2013/09/17/us-cyberattacks-china-idUSBRE98G0M720130917>; Ellen Nakashima, *Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies*, WASH. POST (May 27, 2013), http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html; Michael Riley & Ben Elgin, *China’s Cyberspies Outwit Model for Bond’s Q*, BLOOMBERG (May 2, 2013), <http://www.bloomberg.com/news/2013-05-01/china-cyberspies-outwit-u-s-stealing-military-secrets.html>.

340. Greg Miller, *FBI Director Warns of Cyberattacks; Other Security Chiefs Say Terrorism Threat Has Altered*, WASH. POST (Nov. 14, 2013), http://www.washingtonpost.com/world/national-security/fbi-director-warns-of-cyberattacks-other-security-chiefs-say-terrorism-threat-has-altered/2013/11/14/24fb27a-4d53-11e3-9890-a1e0997fb0c0_story.html (“FBI Director James B. Comey testified Thursday that the risk of cyberattacks is likely to exceed the danger posed by al-Qaeda and other terrorist networks as the top national security threat to the United States and will become the dominant focus of law enforcement and intelligence services.”); see also Jim Garamone, *Clapper Places Cyber at Top of Transnational Threat List*, U.S. DEP’T OF DEF. (Mar. 12, 2013), <http://www.defense.gov/news/newsarticle.aspx?id=119500>.

341. See, e.g., Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong. (2012).

342. Michael Hardy, *New White House Cyber Czar Brings Intell Chops*, FED. COMPUTER WEEK (June 4, 2012), <http://fcw.com/articles/2012/06/15/buzz-howard-schmidt-michael-daniel-cyber-czar.aspx>.

343. See U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-12-137, INFORMATION SECURITY: WEAKNESSES CONTINUE AMID NEW FEDERAL EFFORTS TO IMPLEMENT REQUIREMENTS (2011), available at <http://www.gao.gov/new.items/d12137.pdf>; MINORITY STAFF OF THE HOMELAND SEC. & GOVERNMENTAL AFFAIRS COMM., THE FEDERAL GOVERNMENT’S TRACK RECORD ON CYBERSECURITY AND CRITICAL INFRASTRUCTURE (Feb. 4, 2014), available at <http://www.hsgac.senate.gov/download/?id=8BC15BCD-4B90-4691-BDBA-C1F0584CA66A>.

344. See Amber Corrin, *Budget Shows How Cyber Programs Are Spreading*, FED. COMPUTER WEEK (Apr. 12, 2013), <http://fcw.com/Articles/2013/04/12/budget-cybersecurity.aspx> (“The DHS figure includes nearly \$500 million for cybersecurity research and development and almost \$1 billion expressly for the protection of federal computers and networks against malicious cyber activity.”); Andy Sullivan,

Although most of the cybersecurity concerns expressed by government leaders pertain to the security of government networks and so called “critical infrastructure,”³⁴⁵ such as the electronic power grid and the computer systems controlling power plants, America’s telephone networks have not completely escaped the attention of policy-makers. Sparked by fears that Chinese communications equipment companies, such as Huawei and ZTE, may have hidden surveillance backdoors in their products at the request of the Chinese government,³⁴⁶ the U.S. national security establishment responded.³⁴⁷ According to media reports, both AT&T and Sprint, which had planned to purchase Huawei equipment for their next-generation 4G networks, were threatened by senior officials in the national security community with a consequent loss of government business and the disruption of merger plans.³⁴⁸ Ultimately, both companies did not purchase Huawei equipment, instead opting for network hardware from Western manufacturers.³⁴⁹

Obama Budget Makes Cybersecurity a Growing U.S. Priority, REUTERS (Apr. 10, 2013), <http://www.reuters.com/article/2013/04/11/us-usa-fiscal-cybersecurity-idUSBRE93913S20130411> (“Obama’s budget, released on Wednesday, proposes to boost Defense Department spending on cyber efforts to \$4.7 billion, \$800 million more than current levels . . .”).

345. See, e.g., Exec. Order No. 13,636, 78 Fed. Reg. 11739 (Feb. 19, 2013); Presidential Policy Directive — Critical Infrastructure Security and Resilience (Feb. 12, 2013), available at <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

346. STAFF OF U.S.-CHINA ECON. & SEC. REVIEW COMM’N, THE NATIONAL SECURITY IMPLICATIONS OF INVESTMENTS AND PRODUCTS FROM THE PEOPLE’S REPUBLIC OF CHINA IN THE TELECOMMUNICATIONS SECTOR 7 (Jan. 2011), available at http://origin.www.uscc.gov/sites/default/files/Research/FINALREPORT_TheNationalSecurityImplicationsofInvestmentsandProductsfromThePRCintheTelecommunicationsSector.pdf; Jeremy Wagstaff & Lee Chyen Yee, *ZTE Confirms Security Hole in U.S. Phone*, REUTERS (May 18, 2012), <http://www.reuters.com/article/2012/05/18/us-zte-phone-idUSBRE84H08J20120518>.

347. See Antonio Regaldo, *Before Snowden, There Was Huawei*, MIT TECH. REV. (Mar. 18, 2014), <http://www.technologyreview.com/news/525596/before-snowden-there-was-huawei/> (“[A]nytime [Huawei is near] to closing a sale, their customers get a visit from the FBI or U.S. Department of Commerce. The message from the feds isn’t subtle: buy something else.”); John Pomfret, *History of Telecom Company Illustrates Lack of Strategic Trust between U.S., China*, WASH. POST (Oct. 8, 2010, 12:33 AM), <http://www.washingtonpost.com/wp-dyn/content/article/2010/10/07/AR2010100707210.html> (“The message from the NSA . . . was simple: If AT&T wanted to continue its lucrative business with the U.S. government, it had better select a supplier other than Huawei”); David E. Sanger & Nicole Perlroth, *N.S.A. Breached Chinese Servers Seen as Security Threat*, N.Y. TIMES (March 22, 2014) <http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html> (noting that “[American officials] have blocked [Huawei] at every turn” and citing three U.S. government intervention against the company).

348. Pomfret, *supra* note 347.

349. *Id.* (“In February, AT&T announced that it would buy the equipment it needed from Swedish-owned Ericsson and Paris-based Alcatel-Lucent.”); see also Edward Wyatt, *Sprint Nears a U.S. Deal To Restrict China Gear*, N.Y. TIMES (Mar. 28, 2013), <http://www.nytimes.com/2013/03/29/business/sprint-and-softbank-near-agreement-to-restrict-use-of-chinese-suppliers.html> (“SoftBank and Sprint have already assured members

The House Intelligence Committee also investigated the matter, holding a hearing where executives from both Huawei and ZTE testified. In his opening remarks at that hearing, Committee Chairman Mike Rogers stated that “Americans have to trust our telecommunications networks” and that “[w]hen vulnerabilities in the equipment . . . can be exploited by another country, it becomes a priority and a national security concern.”³⁵⁰ After the hearing, the Committee released a bi-partisan report accusing the companies of collaborating with the Chinese military.³⁵¹

Significantly, when faced with the possibility that U.S. telecommunications networks *might* be vulnerable to exploitation by the Chinese government through security flaws or backdoors, Congress and members of the national security community swiftly examined the problem and took decisive action. In contrast to the resources directed at these Chinese supply chain threats, nothing approaching this kind of effort and focus has been channeled towards other existing security vulnerabilities in our cellular networks that *can* and *are* being exploited by the intelligence services of many countries.

While there are a number of likely reasons why the perceived threat posed by Huawei and ZTE became such a high-profile issue for policymakers, it is worth noting that the “fix” to this problem was rather simple — pressuring major U.S. carriers such as AT&T and Sprint to purchase equipment from Western (thus “trusted”) suppliers. The companies that made the mistrusted products are Chinese and thus subject to ready and politically safe (indeed, politically rewarding) demonization by the intelligence community and their allies in Congress. Moreover, the national security threat posed by Chinese government exploitation of backdoors in Chinese telephony equipment, unlike many other threats, offered the inherent political benefit of being legally amenable to public discussion without putting any U.S. government intelligence sources and methods at risk.

In contrast to the Huawei and ZTE threat, the risks posed by the cellular network vulnerabilities described in this Article present a far more politically delicate problem. The technical fix for them may be

of Congress that they will not integrate equipment made by Huawei into Sprint’s United States systems and will replace Huawei equipment in Clearwire’s network.”).

350. Rep. Mike Rogers, *Huawei and ZTE Testify Before the House Intel Committee Part 1* at 3:51, 5:53, YOUTUBE (Oct. 3, 2012), <http://www.youtube.com/watch?v=ApQjSCUpt4s> (recording of testimony before the House Permanent Select Committee on Intelligence on September 13, 2012).

351. See CHAIRMAN MIKE ROGERS & RANKING MEMBER C.A. DUTCH RUPPERSBERGER OF H. PERMANENT SELECT COMM. ON INTELLIGENCE, 112TH CONG., INVESTIGATIVE REP. ON THE U.S. NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANIES HUAWEI AND ZTE 2, 11 (Oct. 8, 2012), available at [https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20\(FINAL\).pdf](https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf).

expensive and time-consuming,³⁵² and the companies that have long known about these vulnerabilities in their networks, yet have neither fixed the vulnerabilities nor warned consumers about the risks, are large, politically active U.S. corporations. Moreover, the devices that exploit these vulnerabilities, which are manufactured by similarly large, politically active defense contractors, are considered sensitive sources and methods that U.S. law enforcement and intelligence agencies would undoubtedly prefer not to be the subject of open discussion at public hearings. It is therefore not surprising that policymakers have failed to tackle this issue, whether in the context of the existing cybersecurity debate or otherwise.

Now that Congress and the FCC have slowly started to acknowledge the national security threats posed by cellular surveillance technology, however, policymakers are likely to look for solutions to the problem. We present and examine some possible solutions next.

IX. PROTECTING OUR COMMUNICATIONS

The cellular communications of billions of people around the world are vulnerable to interception by their own governments, other governments, and tech-savvy criminals. In spite of the determined efforts of the U.S. law enforcement community to suppress disclosure of information about these vulnerabilities and their exploitation by the government, some information has finally entered into public discourse. State legislatures are asking questions about StingRays,³⁵³ members of Congress want to know about their own vulnerability to foreign government surveillance,³⁵⁴ and the FCC has even created a task force to study various cellular surveillance and cybersecurity threats.³⁵⁵ The endemic insecurity of U.S. cellular communications

352. See Babbage, *supra* note 271. The cost may not be significant if the carriers are already upgrading their networks. See E-mail from Karsten Nohl to author (Apr. 21, 2014, 07:03 AM PDT) on file with author ("The biggest cost item is the replacement of old 2G base stations . . . Sourcing an entire 4G network from non-Chinese suppliers easily adds a few billions to the bill.").

353. Michael Barajas, *HPD Has a Machine that Can Steal Your Phone's Data, Says ACLU*, HOUSTON PRESS (Sept. 23, 2014), http://blogs.houstonpress.com/news/2014/09/hpd_has_a_machine_that_can_steer_your_phones_data.php; John Turk, *Experts Question Transparency of Cell Phone Tracking Device Owned by Sheriff's Office at Legislative Hearing*, OAKLAND PRESS (May 16, 2014), <http://www.theoaklandpress.com/general-news/20140516/experts-question-transparency-of-cell-phone-tracking-device-owned-by-sheriffs-office-at-legislative-hearing>.

354. See Letter from Alan M. Grayson to Tom Wheeler, *supra* note 29.

355. See Letter from Tom Wheeler to Alan M. Grayson, *supra* note 302; Craig Timberg, *For Sale: Systems That Can Secretly Track Where Cellphone Users Go Around the Globe*, WASH. POST (Aug. 24, 2014), http://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html (stating that the FCC IMSI catcher

networks is now front-page news. This increased attention from the media and policymakers is likely to result in action — whether in the form of legislation, regulation, or merely increased pressure on the cellular industry.

By upgrading the security of their networks, the wireless carriers can protect their customers from some of the cellular interception technologies described in this Article. Such upgrades will be neither cheap nor easy to perform, given the significant size and reach of U.S. cellular networks.³⁵⁶ Alternatively, consumers' communications could be protected by transitioning to more-secure, Internet-based voice and text communications services that work on top of cellular data and WiFi networks. Or, perhaps, consumers will start to use counter-surveillance technologies capable of detecting nearby cellular surveillance devices. While a thorough examination of the solutions and the regulatory process necessary to execute them is beyond the scope of this Article, this Part will examine a few likely technical avenues through which solutions could come.

A. Securing Cellular Networks

If the wireless carriers and the phones used by their customers exclusively employed modern cellular encryption algorithms, some of the cellular interception vulnerabilities described in this Article would be cured. But the wireless industry has not switched to modern cryptography. Wireless carriers continue to use weak algorithms that were designed in the 1980s and broken in the 1990s.³⁵⁷ Indeed, the outmoded A5/1 algorithm remains the most widely deployed cellular encryption algorithm in the world.³⁵⁸ An improved encryption algorithm, A5/3, was developed and standardized by the cellular industry in 2002. A5/3-capable hardware, however, was not built into cellular phones until 2009,³⁵⁹ and is still not currently used by many carriers.³⁶⁰ The decade-old A5/3 algorithm, however, may already be

task-force has expanded its mission to cover other cellular network security flaws exploited by commercial surveillance technologies).

356. See Babbage, *supra* note 271.

357. See Green, *supra* note 52 (“GSM is nearly 30 years old. You probably wouldn’t blame today’s Ford execs for the crash performance of a 1982 Ford Escort, and similarly you shouldn’t hold the GSM designers responsible for a 1980s protocol — even if billions of people still rely on it.”).

358. See Timberg & Soltani, *supra* note 8.

359. See Presentation from Harald Welte, *Structural Deficits in Telco Security*, at 19 (Mar. 20, 2012), available at https://www.troopers.de/wp-content/uploads/2011/10/TR12_TelcoSecDay_Welte_Mobsec.pdf.

360. See *infra* notes 367–369 and accompanying main text.

showing its age, since it reportedly has already been broken by the NSA and its British counterpart.³⁶¹

Moreover, even though modern smartphones have the capability to communicate using modern, more secure protocols, they must also be able to complete calls and function over older cellular networks where older, weaker encryption is still in use. This necessity for backward compatibility is a source of persistent security vulnerabilities.

By upgrading the encryption algorithms used by existing second generation (“2G”) networks or by migrating entirely to more-secure third (“3G”) and fourth generation (“4G”) technologies, wireless carriers can protect their subscribers from the passive interception vulnerabilities described in Part V.B.³⁶² Deutsche Telekom (“T-Mobile”), for example, has already upgraded its 2G cellular networks in Germany and four other European countries to A5/3, and has planned similar upgrades in other countries.³⁶³ T-Mobile (U.S.) has quietly begun the process of upgrading the security of its own network.³⁶⁴ AT&T has apparently opted for a different approach: Rather than upgrading the security of its 2G network, the company has instead committed to shut it down by 2017 in order to repurpose the spectrum for newer 3G and 4G networks.³⁶⁵ Although AT&T’s planned network migration is likely motivated by consumer demand for high-speed data,³⁶⁶ it will also improve security, because 3G and 4G networks use newer, more secure encryption algorithms.

361. Ryan Gallagher, *Operation AURORAGOLD, How the NSA Hacks Cellphone Networks Worldwide*, INTERCEPT (Dec. 4, 2014), <https://firstlook.org/theintercept/2014/12/04/nsa-auroragold-hack-cellphones> (“In 2009, the British surveillance agency Government Communications Headquarters conducted a similar effort to subvert phone encryption . . . using powerful computers to perform a ‘crypt attack’ to penetrate the A5/3 algorithm, secret memos reveal. By 2011, GCHQ was collaborating with the NSA . . . to attack A5/3 encryption.”).

362. More recent cellular phone systems, including 3G and 4G networks, include the capability for phones to authenticate the network base stations. *See generally* Zhang & Fang, *supra* note 52.

363. Press Release, Deutsche Telekom, Deutsche Telekom Upgrades Wiretapping Protection in Mobile Communications (Dec. 9, 2013), available at <http://www.telekom.com/media/company/210108>.

364. See Ashkan Soltani & Craig Timberg, *T-Mobile Quietly Hardens Part of Its U.S. Cellular Network Against Snooping*, WASH. POST (Oct. 22, 2014), <http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/22/t-mobile-quietly-hardens-part-of-its-u-s-cellular-network-against-snooping/> (“Testing by The Washington Post has found T-Mobile networks using A5/3 in New York, Washington and Boulder, Colorado, instead of the older A5/1 that long has been standard for second-generation (2G) GSM networks in the United States.”).

365. See Thomas Gryta, *AT&T to Leave 2G Behind*, WALL ST. J. (Aug. 3, 2012, 2:53 PM), <http://online.wsj.com/news/articles/SB10000872396390443687504577567313211264588>.

366. *Id.* (“With every network generation, the technology becomes more efficient at carrying information. As a result, companies can get better and more profitable usage from shutting down older networks in favor of newer ones, something that AT&T has talked about.”).

Protecting telephone subscribers from active surveillance devices is far more difficult, if not practically impossible. Even when a wireless carrier has upgraded their entire network, the telephones used by their subscribers will still connect to networks that use older, insecure networking technology. This backward compatibility, which is a necessary feature in all handsets because any phone might be taken by its owner to rural areas or foreign countries where older networks remain in use, is a vulnerability that can also be exploited for surveillance.³⁶⁷ Indeed, many of the manufacturers of active surveillance openly advertise the ability to jam 3G and 4G networks in order to force telephones to connect an active interception device masquerading as a 2G base station.³⁶⁸

The ability to force modern phones to communicate insecurely is an unintended side effect of the need to maintain compatibility for older, insecure cellular network technologies. As long as phones continue to support older, insecure phone protocols, they can be manipulated into using them, even in cities where all legitimate networks use 3G and 4G technology.

The migration away from 2G, which will be a slow and expensive process for the wireless carriers, will certainly improve the security of cellular networks, but many forms of unmediated surveillance will still be possible. While 3G and 4G networks employ much more secure encryption algorithms that protect calls, text messages, and Internet data from unauthorized interception, sophisticated 4G surveillance devices can still acquire the serial numbers of nearby phones and locate them. Indeed, several law enforcement agencies have already upgraded to the 4G capable Harris Hailstorm, which can locate and identify nearby 4G phones.³⁶⁹ As the wireless industry slowly mi-

367. See *supra* note 52 (discussion of rollback attacks). This is not the only vulnerability that can be exploited in backward compatible phones. An active surveillance device can extract the cryptographic keys associated with particular targeted handsets. This cryptographic key material can then be used to either decrypt call data that had been previously recorded and retained, or used in tandem with a passive interception device to perform real-time interception in the future. See ABILITY COMPUTERS & SOFTWARE INDUS. LTD., *supra* note 42.

368. See *3G UMTS IMSI Catcher*, PKI (last visited Dec. 18, 2014), <http://www.pki-electronic.com/products/interception-and-monitoring-systems/3g-umts-imsi-catcher/> (“With our 3G UMTS IMSI Catcher you can redirect single UMTS mobile phones to specific GSM frequencies, in order to monitor the conversation with our active or passive cellular monitoring systems.”); *3G-GSM Tactical Interception & Target Location*, GAMMA GROUP, at 40 (2011), available at <http://info.publicintelligence.net/Gamma-GSM.pdf> (“This device will emulate a 3G network to attract 3G mobiles and, for designated Targets, selectively push them to GSM where they remain unless they are rebooted or pushed back to 3G by the GSM system.”).

369. See Cyrus Farivar, *Cities Scramble To Upgrade “Stingray” Tracking as End of 2G Network Looms*, ARS TECHNICA (Sept. 1, 2014), <http://arstechnica.com/tech-policy/2014/09/cities-scramble-to-upgrade-stingray-tracking-as-end-of-2g-network-looms/>; Purchase Order, *PIID: DJD13HQG0264*, DRUG ENFORCEMENT AGENCY (Mar. 5, 2014), available at http://usaspending.gov/explore?fiscal_year=all&comingfrom=searchresults&

grates away from 2G, many other law enforcement agencies will respond by upgrading from the 2G StingRay to the 4G Hailstorm. For the many state and local law enforcement agencies that presumably only use cellular surveillance devices to identify and track phones, not to intercept communications, the 4G migration will require the purchase of new, expensive surveillance equipment, but ultimately should not impact their technical surveillance capabilities.

Moreover, while 4G surveillance devices are currently very expensive,³⁷⁰ they will, of course, become cheaper over time and easier for private parties to purchase, as with prior generations of surveillance technology. Indeed, foreign companies are already openly advertising 4G surveillance products.³⁷¹ As a result, even though the wireless carriers may eventually be able to protect their customers' communications from unmediated interception, cell phones will likely remain vulnerable to remote identification and tracking, whether by law enforcement agencies, foreign intelligence services, or criminals.

B. "Over-the-Top" Secure Communication Apps

It is possible to deliver secure communications over an insecure network. The HTTPS encryption built into web browsers, which is used to secure data transmitted to and from websites, does just that, enabling someone safely to check her bank balance or to read her email on a public WiFi network where they would otherwise be vulnerable to WiFi interception.³⁷² Just as the security of Bank of America or Google's websites does not depend on their customers' using secure WiFi networks, so too can the audio and text communications of smartphone users be protected by apps that supply their own encryption, even when the underlying cellular network remains vulnerable to interception.

Smartphone apps already exist, some with hundreds of millions of existing users,³⁷³ which use encryption to protect their users' text,

piid=DJD13HQG0264&typeofview=complete ("Sting[R]ay [II] to Hailstorm Upgrade, ETC. The Hailstorm Upgrade is Necessary for the Sting[R]ay System to Track 4g Lte Phones . . .").

370. See Kelly, *supra* note 21 ("The cell-tracking systems [purchased by U.S. law enforcement agencies] cost as much as \$400,000, depending on when they were bought and what add-ons they have. The latest upgrade, code-named 'Hailstorm,' is spurring a wave of upgrade requests.").

371. See 4G/LTE IMSI/IMEI CATCHER, GSMSOFT (Oct. 3, 2014), http://www.gsmssoft.com.ua/security_4g_ct ("The basic unit of the system is a 4G/LTE module which provides communication with the corresponding types of mobile phones. It also creates a fake BTS (Node B) with the best operation parameters for 4G/LTE communication.").

372. See Murphy, *supra* note 256.

373. See Mikey Campbell, *Apple Sees 2 Billion iMessages Sent Daily from Half a Billion iOS Devices*, APPLE INSIDER (Jan. 23, 2013) <http://appleinsider.com/articles/13/01/23/apple-sees-2b-imessages-sent-every-day-from-half-a-billion-ios-devices>; Derek Snyder, *Skype*

voice, and video communications as they are transmitted over the Internet. Examples of such apps include Microsoft's Skype,³⁷⁴ Apple's FaceTime and iMessage,³⁷⁵ Google's Hangouts³⁷⁶ and Facebook's WhatsApp.³⁷⁷ These apps use the cellular data network, rather than the wireless carriers' legacy voice and text message systems, to transmit content. In many cases, these are available as third-party apps that individuals must download from an app store. However, smartphone operating system companies including Apple and Google pre-install their own communications apps on devices running their respective operating systems. In some cases, these apps are even enabled by default and seamlessly encrypt communications without requiring any configuration by the user.³⁷⁸

Passes 100M Android Installs and Launches Redesigned 4.0, SKYPE BIG BLOG (July 1, 2013), <http://blogs.skype.com/2013/07/01/skype-passes-100m-android-installs-and-launches-redesigned-4-0/>; Daisuke Wakabayashi, *Cook Raises, Dashes Hopes for Excitement at Apple Annual Meeting*, WALL ST. J. (Feb. 28, 2014), <http://blogs.wsj.com/digits/2014/02/28/cook-raises-dashes-hopes-for-excitement-at-apple-annual-meeting/> ("Apple said it sends 'several billion' messages on its iMessage service every day. Apple said users also send 15 million to 20 million FaceTime messages every day.").

374. *Frequently Asked Questions — Does Skype Use Encryption*, SKYPE (last visited Dec. 13, 2014), <https://support.skype.com/en/faq/FA31/does-skype-use-encryption> ("All Skype-to-Skype voice, video, file transfers and instant messages are encrypted. This protects you from potential eavesdropping by malicious users."). *But see* Glenn Greenwald et al., *Microsoft Handed the NSA Access to Encrypted Messages*, GUARDIAN (July 12, 2013), <http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data> (revealing that Skype was served "with a directive to comply signed by the attorney general" and the NSA has since been able to intercept Skype video and audio communications).

375. *See We've Built Privacy into the Things You Use Every Day*, APPLE (last visited Dec. 18, 2014), <http://www.apple.com/privacy/privacy-built-in/> ("Your communications are protected by end-to-end encryption across all your devices when you use iMessage and FaceTime Apple has no way to decrypt iMessage and FaceTime data when it's in transit between devices . . . and we wouldn't be able to comply with a wiretap order even if we wanted to.").

376. *How Hangouts Encrypts Information*, GOOGLE (last visited Dec. 18, 2014), <https://support.google.com/hangouts/answer/6046115?hl=en>.

377. *See* Ellen Nakashima, *WhatsApp, Most Popular Instant-Messaging Platform, To Encrypt Data for Millions*, WASH. POST (Nov. 18, 2014), http://www.washingtonpost.com/world/national-security/whatsapp-worlds-most-popular-instant-messaging-platform-to-encrypt-data-for-millions/2014/11/18/b8475b2e-6ee0-11e4-ad12-3734c461eab6_story.html ("Open Whisper Systems, a group of software developers, said Tuesday it had partnered with Silicon Valley's WhatsApp to build in end-to-end encryption that will make it impossible for foreign governments and U.S. agencies to intercept text messages, even with a warrant."); Andy Greenberg, *WhatsApp Just Switched on End-to-End Encryption for Hundreds of Millions of Users*, WIRED (Nov. 18, 2014), <http://www.wired.com/2014/11/whatsapp-encrypted-messaging/> ("The result is practically uncrackable encryption for hundreds of millions of phones and tablets that have WhatsApp installed — by some measures the world's largest-ever implementation of this standard of encryption in a messaging service.").

378. For example, since 2011, Apple's iOS operating system has used its own iMessage service for all text messages sent between iOS devices. Such text messages are, without requiring any configuration or special action by the user, encrypted and sent over the Internet using Apple's servers, rather than using the wireless carrier's text message servers. *See* Andy Greenberg, *Apple Claims It Encrypts iMessages and Facetime so That Even Its*

Communications made using these apps cannot be intercepted using the surveillance devices discussed in this Article. Moreover, some services, such as Apple's iMessage and FaceTime, Facebook's WhatsApp, and a few other third-party apps that encrypt messages end-to-end, protect against interception not only by wireless carriers and, Internet Service Providers, but also by the companies that provide these apps.³⁷⁹ Indeed, end-to-end encryption technology protects the contents of user communications from interception by all but the most skilled actors.³⁸⁰

Even so, most of these apps, particularly those made by the largest technology companies, do not openly advertise the security advantages of their services. Instead, they typically compete on cost or ease of use. Once the ease with which cellular communications can be intercepted becomes known to more consumers, however, those companies with widely used communications apps are well-placed to compete and deliver a more secure communications experience to consumers.

C. Counter-Surveillance Technology

The FBI, which acts as the national coordinator for law enforcement use of cellular surveillance technology,³⁸¹ has insisted that information about the technology must be kept secret to avoid "provid[ing] adversaries with critical information . . . necessary to develop defensive technology, modify their behaviors and otherwise take countermeasures designed to thwart the use of this technology."³⁸² It may be too late. Indeed, some of the biggest players in the cellular surveillance market have already sought patents, and thus filed public applications describing, in significant detail, techniques

Can't Decipher Them, FORBES (June 17, 2013), <http://www.forbes.com/sites/andygreenberg/2013/06/17/apple-claims-it-encrypts-imessages-and-facetime-so-that-even-it-can't-read-them/>; Greenberg, *supra* note 377 (describing the implementation of WhatsApp's new encryption scheme as "totally frictionless").

379. See *We've Built Privacy into the Things You Use Every Day*, *supra* note 375; Nakashima, *supra* note 377.

380. Even when communications are encrypted, it is still possible for a determined adversary (such as a law enforcement or intelligence agency) to intercept those communications. By infecting the end-point (such as a mobile phone or laptop used by one of the callers) with specially designed surveillance software, sophisticated actors can obtain unencrypted audio, video, and text communications from a target's device. U.S. law enforcement and intelligence agencies already use such software. See Jennifer Valentino-DeVries & Danny Adron, *FBI Taps Hacker Tactics To Spy on Suspects*, WALL ST. J. (Aug. 3, 2013), <http://online.wsj.com/news/articles/SB10001424127887323997004578641993388259674> ("The FBI develops some hacking tools internally and purchases others from the private sector. With such technology, the bureau can remotely activate the microphones in phones running Google Inc.'s Android software to record conversations . . . It can do the same to microphones in laptops without the user knowing . . .").

381. See FCC REPORT AND ORDER, *supra* note 9.

382. Morrison Affidavit 2014, *supra* note 174.

that can detect active cellular surveillance devices.³⁸³ Although it is unlikely that these companies will sell their counter-surveillance products to the general public, there are now a number of other ways for individuals to acquire software or devices capable of detecting cellular surveillance technology.

Over the past several years, several academic researchers and boutique security companies have created their own “IMSI catcher catcher” counter-surveillance products. The first public project, which was released by researchers in 2011, was extremely difficult to use, requiring the user to replace the operating system on a widely available \$15 Motorola phone with custom software.³⁸⁴ According to the researchers who developed the software, IMSI catchers show different behavior from normal base stations to achieve their goals. The software “distinguish[es] between yellow, red, and black flags. Yellow flags are an indication that you might have been caught; red flags are a very strong indication; and black flags tell you: ‘You are being tracked down; throw away your phone and run.’”³⁸⁵ A few years later, a different team of researchers released an Android app for the popular Samsung Galaxy S3 smartphone capable of detecting IMSI catchers. In contrast to the earlier effort, use of this app did not require that the user replace their entire phone operating system.³⁸⁶ The app is available from Google’s App Store, and can be easily installed by anyone in just a few steps.³⁸⁷

In spite of the FBI’s efforts, the tools and information necessary to detect cellular surveillance devices are now public. Academics have published peer-reviewed research describing novel techniques to detect cellular surveillance,³⁸⁸ MIT students in 2014, as a class project, built their own counter-surveillance app,³⁸⁹ and boutique security

383. See Jeffrey F. Bull & Matthew L. Ward, *Interference Detection, Characterization and Location in a Wireless Communications or Broadcast System*, GOOGLE (Dec. 11, 2009), <https://www.google.com/patents/WO2010077790A1>; Ethan Goldfarb, *Systems and Methods for Identifying Rogue Base Stations*, GOOGLE (Apr. 30, 2013), <https://www.google.com/patents/EP2661113A1>.

384. See Krempel, *supra* note 226; *CatcherCatcher*, SECURITY RESEARCH LABS (last visited Dec. 18, 2014), <https://opensource.srlabs.de/projects/mobile-network-assessment-tools/wiki/CatcherCatcher>.

385. See *CatcherCatcher*, *supra* note 384.

386. See Ravishankar Borgaonkar, *Understanding IMSI Privacy*, BLACKHAT USA 2014 (Aug. 7, 2014), <https://www.isti.tu-berlin.de/fileadmin/fg214/ravi/Darshak-bh14.pdf>; *Darshak*, GITHUB (last visited Dec. 18, 2014), <https://github.com/darshakframework/darshak/>.

387. See *Darshak*, GOOGLE PLAY (last visited Dec. 18, 2014), <https://play.google.com/store/apps/details?id=com.darshak&hl=en>.

388. See Adrian Dabrowski et al., *IMSI-Catch Me If You Can: IMSI-Catcher-Catchers*, in ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE (ACSAC) 2014 (Dec. 8–12, 2014), available at <https://www.sba-research.org/wp-content/uploads/publications/AdrianDabrowski-IMSI-Catcher-Catcher-ACSAC2014-preprint-20140820.pdf>.

389. See Jeffrey Warren, *ACLU + the Guardian Project Final Project*, CODESIGN (May 18, 2014), <http://codesign.mit.edu/2014/05/aclu-the-guardian-project-final-project/>.

companies now openly sell, to the general public, surveillance-resistant smartphones with built-in counter-surveillance features.³⁹⁰ Although, for now, such features are not built into the popular Android and Apple smartphones that most consumers use, they may be in the future as big Silicon Valley technology companies begin to compete openly on privacy and security.³⁹¹

X. CONCLUSION

This Article has illustrated how cellular interception capabilities and technology has become, for better or worse, globalized and democratized, placing Americans' cellular communications at risk of interception by foreign governments, criminals, and the tabloid press, to mention a few. Notwithstanding this risk, U.S. government agencies shroud almost every aspect of the StingRay and similar direct interception technology in secrecy, in an ostensible but futile effort to prevent criminals from learning how to thwart the technology. But this narrative, which disingenuously asserts a continuing need for secrecy regarding StingRay technology, does greater harm by inhibiting public awareness and discussion of the risks associated with private use of unmediated surveillance technologies, thus preventing policymakers from addressing the underlying vulnerabilities in cellular networks. Those who cling to the position that a demonstrably illusory veil of secrecy is essential to protect the utility of surveillance capabilities, and who, as a consequence, suppress information necessary to a full public discussion of cellular network security, effectively undermine broader congressional efforts to strengthen cybersecurity. This unnecessary and counterproductive veil must be lifted so that the public and legislators can address the full scope of interception risks in a public policy process that will promote better, stronger cybersecurity practices.

390. E.g., *Cryptophone*, GSMK (last visited Dec. 18, 2014), <http://www.cryptophone.de/>; *Stealth Phone*, X-CELLULAR (last visited Dec. 18, 2014), <http://x-cellular.com/phones.html>.

391. See Craig Timberg, *Apple Will No Longer Unlock Most iPhones, iPads for Police, Even with Search Warrants*, WASH. POST (Sept. 18, 2014), http://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html; Craig Timberg, *Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police*, WASH. POST (Sept. 18, 2014), <http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/>; Matthew Green, *Is Apple Picking a Fight with the U.S. Government? Not Exactly*, SLATE (Sept. 23, 2014), http://www.slate.com/articles/technology/future_tense/2014/09/ios_8_encryption_why_apple_won_t_unlock_your_iphone_for_the_police.html ("Apple is not designing systems to prevent law enforcement from executing legitimate warrants. It's building systems that prevent everyone who might want your data — including hackers, malicious insiders, and even hostile foreign governments — from accessing your phone.").

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 76 of 76

MAIN MENU ▾

MY STORIES: 25 ▾

FORUMS

SUBSCRIBE

JOBS

ARS CONSORTIUM

LAW & DISORDER / CIVILIZATION & DISCONTENTS

Meet the machines that steal your phone's data

Keeping tabs on civilian phones? There's more than one way to skin that cat.

by Ryan Gallagher - Sep 25, 2013 12:00pm CDT

94



Aurich Lawson / HBO

The National Security Agency's spying tactics are being intensely scrutinized following the recent leaks of secret documents. However, the NSA isn't the only US government agency using controversial surveillance methods.

Monitoring citizens' cell phones without their knowledge is a booming business. From Arizona to California, Florida to Texas, state and federal authorities have been quietly investing millions of dollars acquiring clandestine mobile phone surveillance equipment in the past decade.

Earlier this year, a covert tool called the "Stingray" that can gather data from hundreds of phones over targeted areas attracted [international attention](#). Rights groups alleged that its use could be unlawful. But the same company that exclusively manufacturers the Stingray—Florida-based [Harris Corporation](#)—has for years been selling government agencies an entire range of secretive mobile phone surveillance technologies from a catalogue that it conceals from the public on national security grounds.

Details about the devices are not disclosed on the Harris website, and marketing materials come with a warning that anyone distributing them outside law enforcement agencies or telecom firms could be committing a crime punishable by up to five years in jail.

These little-known cousins of the Stingray cannot only track movements—they can also perform denial-of-service attacks on phones and intercept conversations. Since 2004, Harris has earned more than \$40 million from spy technology contracts with city, state, and federal authorities in the US, according to procurement records.

In an effort to inform the debate around controversial covert government tactics, Ars has compiled a list of this equipment by scrutinizing publicly available purchasing contracts published on government websites and marketing materials obtained through equipment resellers. Disclosed, in some cases for the first time, are photographs of the Harris spy tools, their cost, names, capabilities, and the agencies known to have purchased them.

Exhibit 1-K

What follows is the most comprehensive picture to date of the mobile phone surveillance technology that has been deployed in the US over the past decade.

“Stingray”

The Stingray has become the most widely known and contentious spy tool used by government agencies to track mobile phones, in part due to an Arizona court case that [called the legality of its use into question](#). It's a box-shaped portable device, sometimes described as an “IMSI catcher,” that gathers information from phones by sending out a signal that tricks them into connecting to it. The Stingray can be covertly set up virtually anywhere—in the back of a vehicle, for instance—and can be used over a targeted radius to collect hundreds of unique phone identifying codes, such as the International Mobile Subscriber Number (IMSI) and the Electronic Serial Number (ESN). The authorities can then hone in on specific phones of interest to monitor the location of the user in real time or use the spy tool to log a record of all phones in a targeted area at a particular time.

The FBI uses the Stingray to track suspects and says that it does not use the tool to intercept the content of communications. However, this capability does exist. Procurement documents indicate that the Stingray can also be used with software called “[FishHawk](#),” (PDF) which boosts the device’s capabilities by allowing authorities to

**ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CCH-5338
PAGE 208**
eavesdrop on conversations. Other similar Harris software includes “[Porpoise](#),” which is sold on a USB drive and is designed to be installed on a laptop and used in conjunction with transceivers—possibly including the Stingray—for surveillance of text messages.

Similar devices are sold by other government spy technology suppliers, but US authorities appear to buy Harris equipment exclusively. They've awarded the company “sole source” contracts because its spy tools provide capabilities that authorities claim other companies do not offer. The Stingray has become so popular, in fact, that “Stingray” has become a generic name used informally to describe all kinds of IMSI catcher-style devices.

First used: [Trademark records](#) show that a registration for the Stingray was first filed in August 2001. Earlier versions of the technology—sometimes described as “digital analyzers” or “cell site simulators” by the FBI—were being deployed in the mid-1990s. An upgraded version of the Stingray, named the “Stingray II,” was introduced to the spy tech market by Harris Corp. between 2007 and 2008. Photographs filed with the US Patent and Trademark Office depict the Stingray II as a more sophisticated device, with many additional USB inputs and a switch for a “GPS antenna,” which is likely used to assist in location tracking.

Cost: \$68,479 for the original Stingray; \$134,952 for Stingray II.

Agencies: Federal authorities have spent more than \$30 million on Stingrays and related equipment and training since 2004, according to procurement records. Purchasing agencies include the FBI, DEA, Secret Service, US Immigration and Customs Enforcement, the Internal Revenue Service, the Army, and the Navy. Cops in Arizona, Maryland, Florida, North Carolina, Texas, and California have also either purchased or considered purchasing the devices, according to public records. In one case, [procurement records](#) (PDF) show cops in Miami obtained a Stingray to monitor phones at a free trade conference held in Miami in 2003.

“Gossamer”

The Gossamer is a small portable device that can be used to secretly gather data on mobile phones operating in a target area. It sends out a covert signal that tricks phones into handing over their unique codes—such as the [IMSI](#) and [TMSI](#)—which can be used to identify users and home in on specific devices of interest. What makes it different from the Stingray? Not only is the Gossamer much smaller, but it can also be used to perform a denial-of-service attack on phone users, blocking targeted people from making or receiving calls, according to [marketing materials](#) (PDF) published by



[Enlarge](#)

a Brazilian reseller of the Harris equipment. The Gossamer has the appearance of a clunky-looking handheld transceiver. One photograph filed with the US Patent and Trademark Office shows it displaying an option for "mobile interrogation" on its small LCD screen, which sits above a telephone-style keypad.

First used: Trademark records show that a registration for the Gossamer was first filed in October 2001.

Cost: \$19,696.

Agencies: Between 2005 and 2009, the FBI, Special Operations Command, and Immigration and Customs Enforcement spent more than \$1.3 million purchasing Harris' Gossamer technology and upgrading existing Gossamer units, according to procurement records. Most of the \$1.3 million was spent by the FBI as part of a large contract in 2005.



PAGE: 1 **2** NEXT →

READER COMMENTS 94

2462

887

170

756

← OLDER STORY

NEWER STORY →

MAIN MENU ▾

MY STORIES: 25 ▾

FORUMS

SUBSCRIBE

JOBS

ARS CONSORTIUM

LAW & DISORDER / CIVILIZATION & DISCONTENTS

Meet the machines that steal your phone's data

Keeping tabs on civilian phones? There's more than one way to skin that cat.

by Ryan Gallagher - Sep 25, 2013 12:00pm CDT

94

“Triggerfish”

The Triggerfish is an eavesdropping device. It allows authorities to covertly intercept mobile phone conversations in real time. This sets it apart from the original version of the Stingray, which marketing documents suggest was designed mainly for location monitoring and gathering metadata (though software can allow the Stingray to eavesdrop). The Triggerfish, which looks similar in size to the Stingray, can also be used to identify the location from which a phone call is being made. It can gather large amounts of data on users over a targeted area, allowing authorities to identify codes of up to 60,000 different phones at one time, according to marketing materials.



[Enlarge](#)

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014CH15336
PAGE 40

First used: Trademark records show that a registration for the Triggerfish was filed in July 2001, though its “first use anywhere” is listed as November 1997. It is not clear whether the Triggerfish is still for sale or whether its name has recently changed, as the trademark on the device was canceled in 2008, and it does not appear on Harris’ current federal price lists.

Cost: Between \$90,000 and \$102,000.

Agencies: The Bureau of Alcohol, Tobacco, Firearms, and Explosives; the DEA; and county cops in Miami-Dade invested in Triggerfish technology prior to 2004, according to procurement records. However, the [procurement records](#) (PDF) also show that the Miami-Dade authorities complained that the device “provided access” only to Cingular and AT&T wireless network carriers. (This was before the two companies merged.) To remedy that, the force complemented the Triggerfish tool with additional Harris technology, including the Stingray and Amberjack, which enabled monitoring of Metro PCS, Sprint, and Verizon. This gave the cops “the ability to track approximately ninety percent of the wireless industry,” the procurement documents state.

“Kingfish”

The Kingfish is a surveillance transceiver that allows authorities to track and mine information from mobile phones over a targeted area. The device does not appear to enable interception of communications; instead, it can covertly gather unique identity codes and show connections between phones and numbers being dialed. It is smaller than the Stingray, black and gray in color, and can be controlled wirelessly by a conventional notebook PC using Bluetooth. You can even conceal it in a discreet-looking briefcase, according to marketing brochures.



[Enlarge](#)

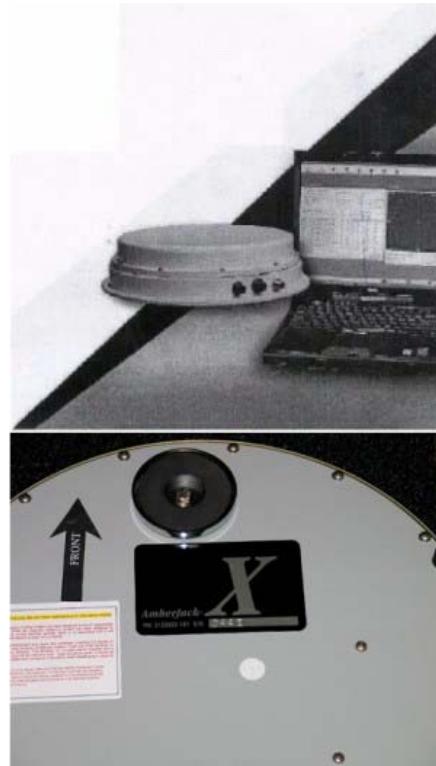
First used: Trademark records show that a registration for the Kingfish was filed in August 2001. Its "first use anywhere" is listed in records as December 2003.

Cost: \$25,349.

Agencies: Government agencies have spent about \$13 million on Kingfish technology since 2006, sometimes as part of what is described in procurement documents as a "vehicular package" deal that includes a Stingray. The US Marshals Service; Secret Service; Bureau of Alcohol, Tobacco, Firearms, and Explosives; Army; Air Force; state cops in Florida; county cops in Maricopa, Arizona; and Special Operations Command have all purchased a Kingfish in recent years.

"Amberjack"

The Amberjack is an antenna that is used to help track and locate mobile phones. It is designed to be used in conjunction with the Stingray, Gossamer, and Kingfish as a "direction-finding system" (PDF) that monitors the signal strength of the targeted phone in order to home in on the suspect's location in real time. The device comes inbuilt with magnets so it can be attached to the roof of a police vehicle, and it has been designed to have a "low profile" for covert purposes. A photograph of the Amberjack filed with a trademark application reveals that the device, which is metallic and circular in shape, comes with a "tie-down kit" to prevent it from falling off the roof of a vehicle that is being driven at "highway speeds."



[Enlarge](#)

ELECTRONICALLY FILED
7/2/2015 12:12 PM
7/2/2015-CHE-1528
15 PAGES

First used: Trademark records show that a registration for the Amberjack was filed in August 2001 at the same time as the Stingray. Its "first use anywhere" is listed in records as October 2002.

Cost: \$35,015

Agencies: The DEA; FBI; Special Operations Command; Secret Service; the Navy; the US Marshals Service; and cops in North Carolina, Florida, and Texas have all purchased Amberjack technology, according to procurement records.

"Harpoon"

The Harpoon is an "amplifier" (PDF) that can boost the signal of a Stingray or Kingfish device, allowing it to project its surveillance signal farther or from a greater distance depending on the location of the targets. A photograph filed with the US Patent and Trademark Office shows that the device has two handles for carrying and a silver, metallic front with a series of inputs that allow it to be connected to other mobile phone spy devices.



[Enlarge](#)

First used: Trademark records show that a filing for the Harpoon was filed in June 2008.

Cost: \$16,000 to \$19,000.

Agencies: The DEA; state cops in Florida; city cops in Tempe, Arizona; the Army; and the Navy are among those to have purchased Harpoons since 2009.

"Hailstorm"

The Hailstorm is the latest in the line of mobile phone tracking tools that Harris Corp. is offering authorities. However, few details about it have trickled into the public domain. It can be purchased as a standalone unit or as an upgrade to the Stingray or Kingfish, which suggests that it has the same

functionality as these devices but has been tweaked with new or more advanced capabilities. [Procurement documents](#) (PDF) show that Harris Corp. has, in at least one case, recommended that authorities use the Hailstorm in conjunction with software made by Nebraska-based surveillance company [Pen-Link](#). The Pen-Link software appears to enable authorities deploying the Hailstorm to directly communicate with cell phone carriers over an Internet connection, possibly to help coordinate the surveillance of targeted individuals.

First used: Unknown.

Cost: \$169,602 as a standalone unit. The price is reduced when purchased as an upgrade.

Agencies: Public records show that earlier this year, the Baltimore Police Department, county cops in Oakland County, Michigan, and city cops in Phoenix, Arizona, each separately entered the procurement process to obtain the Hailstorm equipment. The Baltimore and Phoenix forces each set aside about \$100,000 for the device, and they purchased it as an upgrade to Stingray II mobile phone spy technology. The Phoenix cops spent an additional \$10,000 on Hailstorm training sessions conducted by Harris Corp. in Melbourne, Florida, and Oakland County authorities said they obtained a grant from the Department of Homeland Security to help finance the procurement of the Hailstorm tool. The Oakland authorities noted that the device was needed for "pinpoint tracking of criminal activity." It is highly likely that other authorities—particularly federal agencies—will invest in the Hailstorm too, with procurement records eventually surfacing later this year or into 2014.

No one's talking

Ars contacted the agencies most frequently referenced above, including the FBI; the DEA; the Bureau of Alcohol, Tobacco, Firearms, and Explosives; the Secret Service; and Immigration and Customs Enforcement. Our requests for comment were either not returned or rebuffed on the grounds that the topic is "law enforcement sensitive." Harris Corp. also turned down an interview request and declined to answer any questions for this story.

The FBI has [previously](#) stated in response to questions about the Stingray device that it "strives to protect our country and its people using every available tool" and that location data in particular is a "critical component" of investigations. But when it comes to discussing specific surveillance equipment, it's common for the authorities to remain tight-lipped because they don't want to reveal tactics to criminals.

The code of silence shrouding the above tools, however, is highly contentious. Their use by law enforcement agencies is in a legal gray zone, particularly because interference with communications signals is supposed to be prohibited under the federal [Communications Act](#). In May, an Arizona court [ruled](#) that the FBI's use of a Stingray was lawful in a case involving conspiracy, wire fraud, and identity theft. But according to the American Civil Liberties Union (ACLU), when seeking authorization for the use of the Stingray tool, the feds have sometimes unlawfully [withheld information](#) from judges about the full scope of its capabilities. This means that judges across the country are potentially authorizing the use of the technology without even knowing what it actually does.

That's not all. There is another significant issue raised by the Harris spy devices: security. According to Christopher Soghoian, chief technologist at the ACLU, similar covert surveillance technology is being manufactured by a host of companies in other countries like China and Russia. He believes the US government's "state secrecy" on the subject is putting Americans at risk.

"Our government is sitting on a security flaw that impacts every phone in the country," Soghoian says. "If we don't talk about Stingray-style tools and the flaws that they exploit, we can't defend ourselves against foreign governments and criminals using this equipment, too."

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CR-1328
PAGE 6 OF 6

PAGE: 1 2

READER COMMENTS 94

2462

887

170

756

← OLDER STORY

NEWER STORY →

11/13/14 Denv. Post Zo
2014 WLNR 32235603

Denver Post (CO)
Copyright © 2014 The Denver Post

November 13, 2014

Section: Z

Americans' cellphones targeted in secret U.S. spy program

Devlin Barrett; The Wall Street Journal

WASHINGTON The Justice Department is scooping up data from thousands of cellphones through fake communications towers deployed on airplanes, a high-tech hunt for criminal suspects that is snagging a large number of innocent Americans, according to people familiar with the operations.

The U.S. Marshals Service program, which became fully functional around 2007, operates Cessna aircraft from at least five metropolitan-area airports, with a flying range covering most of the U.S. population, according to people familiar with the program.

Planes are equipped with devices -- some known as "dirtboxes" to law-enforcement officials because of the initials of the Boeing Co. unit that produces them -- which mimic cell towers of large telecommunications firms and trick cellphones into reporting their unique registration information.

The technology in the two-foot-square device enables investigators to scoop data from tens of thousands of cellphones in a single flight, collecting their identifying information and general location, these people said.

People with knowledge of the program wouldn't discuss the frequency or duration of such flights, but said they take place on a regular basis.

A Justice Department official would neither confirm nor deny the existence of such a program. The official said discussion of such matters would allow criminal suspects or foreign powers to determine U.S. surveillance capabilities. Justice Department agencies comply with federal law, including by seeking court approval, the official said.

The program is the latest example of the extent to which the U.S. is training its surveillance lens inside the U.S. It is similar in approach to the National Security Agency's program to collect millions of Americans phone records, in that it scoops up large volumes of data in order to find a single person or a handful of people. The U.S. government justified the phone-records collection by arguing it is a minimally invasive way of searching for terrorists.

Christopher Soghoian, chief technologist at the American Civil Liberties Union, called it "a dragnet surveillance program. It's inexcusable and it's likely -- to the extent judges are authorizing it -- [that] they have no idea of the scale of it."

Exhibit 1-L

Cellphones are programmed to connect automatically to the strongest cell tower signal. The device being used by the U.S. Marshals Service identifies itself as having the closest, strongest signal, even though it doesn't, and forces all the phones that can detect its signal to send in their unique registration information. Even having encryption on one's phone, such as Apple Co.'s iPhone 6 now includes, doesn't prevent this process.

The technology is aimed at locating cellphones linked to individuals under investigation by the government, including fugitives and drug dealers, but it collects information on cellphones belonging to people who aren't criminal suspects, these people said. They said the device determines which phones belong to suspects and "lets go" of the non-suspect phones.

The device can briefly interrupt calls on certain phones. Authorities have tried to minimize the potential for harm, including modifying the software to ensure the fake tower doesn't interrupt anyone calling 911 for emergency help, one person familiar with the matter said.

The program cuts out phone companies as an intermediary in searching for suspects. Rather than asking a company for cell-tower information to help locate a suspect, which law enforcement has criticized as slow and inaccurate, the government can now get that information itself. People familiar with the program say they do get court orders to search for phones, but it isn't clear if those orders describe the methods used because the orders are sealed.

Also unknown are the steps taken to ensure data collected on innocent people isn't kept for future examination by investigators. A federal appeals court ruled earlier this year that over-collection of data by investigators, and stockpiling of such data, was a violation of the Constitution.

The program is more sophisticated than anything previously understood about government use of such technology. Until now, the hunting of digital trails created by cellphones had been thought limited to devices carried in cars that scan the immediate area for signals. Civil-liberties groups are suing for information about use of such lower-grade devices, some of them called stingrays, by the Federal Bureau of Investigation.

By taking the program airborne, the government can sift through a greater volume of information and with greater precision, these people said. If a suspect's cellphone is identified, the technology can pinpoint its location within about three meters, down to a specific room in a building. Newer versions of the technology can be programmed to do more than suck in data: They can also jam signals and retrieve data from a target phone such as texts or photos. It isn't clear if this domestic program has ever used those features.

Similar devices are used by U.S. military and intelligence officials operating in other countries, including in war zones, where they are sometimes used to locate terrorist suspects, according to people familiar with the work. In the U.S., these people said, the technology has been effective in catching suspected drug dealers and killers. They wouldn't say which suspects were caught through this method.

The scanning is done by the Technical Operations Group of the U.S. Marshals Service, which tracks fugitives, among other things. Sometimes it deploys the technology on targets requested by other parts of the Justice Department.

Within the Marshals Service, some have questioned the legality of such operations and the internal safeguards, these people said. They say scooping up of large volumes of information, even for a short period, may not be properly understood by judges who approve requests for the government to locate a suspect's phone.

Some within the agency also question whether people scanning cellphone signals are doing enough to minimize intrusions into the phone system of other citizens, and if there are effective procedures in place to safeguard the handling of that data.

It is unclear how closely the Justice Department oversees the program. "What is done on U.S. soil is completely legal," said one person familiar with the program. "Whether it should be done is a separate question."

Referring to the more limited range of Stingray devices, Mr. Soghoian of the ACLU said: "Maybe it's worth violating privacy of hundreds of people to catch a suspect, but is it worth thousands or tens of thousands or hundreds of thousands of peoples' privacy?"

The existence of the cellphone program could escalate tensions between Washington and technology companies, including the telecom firms whose devices are being redirected by the program.

If a suspect is believed to have a cellphone from Verizon Inc., for example, the device would emit a signal fooling Verizon phones and those roaming on Verizon's network into thinking the plane is the nearest available Verizon cell tower. Phones that are turned on, even if not in use, would "ping" the flying device and send their registration information. In a densely populated area, the dirtbox could pick up data of tens of thousands of cellphones.

The approach is similar to what computer hackers refer to as a "man in the middle" attack, in which a person's electronic device is tricked into thinking it is relaying data to a legitimate or intended part of the communications system.

A Verizon spokesman said the company was unaware of the program. "The security of Verizon's network and our customers' privacy are top priorities," the spokesman said. "However, to be clear, the equipment referenced in the article is not Verizon's and is not part of our network."

An AT&T Inc. spokeswoman declined to comment, as did a spokeswoman for Sprint Corp.

For cost reasons, the flights usually target a number of suspects at a time, rather than just a single fugitive. But they can be used for a single suspect if the need is great enough to merit the resources, these people said.

The dirtbox and Stingray are both types of what tech experts call "ISMI catchers," named for the identification system used by networks to identify individual cellphones.

The name "dirtbox" came from the acronym of the company making the device, DRT, for Digital Recovery Technology Inc., people said. DRT is now a subsidiary of Boeing. A Boeing spokeswoman declined to comment.

"DRT has developed a device that emulates a cellular base station to attract cellphones for a registration process even when they are not in use," according to a 2010 regulatory filing Boeing made with the U.S. Commerce Department, which touted the device's success in finding contraband cellphones smuggled in to prison inmates.

---- Index References ----

News Subject: (Major Corporations (1MA93))

Industry: (Consumer Electronics (1CO61); Consumer Products & Services (1CO62); Electronic Components (1EL91); Electronics (1EL16); I.T. (1IT96); Mobile Phones & Pagers (1WI07); Networking (1NE45); Next Generation Wireless Technology (1NE48); Semiconductor (1SE88); Semiconductor Products (1SE02); Telecom (1TE27); Telecom Carriers & Operators (1TE56); Telecom Consumer Equipment (1TE03); Wireless Networking (1WI62); Wireless Semiconductors & Components (1WI91))

Language: EN

Other Indexing: (Christopher Soghoian)

Edition: UNK

Word Count: 1422

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

NewsRoom

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 4 of 4

June 30, 2015

2014-CH-15338

CALENDAR: 11

PAGE 1 of 4

CIRCUIT COURT OF
COOK COUNTY, ILLINOIS
CHANCERY DIVISION
CLERK DOROTHY BROWN

FBI Confirms Wide-Scale Use Of Surveillance Flights Over U.S. Cities

AP | By JACK GILLUM, EILEEN SULLIVAN and ERIC TUCKER

Posted: 06/02/2015 3:07 am EDT | Updated: 06/03/2015 1:59 am EDT



WASHINGTON (AP) -- The FBI is operating a small air force with scores of low-flying planes across the U.S. carrying video and, at times, cellphone surveillance technology -- all hidden behind fictitious companies that are fronts for the government, The Associated Press has learned.

The planes' surveillance equipment is generally used without a judge's approval, and the FBI said the flights are used for specific, ongoing investigations. In a recent 30-day period, the agency flew above more than 30 cities in 11 states across the country, an AP review found.

Aerial surveillance represents a changing frontier for law enforcement, providing what the government maintains is an important tool in criminal, terrorism or intelligence probes. But the program raises questions about whether there should be updated policies protecting civil liberties as new technologies pose intrusive opportunities for government spying.

The FBI confirmed for the first time the wide-scale use of the aircraft, which the AP traced to at least 13 fake companies, such as FVX Research, KQM Aviation, NBR Aviation and PXW Services. Even basic aspects of the program are withheld from the public in censored versions of official reports from the Justice Department's inspector general.

"The FBI's aviation program is not secret," spokesman Christopher Allen said in a statement. "Specific aircraft and their capabilities are protected for operational security purposes." Allen added that the FBI's planes "are not equipped, designed or used for bulk collection activities or mass surveillance."

But the planes can capture video of unrelated criminal activity on the ground that could be handed over for prosecutions.

Some of the aircraft can also be equipped with technology that can identify thousands of people below through the cellphones they carry, even if they're not making a call or in public. Officials said that practice, which mimics cell towers into coughing up basic subscriber information, is rare.

Details confirmed by the FBI track closely with published reports since at least 2003 that a government surveillance program might be behind suspicious-looking planes slowly circling neighborhoods. The AP traced at least 50 aircraft back to the FBI, and identified more than 100 flights since late April orbiting both major cities and rural areas.

One of the planes, photographed in flight last week by the AP in northern Virginia, bristled with unusual antennas under its fuselage and a camera on its left side. A federal budget document from 2010 mentioned at least 115 planes, including 90 Cessna aircraft, in the FBI's surveillance fleet.

The FBI said it also occasionally helps local police with aerial support, such as during the recent disturbance in Baltimore that followed the death of 25-year-old Freddie Gray, who sustained grievous injuries while in police custody. Those types of requests are reviewed by senior FBI officials.

The surveillance flights comply with agency rules, an FBI spokesman said. Those rules, which are heavily redacted in publicly available documents, limit the types of equipment the agency can use, as well as the justifications and duration of the surveillance.

Details about the flights come as the Justice Department seeks to navigate privacy concerns arising from aerial surveillance by unmanned aircrafts, or drones. President Barack Obama has said he welcomes a debate on government surveillance, and has called for more transparency about spying in the wake of disclosures about classified programs.

"These are not your grandparents' surveillance aircraft," said Jay Stanley, a senior policy analyst with the American Civil Liberties Union, calling the flights significant "if the federal government is maintaining a fleet of aircraft whose purpose is to circle over American cities, especially with the technology we know can be attached to those aircraft."

During the past few weeks, the AP tracked planes from the FBI's fleet on more than 100 flights over at least 11 states plus Washington, D.C., most with Cessna 182T Skylane aircraft. These included parts of Houston, Phoenix, Seattle, Chicago, Boston, Minneapolis and Southern California.

Evolving technology can record higher-quality video from long distances, even at night, and can capture certain identifying information from cellphones using a device known as a "cell-site simulator" -- or Stingray, to use one of the product's brand names. These can trick pinpointed cellphones into revealing identification numbers of subscribers, including those not suspected of a crime.

Officials say cellphone surveillance is rare, although the AP found in recent weeks FBI flights orbiting large, enclosed buildings for extended periods where aerial photography would be less effective than electronic signals collection. Those included above Ronald Reagan Washington National Airport and the Mall of America in Bloomington, Minnesota.

After The Washington Post revealed flights by two planes circling over Baltimore in early May, the AP began analyzing detailed flight data and aircraft-ownership registrations that shared similar addresses and flight patterns. That review found some FBI missions circled above at least 40,000 residents during a single flight over Anaheim, California, in late May, according to Census data and records provided by the website FlightRadar24.com.

Most flight patterns occurred in counter-clockwise orbits up to several miles wide and roughly one mile above the ground at slow speeds. A 2003 newsletter from the company FLIR Systems Inc., which makes camera technology such as seen on the planes, described flying slowly in left-handed patterns.

"Aircraft surveillance has become an indispensable intelligence collection and investigative technique which serves as a force multiplier to the ground teams," the FBI said in 2009 when it asked Congress for \$5.1 million for the program.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 2 of 4

FBI in the sky

These flights are among dozens of recent surveillance flights run by the FBI equipped with video-recording technology. They're used primarily to target FBI suspects, but also can be used, like in Baltimore, to support local police operations.



SAN DIEGO

April 29, 2015

Plane: Cessna 182T Skylane

Owner: NBR Aviation

Average altitude: 4,546 feet

Average speed: 57 knots

(66 mph)



BALTIMORE

April 30, 2015 (during

Freddie Gray unrest)

Plane: Cessna 182T Skylane

Owner: NG Research

Average altitude: 3,621 feet

Average speed: 63 knots

(72 mph)



WASHINGTON D.C.

May 20, 2015

Plane: Cessna 182T Skylane

Owner: NG Research

Average altitude: 7,418 feet

Average speed: 73 knots

(84 mph)

SOURCE: FlightRadar24.com

AP
ASSOCIATED PRESS

Recently, independent journalists and websites have cited companies traced to a bank of Virginia post office boxes, including one shared with the Justice Department. The AP analyzed similar data since early May, while also drawing upon aircraft registration documents, business records and interviews with U.S. officials to understand the scope of the operations.

The FBI asked the AP not to disclose the names of the fake companies it uncovered, saying that would saddle taxpayers with the expense of creating new cover companies to shield the government's involvement, and could endanger the planes and integrity of the surveillance missions. The AP declined the FBI's request because the companies' names -- as well as common addresses linked to the Justice Department -- are listed on public documents and in government databases.

At least 13 front companies that AP identified being actively used by the FBI are registered to post office boxes in Bristow, Virginia, which is near a regional airport used for private and charter flights. Only one of them appears in state business records.

Included on most aircraft registrations is a mysterious name, Robert Lindley. He is listed as chief executive and has at least three distinct signatures among the companies. Two documents include a signature for Robert Taylor, which is strikingly similar to one of Lindley's three handwriting patterns.

The FBI would not say whether Lindley is a U.S. government employee. The AP unsuccessfully tried to reach Lindley at phone numbers registered to people of the same name in the Washington area since Monday.

Law enforcement officials said Justice Department lawyers approved the decision to create fictitious companies to protect the flights' operational security and the Federal Aviation Administration was aware of the practice. One of the Lindley-headed companies shares a post office box openly used by the Justice Department.

Such elusive practices have endured for decades. A 1990 report by the then-General Accounting Office noted that, in July 1988, the FBI had moved its "headquarters-operated" aircraft into a company that wasn't publicly linked to the bureau.

The FBI does not generally obtain warrants to record video from its planes of people moving outside in the open, but it also said that under a new policy it has recently begun obtaining court orders to use cell-site simulators. The Obama administration had until recently been directing local authorities through secret agreements not to reveal their own use of the devices, even encouraging prosecutors to drop cases rather than disclose the technology's use in open court.

A Justice Department memo last month also expressly barred its component law enforcement agencies from using unmanned drones "solely for the purpose of monitoring activities protected by the First Amendment" and said they are to be used only in connection with authorized investigations and activities. A department spokeswoman said the policy applied only to unmanned aircraft systems rather than piloted airplanes. The First Amendment of the U.S. Constitution guarantees freedom of speech and assembly.

Associated Press writers Sean Murphy in Oklahoma City; Joan Lowy and Ted Bridis in Washington; Randall Chase in Wilmington, Delaware; and news researchers Monika Mathur in Washington and Rhonda Shafner in New York contributed to this report.

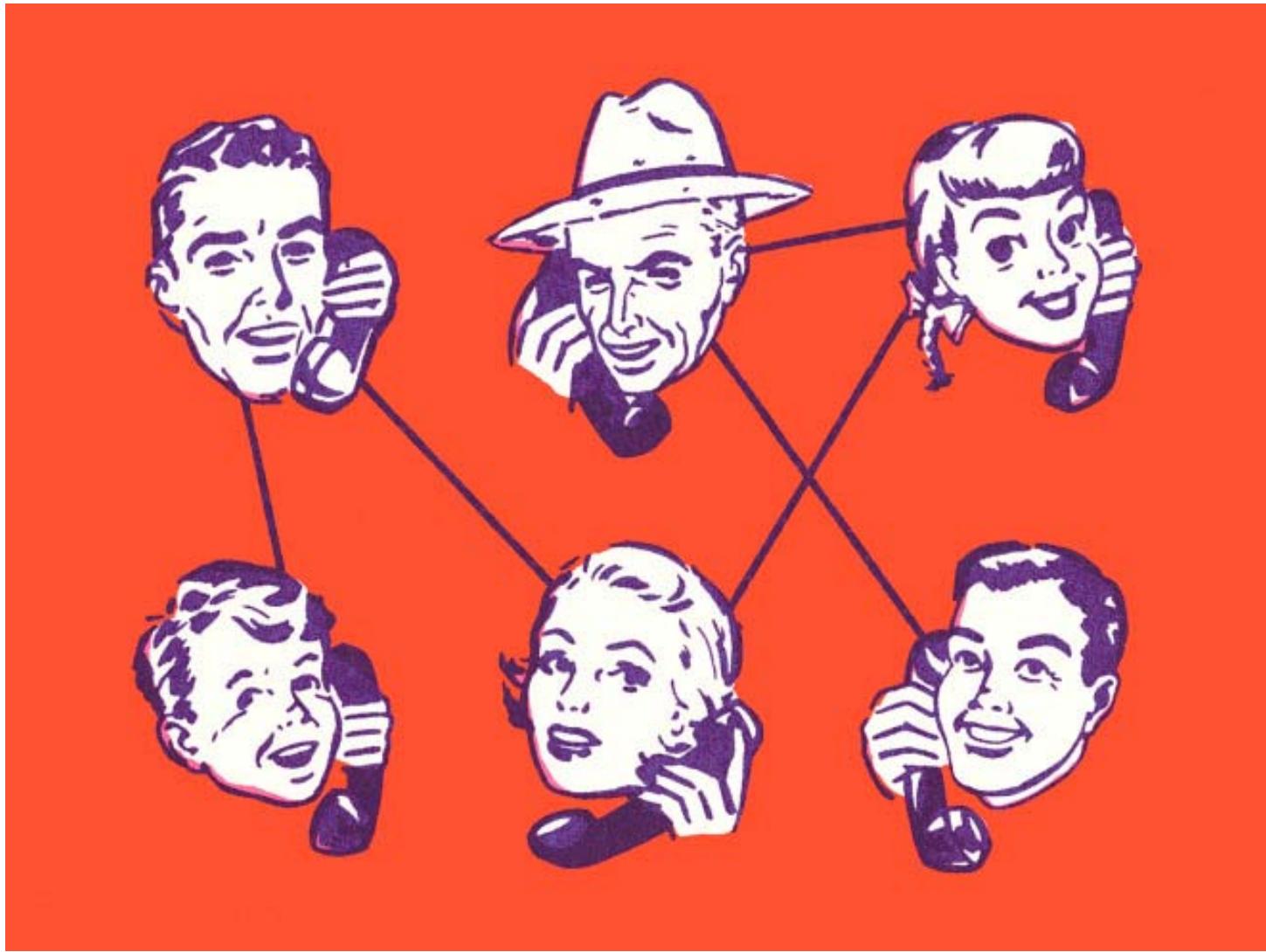
ELECTRONICALLY FILED
7/2/2015 12:12 PM

2014-CHE-1538
MORE 4 of 4

View documents: <http://apne.ws/1HEvPot>

[Fbi Surveillance Flights](#) [Fbi Surveillance Aircraft](#) [FVX Research](#) [KQM Aviation](#) [NBR Aviation](#) [PXW Services](#) [Fbi Secret Air Force](#) [FBI Video](#)

FEDS ADMIT STINGRAYS CAN DISRUPT CELL SERVICE OF BYSTANDERS



© Getty Images

FOR YEARS THE government has kept mum about its use of a powerful phone surveillance technology known as a stingray.

The Justice Department and local law enforcement agencies insist that the only reason for their secrecy is to prevent suspects from learning how the devices work

Exhibit 1-N

and devising methods to thwart them.

But a court filing recently uncovered by the ACLU suggests another reason for the secrecy: the fact that stingrays can disrupt cellular service for any phone in their vicinity—not just targeted phones—as well as any other mobile devices that use the same cellular network for connectivity as the targeted phone.

Civil liberties groups have long asserted that stingrays are too invasive because they can sweep up data about every phone in their vicinity, not just targeted phones, and can interfere with their calls. Justice Department and local law enforcement agencies, however, have refused to confirm this or answer other questions about the tools.

But in the [newly uncovered document](#) (.pdf)—a warrant application requesting approval to use a stingray—FBI Special Agent Michael A. Scimeca disclosed the disruptive capability to a judge.

Because of the way, the Mobile Equipment sometimes operates,” Scimeca wrote in his application, “its use has the potential to intermittently disrupt cellular service to a small fraction of Sprint’s wireless customers within its immediate vicinity. Any potential service disruption will be brief and minimized by reasonably limiting the scope and duration of the use of the Mobile Equipment.”

ELECTRONICALLY FILED
7/2/2015 12:12 PM
HHS-15-1588
PAGE 2 OF 2

The document was previously sealed and only came to light after the defense attorney for a defendant in the case filed a motion last year to dismiss evidence collected by the stingray. It’s the first time the ACLU has seen the FBI acknowledge the stingray’s disruptive capabilities and raises a number of questions about the

nature of the disruption and whether the Federal Communications Commission knew about it when it certified the equipment.

“We think the fact that stingrays block or drop calls of cell phone users in the vicinity should be of concern to cell service providers, the FCC, and ordinary people,” says Nate Wessler staff attorney with the ACLU’s Speech, Privacy, and Technology Project. “If an emergency or important/urgent call (to a doctor, a loved one, etc.) is blocked or dropped by this technology, that’s a serious problem.”

Stingrays are mobile surveillance systems the size of a small briefcase that impersonate a legitimate cell phone tower in order to trick mobile phones and other mobile devices in their vicinity into connecting to them and revealing their unique ID and location. Stingrays emit a signal that is stronger than the signal of other cell towers in the vicinity in order to force mobile phones and other devices to establish a connection with them and reveal their unique ID. Stingrays can then determine the direction from which the phone connected with them, data that can then be used to track the movement of the phone as it continuously connects to the fake tower.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
SEARCHED
PAGE 3 OF 38

Although stingrays are designed to recognize 911 calls and let them pass to legitimate cell towers without connecting to the stingray, the revelation from the FBI agent raises the possibility that other kinds of emergency calls not made to 911 may not get through.

Law enforcement agencies around the country have been using variations of the stingray since the mid-90s to track the movement of suspects in this way. The technology is used by the FBI, the Secret Service, the U.S. Marshals Service, Customs and Border Patrol agents and the Drug Enforcement Agency as well as local law enforcement agencies in more than a dozen states.

But the secrecy around their use has been extreme, due in part to non-disclosure agreements that law enforcement agencies sign with the companies that make stingrays.

Stingrays Cloaked in Secrecy

Authorities in several states have been caught deceiving judges and defense attorneys about how they use the controversial technology or have simply used the devices without obtaining a warrant in order to avoid disclosing their use to a court. In other cases they have withheld information from courts and defense attorneys about how the stingrays work, refraining from disclosing that the devices pick up location data on all systems in their vicinity, not just targeted phones. Law enforcement agencies have even gone so far as to intervene in public records requests to prevent the public from learning about the technology.

The revelation in the court document is therefore significant and also begs the question: Who else knew about this capability and for how long? The Federal Communications Commission is responsible for certifying equipment that operates on radio frequencies to make sure that devices comply with certain technical standards and do not cause radio interference. If the companies that make stingrays failed to disclose the disruption of service to the federal agency, it would mean the devices had potentially been approved under false pretenses.

ELECTRONICALLY FILED
7/22/2015 12:12 PM
EFC-14-1533
PAGE 4 OF 7

The Harris Corporation in Florida—the leading maker of stingrays for law enforcement in the U.S. and an aggressive proponent of secrecy around their use—has already been singled out for a questionable statement the company made to the FCC in a 2010 email. In the correspondence, a Harris representative told the FCC that the technology was used by law enforcement only “in emergency situations.” But according to records the ACLU obtained from the police department in Tallahassee, Florida, in nearly 200 cases that the equipment was used since 2007 only 29 percent of these involved an emergency. Stingrays are regularly used in day-to-day criminal investigations to track suspected drug dealers, bank robbers and others.

The FCC certified stingray equipment from Harris in April 2011 and March 2012.

Asked whether the company disclosed the stingray’s disruptive capabilities to the FCC when it sought certification, an FCC official told WIRED, “We can’t comment on how the devices operate because that information is confidential in accordance with the FCC’s application process.” She said Harris had specifically “requested confidentiality in the application process.”

She also said that if “wireless customers experiencing unexplained service disruptions or interference” report it to the FCC, the agency will “investigate the causes.”

How Stingray Disruption Works

The case in which the FBI disclosed the service disruption is ongoing and involves a defendant named Claude Williams who was suspected of participating in a string of armed bank robberies. In July 2012, the FBI’s Scimeca submitted an application for a warrant to use a stingray to track Williams’s phone.

Although Scimeca was seeking authorization to use a stingray, he referred to it alternatively as mobile pen register and trap and trace equipment in his application. The nomenclature is important because the ACLU has long accused the government of misleading judges by using this term. Pen registers record the numbers dialed from a specific phone number, while trap and trace devices record the numbers that dial into a particular number. But stingrays are used primarily to track the location and movement of a device.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
E-COURT
PAGE 13 OF 17

Although Scimeca disclosed to the magistrate that the equipment could disrupt phone service, he didn’t elaborate about how the disruption might occur. Experts suspect it has something to do with the “catch-and-release” way stingrays work. For example, once the stingray obtains the unique ID of a device, it releases it so that it can connect to a legitimate cell tower, allowing data and voice calls to go through.

“As each phone tries to connect, [the stingray] will say, ‘I’m really busy right now so

go use a different tower. So rather than catching the phone, it will release it,” says Chris Soghoian, chief technologist for the ACLU. “The moment it tries to connect, [the stingray] can reject every single phone” that is not the target phone.

But the stingray may or may not release phones immediately, Soghoian notes, and during this period disruption can occur.

Disruption can also occur from the way stingrays force-downgrade mobile devices from 3G and 4G connectivity to 2G to get them to connect and reveal their unique ID and location.

In order for the kind of stingray used by law enforcement to work, it exploits a vulnerability in the 2G protocol. Phones using 2G don’t authenticate cell towers, which means that a rogue tower can pass itself off as a legitimate cell tower. But because 3G and 4G networks have fixed this vulnerability, the stingray will jam these networks to force nearby phones to downgrade to the vulnerable 2G network to communicate.

Depending on how long the jamming is taking place, there’s going to be disruption,” says Soghoian. “When your phone goes down to 2G, your data just goes to hell. So at the very least you will have disruption of internet connectivity. And if and when the phones are using the stingray as their only tower, there will likely be an inability to receive or make calls.”

ELECTRONICALLY FILED
7/30/2015 12:12 PM
Case# H-15338
Page 6 of 7

“A Grave Threat to Privacy”

Concerns about the use of stingrays is growing. Last week, Senator Bill Nelson (D—Florida) sent a letter to the FCC calling on the agency to disclose information about its certification process for approving stingrays and any other tools with similar functionality. Nelson asked in particular for information about any oversight put in place to make sure that use of the devices complies with the manufacturer’s representations to the FCC about how the technology works and is used.

Nelson also raised concerns about their use in a remarkable speech on the Senate floor. The Senator said the technology “poses a grave threat to consumers’ cellphone

and Internet privacy,” particularly when law enforcement agencies use them without a warrant. He also noted that invasive devices like the stingray will inevitably force lawmakers to come up with new ways to protect privacy.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 7 of 7

His combative speech marks the first time a lawmaker has called out the controversial technology in the public chamber. But his speech was also remarkable for another reason: Nelson’s state of Florida is home to the Harris Corporation, and the company is his second biggest campaign donor.

Baltimore judge allows police use of Stingray phone tracking in murder case

By **Justin Fenton**
The Baltimore Sun

APRIL 20, 2015, 10:05 PM

A city judge turned back a challenge Monday to the Baltimore Police Department's use of a controversial cellphone surveillance tool in a murder case, ruling that a suspect can't complain about police deploying the device to find a stolen phone.

The case is the latest in recent months in which police disclosed use of a cell site simulator, which for years was shrouded in secrecy. Anthony Todd is accused of killing Kevin Gipson in March 2013, and police traced the victim's stolen cellphone to Todd's home. Detectives testified that the killing created an urgency that left no time to get a court order.

Circuit Court Judge Timothy J. Doory ruled that Todd, 47, had no ability to "complain about a phone that isn't his, taken during commission of a murder." Todd, whose trial will begin later this week, claims he found the phone on the porch of a vacant home the day of his arrest.

The judge's ruling was a victory for law enforcement amid recent questions about the device, known as a "stingray." The device is so secretive that the FBI has required police and prosecutors to sign a document agreeing not to discuss its use, even to judges or legislators.

The stingray works by mimicking a cellphone tower and tricking all phones within a range of up to a mile to connect with it. For years, police have referred to it in affidavits using terms such as "sophisticated technology," and if questions arose, the nondisclosure agreement instructed prosecutors to drop cases rather than reveal details about it.

But in recent weeks, officials have been opening up about the stingray and discussing its use in courtrooms. Assistant State's Attorney Rita Wisthoff-Ito said Monday that privacy concerns about the stingray were unfounded.

"There's a big issue being made of a device that does nothing but look for a signal out of a cellphone," she told Doory.

Police outlined for the first time this month their usage of the stingray, pegging it at more than 4,300 times — a figure experts called a "huge number" compared to a trickle of disclosures in other cities.

At Monday's hearing, Detective Michael Dressel said the device is used without court orders under urgent circumstances, and though he was unsure how often that happened, he called it "rare."

David Rocah, a staff attorney with the American Civil Liberties Union of Maryland, said Todd's case had very specific circumstances and did not address the general concerns expressed by privacy advocates over how authorities have been using the device.

"Does the use of a stingray absent exigent circumstances require a warrant? Our view is clearly yes, it does," Rocah said. "It's not a targeted search but a blunderbuss search of everything in range. All of that means to us that a

Exhibit 1-O

warrant — a real warrant — is required."

The hearing came in pretrial motions in the killing of Gipson, 43. Prosecutors say he and a friend were buying drugs in the 1100 block of Barclay St. from a man they knew as "Mike" when an argument erupted. Gipson was fatally shot.

Two days later, police realized Gipson had a phone that had been taken. A relative had called the phone, and a man answered, saying he had found it, police wrote in court documents.

Homicide Detective Shawn Reichenberg faxed a request to the agency's Advanced Technical Team to find the phone. Though police say their policy is to get a court order, the circumstances — notably that a killing had occurred — caused them to go directly to the phone company for permission to get a general range of the phone's location.

That led them to Todd's home in the 4500 block of Pimlico Road in the Park Heights area.

Todd's attorney, Richard Woods, said in court that his client does not match the initial description of Gipson's killer, and that Todd picked up the phone after he found it ringing on the porch of a vacant home in his neighborhood. Woods said surveillance video shows other people walking past the house who seem to be looking in the direction of a noise.

Monday's hearing focused on the stingray. Dressel testified that the device temporarily knocks out phone service to everyone in the area who is using the same subscriber as the phone they are looking for.

~~I was calling Aunt Mabel, my phone may be disconnected temporarily?" Woods asked, to which Dressel responded, yes.~~

Dressel said the stingray collects unique identifying information of the phones in range, but only stores the target and does not collect other data or listen to calls.

He said the criteria for obtaining location data without a warrant is broad, but the phone companies themselves require police to show imminent threat of death or bodily harm, "conspiratorial activities characteristic of organized crime," or an imminent threat to national security interests.

An earlier version of this article misstated the number of times Baltimore police have used the stingray device.

jfenton@baltsun.com

Copyright © 2015, The Baltimore Sun

CELL PHONE INVESTIGATIONS

Search Warrants, Cell Sites and Evidence Recovery



Exhibit 1-P

AARON EDENS
POLICE PUBLISHING

A DIVISION OF POLICE TECHNICAL

Cell Phone Tracking Using Stingray/Trigger Fish

Before anyone blows a gasket and accuses me of leaking law enforcement sensitive techniques, everything in this book, including this topic, are publicly available.

Cell phone tracking and the use of site emulators are commonly known within our field by the code word "Triggerfish" or "Stingray." The equipment works by emulating a cell tower and querying the particular serial number of a given device and measuring the signal strength to the device. This allows the operators to locate the device and, hopefully, its user. Due to the cost of the equipment, Triggerfish equipment is usually maintained by federal law enforcement (FBI, Secret Service, etc.), state law enforcement, and large municipal law enforcement agencies. Depending on the configuration, the equipment is also capable of capturing the unique serial numbers of all devices in a certain area. This assists investigators to isolate a suspect's previously unknown cell device.

To be used effectively, Triggerfish relies on an operational pen register to locate the cell tower and sector the device most recently used. The Triggerfish team will then go to the area the cell phone sector covers and try to locate the device. In my experience, the equipment is extremely accurate but relies on skilled technicians operating the device, a responsive and competent surveillance element, some degree of intelligence regarding the suspect's associates, and an active cell phone associated with your target.

If your agency requires the equipment, I suggest checking with a larger state investigative agency. Federal law enforcement will use their equipment to assist local law enforcement investigations; however, they typically require "adoption" of the case. This can be a cumbersome process, depending on which federal law enforcement agency you approach. At times they are required to replicate the investigative work already completed to ensure that a federal standard is met.

Is Cell Site Information Valuable Evidence or "Junk Science?"

Prosecutor: "Your Honor, I'll submit Agent Shute as an expert in cell site analysis."

Judge: "Okay. Any voir dire?"

Defense: "I wouldn't know how to cross examine him. I'll have to accept him."

Judge: "I will therefore certify that Special Agent Shute is an expert in historical cell site [sic] analysis."⁹

It took a while, but defense attorneys are finally coming to grips with cell site location information (CSLI). Defense attorneys do not like CSLI evidence or any evidence that leads to their client's conviction, for that matter. A few of them have taken their experiences and readily shared it with other attorneys. It is helpful to review their literature so you will know what you might be up against when you testify about CSLI. Be aware that the prosecutor probably knows just as little about CSLI as the defense attorney does and take the time to educate them before going on the stand.

Cell site evidence can never be the smoking gun; rather, it is a valuable piece of evidence that complements the entire picture. From reading many defense articles involving cases where CSLI is relevant, it appears the defense was completely unprepared for the introduction of this evidence. Without effective cross examination, judges and juries involved in early CSLI cases were left with the impression that the evidence was ironclad and irrefutable. Unfortunately, not only do the facts not support this, but defense attorneys have found a couple of hired guns who are willing to testify to the contrary.

It's important to learn from the mistakes of others so we do not repeat them. If the defense has success casting doubt on the expertise of a witness because they were unaware if the specific tower was

⁹ From the testimony of FBI Special Agent William Shute in US v Sims 06-674 Eastern District of Pennsylvania

undergoing an update or maintenance, you can be sure that they are going to share it with the rest of their community. A defense attorney is going to attempt to instill reasonable doubt into the minds of a jury by pointing out all of the variables that could have affected how a cell site handled a call. Be prepared to address these.

There are several ways for a defense attorney, without the aid of a hired gun expert witness, to cast reasonable doubt on CSLI evidence. Here are a few:

Defense Technique #1:

Subtle belittling of the evidence. The police and prosecution call this “call detail records,” but the defense calls it “accounting data and billing records.” To subtly lessen the impact of these records – no matter what one calls them – the defense will often use these terms. It is ironic that, on one hand, the defense tries to lower the data’s integrity by referring to records as mere accounting records while maintaining it would be invasive to require a search warrant. For an example of this contradictory logic, as well as some specific defense objections, see “Defense Against the Disclosure, Admission, and Credibility of Cell Phone Tracking Data by Courtney Montiero” in *Federal Criminal Defense Journal Vol. II*

Defense Technique #2:

It takes information from at least three cell sites to locate a cell device. True. Precise location would require trilateration/triangulation, which can be a proactive technique for locating a phone. The defense knows it is impossible to go back two years and get this information for trial; instead, they imply that any CSLI that does not rely on trilateration/triangulation is inherently false. What is at issue is the handset’s exact location. I would never testify that a cellular device was precisely anywhere in the first place. There are too many variables that can affect which cell site a device is in communication with. It is not possible to show that a suspect was at the scene of a crime using the information from one cell site. However, it is possible to say the device was in communication with the same cell site and sector that encompassed the crime scene.

There are a couple of subtle differences in the last sentence. I’m providing testimony regarding the device’s communication with the cell service provider’s network as documented with the call detail records – not the suspect. I have no idea and can provide no testimony as to whether the suspect was actually using the device at the time. There are no absolutes with regards to CSLI, so the device was likely in communication with a particular cell site. And I’m not saying definitively the suspect or his phone were at the crime scene – just in the same coverage area for the cell site.

Defense Technique #3:

There are so many factors that can affect which cell site handles communication with a mobile device that it’s impossible to place the handset within the coverage area of a single cell site. This is true but with some important caveats. What is critical is understanding what the factors are and proactively addressing them. It may be impossible to determine whether a cell site was undergoing a routine upgrade or maintenance during the time frame of the crime. It is doubtful investigators will remember if there were any unusual occurrences in their jurisdiction that could have overwhelmed a particular cell site and caused traffic to shift to another site. Learning what conditions can affect a cell site and documenting them during the initial investigation will help to overcome this objection.

Defense Technique # 4:

"Isn't it possible the mobile device was actually ___ miles/minutes away from the scene of the crime?" Be careful of the language the defense attorney is using. It's common to see them refer to driving time in lieu of distance. Thirty minutes of driving time can take you quite a distance in a rural area with no traffic. Thirty minutes of driving time in Los Angeles during rush hour, however, won't take you very far. Also be aware of the introduction of the "square mile" and "miles squared" language. If you took the 25 miles theoretical maximum range of a GSM cell site and represented it as miles squared, it would be 625 miles. Don't be shocked to see a defense attorney start throwing around these big numbers in an attempt to cause the jurors to believe the suspect's mobile phone could have been anywhere in that area. Theoretical maximums are just that: theory.

Defense Technique # 5:

Your experience and training is insufficient to be able to render an expert opinion on anything related to CSLI. I like to read what the defense has to say. In one case they criticized a detective for only having 80 hours of training in call detail records, GPS, and geo-location. While 80 hours of training does not make you the best in the world, it is significantly more training than most investigators receive. In fact, I think one would be hard pressed to find much more than 80 hours of training on those topics offered nationwide. However, the defense attorneys like to portray their expert, who spent his dubious career as a fingerprint examiner or an electrical engineer, as much more capable of testifying about cell sites as someone who attended training on how to use CSLI to complement investigations. The distinction here is to limit testimony to what is in the call detail records and how that information relates to the case. Unless you are a cell site engineer and understand the complexities of a particular provider's equipment, don't try to testify like one.

Know who the defense is likely to call as a rebuttal witness. See what they've testified to in the past. There are not a lot of them so it's not very difficult to research them and see how they are going to try to attack your testimony.

A resource available to state and local law enforcement officers for technical assistance and to help prepare for testimony is the Federal Bureau of Investigation's Cell Analysis Survey Team (CAST). These teams are located at most major field offices and are comprised of federal agents who have received special training in using the same techniques and equipment as cell site engineers who work for the cell phone companies. The team members can perform surveys of particular areas and then testify as to the results.

Lastly, don't forget to compel the provider to turn over their propagation maps using a search warrant. Not only do they help focus the investigations but they can also serve as compelling evidence.

Defense Technique #6:

Warrantless searches. This area is going to be much more interesting in light of the United States Supreme Court decision in *United States v. Jones* regarding the need to obtain a warrant for GPS tracker placement. Previously, defense attorneys would often object to the "warrantless search" of cell phone records. Semantics again. They know full well the records were obtained with a court order pursuant to 18 USC 2703(d), administrative subpoena, or other legal procedure. They are trying to taint the jury's perception of the evidence by implying the law enforcement officer did something underhanded to obtain the records without a warrant. This area is going to be contentious until the Supreme Court rules on it, so

let me say this loud and clear. When in doubt get a search warrant. If the case is significant or important get a search warrant instead of using a court order. This allows an investigator to preemptively close the door on a potential defense objection.

Defense Technique #7:

Call detail records cannot be authenticated. States each have different rules regarding the authentication and admissibility of business records into evidence, including call detail records. However, the Federal Rules of Evidence has a universal standard for admissibility. The Federal Rules of Evidence require the records be accompanied by a written certification that they were made near the time of the event documented, it was regular practice of the business to make such records, and the records were kept during the normal course of business. These elements must be testified to by a qualified witness such as the custodian of records, or through certification. It can be difficult for a defense attorney to attack the credibility of this information so they will look for other means to raise doubt and confusion among the judge or jurors.

Defense Technique #8:

There is no way to prove who was using the phone at the time. Some of the interesting techniques are bringing up the issue of cloning and other third party misappropriation of the suspect's phone by other methods including identity theft. Let's examine the technological issues surrounding the feasibility of these methods. Once upon a time, cloning of cell phones was big business among criminals. It was possible using some simple techniques to capture a cell phone's unique serial number and then program it into another phone. This caused the legitimate user to be billed for all of the cloned phone's calls. Cloning is an old school crime which occurred when cell phone minutes were very expensive. Currently, the equipment needed to intercept cell transmissions and then program a mobile phone costs more than an unlimited plan from most service providers.

In one frequently cited article, one defense attorney states, "In fact, 80 percent of cellular phones utilized in the commission of a crime are clones." Really? I'm not sure where she got that information because the URL in her footnotes is dead and I can't find the information anywhere. However, be prepared for a defense attorney who read her article to try to introduce this "fact" in trial. The defense's introduction of cloning as a reason for a call at a crime scene also overlooks the technological innovation the providers created to prevent fraud. These include software designed to thwart multiple activation of the same serial numbers and encryption built into the mobile device itself.

Another potential technological issue the defense could use is the target phone was bluejacked or Bluetooth snarfed. These were techniques utilized to access a victim's phone by pairing with the device as if it were a legitimate Bluetooth device. The security flaw that was exploited has since been patched and this would only work if the mobile device was set to be discoverable by any other device in range. Also, it would require continuous proximity of the hacker to the other phone.

Is it possible someone stole the phone and used it to make the incriminating call? Is it possible someone used the suspect's identity to open an account in his name? It is absolutely possible for either one to happen. It is also pretty easy to show otherwise. A common mistake many investigators overlook is to focus only on a narrow time frame during which the crime occurred. Take a look at the entire record and find the phone calls to the suspect's work, significant other, and family members. It's not likely someone stole the victim's identity and then used the phone to call the victim's mother. The simplest way to overcome this is to ask the suspect if it is his phone. Most of them want the phone back and don't

136 Cell Phone Investigations

realize the incriminating value of their statement of ownership. Even if they won't admit ownership, documentation of where the phone was located can help establish dominion and control.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
CALENDAR: 11
CIRCUIT COURT OF
COOK COUNTY, ILLINOIS
CHANCERY DIVISION
CLERK DOROTHY BROWN

Baltimore Police used secret technology to track cellphones in thousands of cases

By **Justin Fenton**

The Baltimore Sun

APRIL 9, 2015, 6:42 AM

The Baltimore Police Department has used an invasive and controversial cellphone tracking device thousands of times in recent years while following instructions from the FBI to withhold information about it from prosecutors and judges, a detective revealed in court testimony Wednesday.

The testimony shows for the first time how frequently city police are using a cell site simulator, more commonly known as a "stingray," a technology that authorities have gone to great lengths to avoid disclosing.

The device mimics a cellphone tower to force phones within its range to connect. Police use it to track down stolen phones or find people.

Until recently, the technology was largely unknown to the public. Privacy advocates nationwide have raised questions whether there has been proper oversight of its use.

Baltimore has emerged in recent months as a battleground for the debate. In one case last fall, a city detective said a nondisclosure agreement with federal authorities prevented him from answering questions about the device. The judge threatened to hold him in contempt if he didn't provide information, and prosecutors withdrew the evidence.

The nondisclosure agreement, presented for the first time in court Wednesday, explicitly instructs prosecutors to drop cases if pressed on the technology, and tells them to contact the FBI if legislators or judges are asking questions.

Detective Emmanuel Cabreja, a member of the Police Department's Advanced Technical Team, testified that police own a Hailstorm cell site simulator — the latest version of the stingray — and have used the technology 4,300 times since 2007.

Cabreja said he had used it 600 to 800 times in less than two years as a member of the unit.

Nate Wessler, an attorney with the American Civil Liberties Union, said 4,300 uses is "huge number." He noted that most agencies have not released data.

The Florida Department of Law Enforcement says its officers have used the device about 1,800 times. Police in Tallahassee say they have used it more than 250 times; police in Tacoma, Wash., 170 times.

Former U.S. Judge Brian L. Owsley, a law professor at Indiana Tech, said he was "blown away" by the Baltimore figure and the terms of the nondisclosure agreement. "That's a significant amount of control," he said.

Agencies have invoked the nondisclosure agreement to keep information secret. At a hearing last year, a Maryland State Police commander told state lawmakers that "Homeland Security" prevented him from discussing the technology.

Exhibit 1-Q

Wessler said the secrecy is upending the system of checks and balances built into the criminal justice system.

"In Baltimore, they've been using this since 2007, and it's only been in the last several months that defense attorneys have learned enough to start asking questions," he said. "Our entire judicial system and constitution is set up to avoid a 'just trust us' system where the use of invasive surveillance gear is secret."

Cabreja testified Wednesday during a pretrial hearing in the case of Nicholas West, 21, and Myquan Anderson, 17. West and Anderson were charged in October 2013 with armed carjacking, armed robbery, theft and other violations stemming from an attack on a man in Federal Hill.

Cabreja took what he said was a copy of the nondisclosure agreement to court. It was dated July 2011 and bore the signatures of then-Police Commissioner Frederick H. Bealefeld III and then-State's Attorney Gregg Bernstein.

Defense attorney Joshua Insley asked Cabreja about the agreement.

"Does this document instruct you to withhold evidence from the state's attorney and Circuit Court, even upon court order to produce?" he asked.

"Yes," Cabreja said.

Cabreja did not comply with a defense subpoena to produce the device in court. He said he was barred from doing so by the nondisclosure agreement.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014CH-15338
JAG/25An FBI spokesman declined to comment on the technology or the document.

The signatories to the document agree that disclosing the existence of the stingray would "reveal sensitive technological capabilities possessed by the law enforcement community and may allow individuals who are the subject of investigation ... to avoid detection."

They agree that "disclosure of this information could result in the FBI's inability to protect the public from terrorism and other criminal activity" by rendering the technology useless for investigations.

The signatories agree that if they receive a public records request or an inquiry from judges or legislators, they will notify the FBI immediately to allow "sufficient time for the FBI to intervene."

Cabreja testified Wednesday that his unit received information about a stolen cellphone. He said detectives obtained a court order to get the phone's general location using cellphone towers from a cellphone company.

With that information, detectives ventured out to the Waverly neighborhood with the Hailstorm. The device is portable and can be used from a moving vehicle. Cabreja likened it to a metal detector for cellphone signals.

The device forces cellphones to connect to it. In this case, it was a Verizon phone, so identifying information from every Verizon customer in the area was swept up.

Cabreja said the data was collected but "not seen." Detectives were interested only in the target phone.

Cabreja said the device allows police to make a stronger signal emanate from the phone to help them find it.

"It, on screen, shows me directional arrows and signal strength, showing me the phone's direction," he testified.

The detectives traced the phone to a group home and knocked on the door. They told the woman who answered that they were conducting a general criminal investigation and asked to come inside, Cabreja said, and the woman

agreed.

Seven detectives entered the home, he said. They used the Hailstorm to make the phone ring before anyone knew why they were really there.

Amid growing questions about the stingray, details of the technology have been trickling out of some jurisdictions, and it is now relatively easy to find descriptions online of what it does.

Insley, the defense attorney, called it the "worst-kept secret," and questioned why local police continue to be gagged.

Cabreja took notes with him to court that he said came from a discussion last week in which the FBI coached him on what to say in court.

The talking points included: "Data is not retained."

Cabreja did not refuse to answer any of Insley's questions, but he said his answers were constrained by the nondisclosure agreement.

Defense attorneys and privacy advocates express concern about the scope of the stingray's powers, and whether the courts are equipped to provide proper oversight of the police who use it. They argue that the use of the device amounts to a search and requires a warrant.

Baltimore police obtain court orders under the state's "pen register" statute. Insley says that law authorizes police to capture only the numbers that are called or received by a phone, not the more detailed metadata and location information the stingray collects.

He said those orders also require a lower standard of proof than a search warrant, and judges are not aware of what they are authorizing.

"They're basically duping these judges into signing authorizations to use stingrays," Insley said. "If they can increase the signal strength of your phone or make it ring, they can pretty much make it do anything."

But prosecutors say the language in the orders authorizes real-time GPS location, and Cabreja testified that police only use the stingray to find "target" phones and not to spy on the innocent.

In Maryland U.S. District Court last fall, an argument about the stingray device was cut short when the suspects took plea deals. And on Wednesday, following Cabreja's testimony, prosecutors and defense attorneys entered into plea negotiations instead of debating the merits of the stingray further.

In cases where the stingray becomes a sticking point, Wessler said, "defense attorneys are being able to get really good deals for their clients, because the FBI is so insistent on hiding all of these details."

"There are likely going to be a lot of defense attorneys in Baltimore who may have an opportunity to raise these issues," Wessler said. "They are on notice now that their clients may have some arguments to make in these cases."

jfenton@baltsun.com

Copyright © 2015, The Baltimore Sun

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA

v.

ROBERT HARRISON

Defendant.

*
*
*
*
*
*
*
*
*
*

CRIMINAL NO. 1:14-CR-00170-CCB

**RESPONSE BY THE UNITED STATES OF AMERICA
TO HARRISON'S MOTION TO COMPEL**

Now comes the United States of America by its attorneys, Rod J. Rosenstein, United States Attorney for the District of Maryland James Warwick, Assistant United States Attorney; and Anthony J. Enright, Special Assistant United States Attorney, and responds in opposition to Defendant Robert Harrison's Motion to Compel Disclosure of Evidence Related to the Government's Use of a Cell Site Simulator (hereinafter "Mot"). Harrison has moved to suppress evidence resulting from the Government's use of a cell-site simulator during the investigation of Harrison (Dkt. # 29), and seeks the production of additional documents about the simulator and the identities of officers who operated it. Harrison is not entitled to any additional information and, accordingly, the Government respectfully requests that this Court deny his Motion.

I. BACKGROUND

A. *The Investigation of Harrison*

In early 2014, law-enforcement agents were investigating the involvement of Derrick Smith in a murder-for-hire conspiracy. Sources had stated to law enforcement that Smith had, on

September 28, 2008, worked with others to kill an individual named Kevin Rouser and that Smith had recently been hired to commit another murder.

Law-enforcement agents purchased a phone for purposes of this investigation (hereinafter the "Subject Phone") in early 2014. Through confidential sources, agents learned that several calls involving both Smith and Harrison were placed to and from the Subject Phone coordinating the murder for hire. On February 4, 2014 an undercover police officer gave the Subject Phone to Smith.

On the day after agents gave the Subject Phone to Smith, February 5, agents obtained an Order from the Baltimore City Circuit Court permitting them to wirelessly track for 60 days the Subject Phone. The Order, which is attached as Exhibit 1 to Harrison's Motion to Suppress, explicitly authorizes use of a "Cellular Tracking Device." (Harrison Motion to Suppress Exhibit 1, at 12.) It also authorizes the use of a "Pen Register," which is a term defined under Maryland law as a "device or process that records and decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." Md. Code, Cts. & Jud. Proc. § 10-4B-01(c)(1). The Order further authorizes use of a "Trap & Trace," which is defined under Maryland Law as a "device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." *Id.* § 10-4B-01(d)(1). Additionally, the Order explicitly permits government to "initiate a signal to determine the location of the subject's mobile device," to obtain precision location information, and to "employ surreptitious or duplication of facilities, technical devices or equipment." (Harrison Motion to Suppress

Exhibit 1, at 12-13.) The Order was based on a finding of probable cause, and was signed by Judge Barry G. Williams of the Baltimore City Circuit Court (*Id.* at 11, 17.)

In late March of 2014, law-enforcement officers used a cell-site simulator to assist them in identifying the location of the phone. The cell-site simulator is a device that can transmit to a cell phone a radio signal to which the phone will respond by registering its mobile identification number and its electronic serial number, which is a number assigned by the phone's manufacturer and programmed into the telephone. The cell-site simulator can only interact with the cell-phone when the cell-phone is turned on. The simulator can also collect radio signals containing the channel and cell-site codes identifying the cell location and geographical sub-sector from which the telephone is transmitting. The mobile identification number, electronic serial number, channel codes, and cell-site codes are transmitted continuously as a necessary component of cellular telephone call direction and processing. This information is not dialed or otherwise controlled by the cellular-telephone user. Instead, the transmission of the telephone's electronic serial number and mobile identification number to the nearest cell site occurs automatically when the cellular telephone is turned on. This automatic registration with the nearest cell site is the means by which the cellular service provider ordinarily connects with and identifies the account, determines where to send calls, and reports constantly to the customer's telephone information regarding signal power, status, and mode.

Law enforcement agents initially determined that the phone was located somewhere within the multi-dwelling structure at 3805 Chatham Road in Baltimore City. Agents knocked on the door to the third floor apartment at that location, and Harrison answered and invited them into the apartment where they recognized, and later seized, the Subject Phone.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 6 of 11

B. Discovery

In April of 2014, after Harrison was indicted, the Government and Harrison entered into a written agreement stating the terms under which the government would provide discovery in this case. Consistent with its obligations under applicable law, the Government has provided discovery to Harrison in accordance with the terms of this agreement. That discovery has included items sought by Harrison's motion to compel, such as reports of the investigation of Harrison that are within the Government's possession, custody, and control.

Additionally, the Government has attached as Exhibit 1 to this response a stipulation of facts about the government's use of a cell-site simulator. The stipulation identifies facts sufficient to enable the Court to resolve Harrison's Motion to Suppress.

II. DISCUSSION

To the extent Harrison's Motion to Compel seeks information beyond what the Government has already produced, it is without merit for at least two reasons. First, the Government has already produced discovery as required under applicable law, and Harrison has not identified any basis for obtaining the additional discovery that he seeks. Second, the additional information that Harrison seeks is protected from discovery by the qualified privilege for sensitive law-enforcement techniques, and Harrison has failed to meet the standard for overcoming that privilege. Each of these reasons is addressed in turn.

First, Harrison has not identified any basis for obtaining additional discovery. The obligation of the Government to provide a criminal defendant with discovery is ordinarily limited to the extent required by "a statute, rule of criminal procedure, or some other entitlement." *United States v. Uzenski*, 434 F.3d 690, 709 ("Generally, criminal defendants do not have a constitutional right to discovery, absent a statute, rule of criminal procedure, or some

other entitlement.”). Nothing about the information that Harrison seeks suggests that it is discoverable under the Jencks Act, 28 U.S.C. § 3500, *Brady v. Maryland*, 373 U.S. 83 (1963), or *Giglio v. United States*, 405 U.S. 150 (1972). And the government has already produced materials under Rule 16. Harrison does not cite any authority for the additional discovery he requests, but presumably he seeks to invoke Rule 16(a)(1)(E)(i), which permits discovery of items “material to preparing the defense.” (See Mot. 3 (seeking “access to information that is material to various suppression issues.”)).

Rule 16(a)(1)(E)(i) does not entitle Harrison broadly to “information”; instead it is limited to “documents and objects” material to preparing the defense that are “within the government’s possession, custody, or control.” Fed. R. Crim. P. 16(a)(1)(E). The Rule does not entitle Harrison to information not contained in documents that already exist, such as the “[t]he identities of the officers or other personnel” that he requests. (Mot. 4.) See *United States v. Rigmaiden*, 844 F. Supp. 2d 982, 997 (D. Ariz. 2012) (Rule 16(a)(1)(E)(i) “does not require the government to create documents that may provide information a defendant desires to obtain, nor does it require the government to present agents or witnesses for interviews or in-court examination.”).

Harrison has not made the “prima facie showing of materiality” required to prevail on a motion to compel discovery under Rule 16(a)(1)(E). 2 Charles Alan Wright et al., *Federal Practice & Procedure* § 254 (4th ed.). To make that showing, “there must be some indication that the pretrial disclosure of the disputed evidence would . . . enable[] the defendant significantly to alter the quantum of proof in his favor.” *United States v. Caro*, 597 F.3d 608, 621 (4th Cir. 2010) (quotation marks omitted) (quoting *United States v. Ross*, 511 F.2d 757, 763 (5th Cir. 1975)). Harrison notes that, in his motion to suppress, he “argues that use of the device

amounted to searches of his home, cell phone, and person" and offers the conclusion that "[t]he details of how the cell site simulator was used, and how it works, are necessary to determine whether the officers' conduct was unlawful." (Mot. 4-5.) Harrison's Motion, however, contains no explanation of how the evidence he seeks would significantly "alter the quantum of proof" beyond the discovery that he has already received and the Government's stipulation, and his conclusion to the contrary offers him no support. *Caro*, 597 F.3d 608, 621-22 (4th Cir. 2010) ("Neither a general description of the information sought nor conclusory allegations of materiality suffice" (quotation marks omitted) (quoting *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990))). On that basis, Harrison's Motion to Compel should be denied.

Second, to the extent Harrison's Motion seeks additional information about the Government's use of a cell-site simulator that otherwise would be discoverable, this Court should reject Harrison's Motion on the basis of the privilege applicable to information about sensitive law-enforcement techniques. Courts have applied this privilege to limit discovery and testimony about information that could enable criminals to frustrate future government investigations and potentially jeopardize the security of ongoing investigations. See *United States v. Cintolo*, 818 F.2d 980, 1002 (1st Cir. 1987). The privilege is qualified, but a defendant can overcome it only by showing that he "needs the evidence to conduct his defense and that there are no adequate alternative means of getting at the same point." *Id.*

The information that Harrison seeks is subject to the privilege for sensitive law-enforcement techniques. Courts have found information that could limit the effectiveness of future investigations or jeopardize the security of ongoing investigations to be subject to the privilege in a number of different contexts. For example, the Supreme Court has recognized a privilege to withhold the identity of government informants. *Roviaro v. United States*, 353 U.S.

53,59-60 (1957). And courts have held the privilege applicable to information about the location of a police surveillance post, *United States v. Harley*, 682 F.2d 1018, 1020 (D.C. Cir. 1982), and about “the nature and location of electronic surveillance equipment,” *United States v. Van Horn*, 789 F.2d 1492, 1507 (11th Cir. 1986); *accord Cintolo*, 818 F.2d at 1002.

What Harrison requests, “[t]he details of how the cell-site simulator was used, and how it works,” (Mot. 4) falls squarely within the scope of the privilege. As one court recently explained in the context of holding the privilege applicable to information about a cell-site simulator used in another investigation, “the precise technology used . . . and the precise manner in which it was used, if disclosed, would educate the public and adversaries of law enforcement on how precisely to defeat [law-enforcement] surveillance efforts.” *United States v. Rigmaiden*, 844 F. Supp. 2d 982, 994 (D. Ariz. 2012). Similarly, the *Rigmaiden* court explained, “[d]isclosures of the specific identities of agents involved in this operation could jeopardize their safety and would effectively eliminate them as law-enforcement assets used in electronic surveillance.” *Id.* The same concerns attend the information that Harrison seeks about the government’s use of a cell-site simulator in this case. Accordingly, the information is subject to the privilege for sensitive law-enforcement techniques and is not subject to discovery absent a sufficient showing of necessity by Harrison. *See id.; Cintolo*, 818 F.2d at 1002.

Harrison has not shown that he “needs the evidence to conduct his defense and that there are no adequate alternative means of getting at the same point,” as required to overcome the privilege. *United States v. Cintolo*, 818 F.2d 980, 1002 (1st Cir. 1987). Harrison has already filed a detailed motion to suppress that cites a host of public information and argues that the Government’s use of a cell-site simulator constituted a search — under both a trespass and reasonable expectation of privacy theory — of Harrison’s home, phone, and even his person, and

that the search was conducted without a warrant. (*See generally* Motion to Suppress.) Harrison can make all of the points that he has raised based on information described in his Motion to Suppress and materials already produced by the Government. Harrison's Motion to Compel contains no showing of greater need; it contains little more than a brief summary of his Motion to Suppress and conclusory statements that the "details" he requests are "necessary to determine whether the officers' conduct was unlawful" and that "Harrison has no alternative means of learning how the technology was used in the investigation leading to his arrest." (Mot. 4-5.)

III. CONCLUSION

Because no basis exists for requiring the Government to provide the additional discovery sought by Harrison and the information he seeks is subject to the privilege for sensitive law-enforcement techniques, the Government respectfully requests that this Court deny Harrison's motion to compel.

Respectfully submitted,

Rod J. Rosenstein
United States Attorney

/s/ _____

Anthony J. Enright
Special Assistant United States Attorney
36 S. Charles Street
Fourth floor
Baltimore, Maryland 21201
(410) 209-4800

/s/ _____

James G. Warwick
Assistant United States Attorney
36 S. Charles Street
Fourth floor
Baltimore, Maryland 21201
(410) 209-4800

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 11 of 11

ACLU-Obtained Documents Reveal Breadth of Secretive Stingray Use in Florida



By Nathan Freed Wessler, Staff Attorney, ACLU Speech, Privacy & Technology Project

FEBRUARY 22, 2015 | 5:30 PM



The ACLU is releasing records today obtained from law enforcement agencies across Florida about their acquisition and use of sophisticated cell phone location tracking devices known as “Stingrays.” These records provide the most detailed account to date of how law enforcement agencies across a single state are relying on the technology. (The full records are available [here](#).)

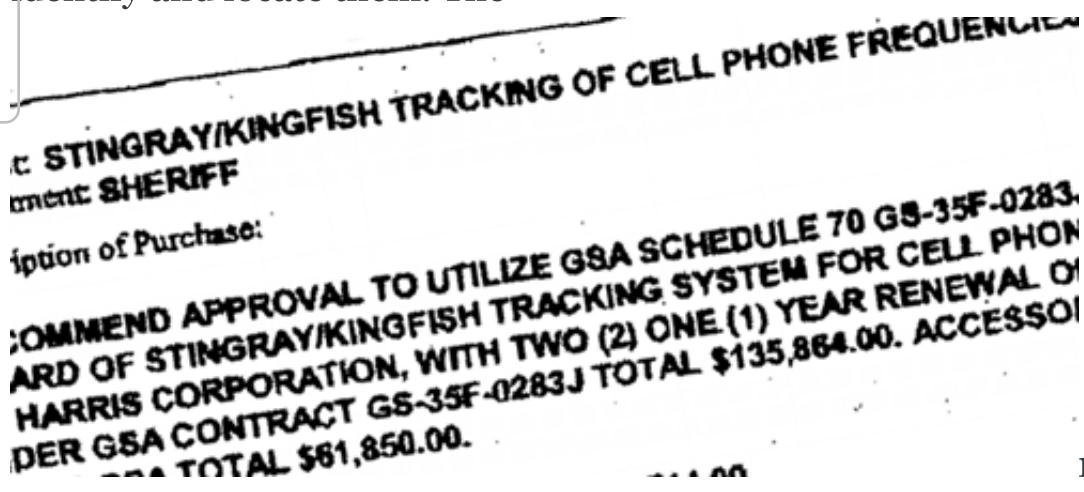
Exhibit 1-R

The results should be troubling for anyone who cares about privacy rights, judicial oversight of police activities, and the rule of law. The documents paint a detailed picture of police using an invasive technology — one that can follow you inside your house — in many hundreds of cases and almost entirely in secret.

The secrecy is not just from the public, but often from judges who are supposed to ensure that police are not abusing their authority. Partly relying on that secrecy, police have been getting authorization to use Stingrays based on the low standard of “relevance,” not a warrant based on probable cause as required by the Fourth Amendment.

Records Show Widespread Stingray Use

Last year, we sent public records requests to three dozen police and sheriffs' departments in Florida seeking information about their use of Stingrays, also called “cell cite simulators” because they mimic cell phone towers and force phones in the area to broadcast information that can be used to identify and locate them. The



records we obtained document millions of dollars spent purchasing the technology and show their use in many hundreds of investigations in every corner of the state.

As we revealed last year, the Florida Department of Law Enforcement has

spent more than \$3 million on Stingrays and related equipment since 2008. But it isn't keeping the technology to itself. The FDLE has signed agreements with at least 11 local and regional law enforcement agencies allowing them to use the FDLE's Stingrays and to share them with neighboring jurisdictions. (Though the version of the sharing agreement released by the FDLE is partially redacted, a local police department near Tampa provided an unredacted copy.)

Use of the FDLE's Stingrays has been extensive. In a May 2014 email, the FDLE identified a staggering 1,835 uses of cell site simulator equipment, likely reflecting deployment in both state and local investigations throughout Florida.

The Tallahassee Police Department (TPD) provided the most extensive information about a local agency's use of Stingrays on loan from the FDLE, including a detailed list of more than 250 investigations in which it used Stingrays from September 2007 through February 2014. Although law enforcement agencies often justify their purchase of Stingrays—and the excessive secrecy surrounding their use — on homeland security grounds, the Tallahassee list reveals not a single national security-related investigation. Robbery, burglary, and theft investigations represent nearly a third of the total, followed by "wanted person" investigations, and then a laundry list of other run-of-the-mill offenses. The list also shows that the TPD allowed other police departments to access Stingrays, even crossing state lines into Georgia on at least five occasions.

Technology Hidden From the Courts

In many of the investigations, police never sought a court order authorizing Stingray use. In others, they sought a court order on a low "relevance" standard, but not a warrant based on probable cause. Perhaps most troublingly, the records indicate a pattern of excessive secrecy, including

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 3 of 9

concealment of information that should appear in investigative files and court filings. For example, the TPD provided a sample of judicial applications and orders it says were used to justify Stingray use, but not one of them contains a single mention or description of Stingray technology. This suggests that judges weren't being fully informed about what they were approving.

The TPD also released the full investigative files from 11 cases where the agency used Stingrays.* But officers' notes and other documentation in the files never once mention Stingrays or provide descriptions of their use. Instead, there are only fleeting references that would likely be inscrutable to a defense attorney or judge not already on the lookout for signs of covert Stingray surveillance. Two files mention use of "electronic surveillance measures" to track a cell phone. Another says only that "Confidential intelligence" indicated the location of a phone. A fourth states that "Inv Corbett [sic] arrived and determined that [the tracked] telephone was on the second floor of the apartment." We know from a court transcript that the ACLU successfully petitioned to unseal last year that Corbitt is the TPD officer who operates Stingrays for the department.

The Tallahassee Police aren't alone in obfuscating references to Stingray use in case files and court documents. As we have previously reported, for example, police in the Sarasota area were instructed by the U.S. Marshals Service to eliminate descriptions of Stingray cell phone tracking in court filings and replace them with the cryptic phrase "received information from a confidential source regarding the location of the suspect."

A new Washington Post article, based partly on the records obtained by the ACLU, provides further detail about how Stingray secrecy functions — and malfunctions — in Tallahassee. In one case detailed by the Post, prosecutors opted to offer a defendant a no-jail plea deal instead of revealing details about the Stingray as part of court-ordered pre-trial discovery. As we've

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 4 of 9

seen elsewhere in the country, our justice system can't properly function when judges and defense attorneys are kept in the dark about covert electronic surveillance by police.

Excessive Secrecy Persists

Below we detail our findings about Stingray use in other departments across the state, including records showing hundreds of thousands of dollars in expenditures and information on the number of cases in which they have been used. But for all these disclosures, many details about Stingray use in Florida are still shrouded in secrecy.

Several agencies refused to comply with Florida's open records laws by properly providing documents. Some acknowledged that they had responsive records, but refused to release them. The Brevard County Sheriff's Office, for example, denied our records request in full, partly relying on a "non-disclosure agreement or requirement" with a "federal agency." (We know the FBI has been making local agencies sign non-disclosure agreements before buying Stingrays; a fully redacted copy of the FBI agreement is likely contained in the pages released by the FDLE. The FDLE also released a copy of a non-disclosure agreement with the Harris Corporation.) The Sheriffs' Offices in Broward and Pinellas Counties issued similar denials. Police Departments in Pembroke Pines and Port St. Lucie failed to respond to the ACLU's request at all.

Other agencies tried to withhold records, but apparently forgot that they had already released documents on the web. The Miami Police Department responded only that it had "No departmental orders or standard operating procedures covering 'cell site simulators,'" but did not reply to a follow-up request for other kinds of records. Documents posted on the city's website, however, show that Miami spent tens of thousands of dollars buying and upgrading Stingrays in 2008.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 5 of 9

And in the City of Sunrise, the police at first refused to confirm or deny whether any responsive records existed. After the ACLU pointed out that Sunrise had already posted purchase records for Stingray devices on its public website, the city saw fit to send the ACLU copies of those already-publicly available documents . . . and a request for \$20,000 to cover the expense of searching for additional records.

Unanswered Questions

Not a single department produced any policies or guidelines governing use of Stingrays or restricting how and when they could be deployed, suggesting a lack of internal oversight. And no department provided evidence that it gets warrants before using the technology.

Indeed, records from Tallahassee and elsewhere indicate that police have not been getting warrants. That must change. In a strong ruling last year, the Florida Supreme Court held that the Fourth Amendment requires police to get a warrant before asking a phone company to track a cell phone user's location in real time. The logic of that opinion should apply equally to cell phone tracking using Stingrays. And because Stingrays sweep up information not just about suspects, but also bystanders, the need for robust judicial oversight is all the greater.

The documents we obtained add to the growing picture of surreptitious Stingray surveillance by local police around the country. By shining a light on police practices, we hope to help bring constitutional violations and a culture of impunity to an end.

Details on Stingray Use by Departments Across Florida

Records from elsewhere in Florida show how use of the technology and secrecy about it has proliferated. Following is what we found about

particular departments across the state:

- The Miami-Dade Police Department produced purchase records for hundreds of thousands of dollars' worth of equipment from the Harris Corporation, the Florida-based maker and seller of Stingrays. The Miami-Dade PD also stated that it had used Stingrays in 59 closed criminal cases within a one-year period ending in May 2014. The total number of investigations where the agency used Stingrays is surely larger, since that figure does not include cases that were still active at the time of its response. The department has a troubling history when it comes to Stingrays: according to a documentavailable on the internet but not among the records produced to the ACLU, the Miami-Dade PD first purchased a cell site simulator in 2003 in order to surveil protesters at a Free Trade of the Americas Agreement conference.
- The Palm Bay Police Department provided records from a 2006 investigation where they used a Stingray to track a suspect's phone. Instead of seeking court authorization or even asking for assistance from the FDLE, a Palm Bay officer "contacted Harris Corporation and utilized some of their technology and engineers to track the cell call." This irregular procedure was possible because Palm Bay is just minutes away from the Harris Corporation's headquarters in Melbourne.
- The Pensacola Police Department identified five cases where it used Stingrays and provided investigative files for each of them; none of the files mention or describe Stingray use. The department also stated that it "has not acquired a cell site simulator" and had no records regarding agreements with the FDLE to borrow the technology. However, the FDLE sharing agreementssigned by the Tallahassee Police Department and the Leon County Sheriff's Office both cover the "Tallahassee and Pensacola Regions," perhaps explaining where Pensacola got the devices used in these investigations.
- The Lakeland Police Department stated that it "relies on the Florida Department of Law Enforcement to assist" in cell phone tracking cases,

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 7 of 9

and produced files from three 2013 cases where it used Stingrays.

Nothing in the files actually describes Stingray use. The FDLE produced a copy of its sharing agreement signed by the Lakeland PD.

- The Orange County Sheriff's Office stated that it had no records regarding acquisition of Stingrays, but acknowledged that it had signed an agreement with the FDLE through which it could borrow the devices. The OCSO said that between 2008 and 2014 it "conducted 558 investigations in which cell site simulators may have been used."
- The Jacksonville Police Department explained that it owns two Stingrays, but "neither of them is functional with the current technology. They are analog, outdated, of no value, and not used. Our agency has elected not to upgrade them due to the cost and frequency." Records show that Jacksonville purchased its first Stingray device in 2001 (a "Triggerfish" model). In 2008 it used nearly \$200,000 of federal grant funds to purchase additional devices, including a "Kingfish" handheld unit. The documents describe how the Kingfish is "capable of pinpointing a phone's location inside buildings or other locations where a vehicle could not travel."
- Agencies that signed sharing agreements with the FDLE but did not produce additional records concerning Stingray use include the Lee County Sheriff's Office, Leon County Sheriff's Office, and Seminole County Sheriff's Office, among others. (See the documents released by the FDLE for the full list).
- A number of departments either explained that have not purchased Stingrays or have not used them, or stated that they did not have records responsive to the ACLU's request, including: Cape Coral Police Department, Clearwater Police Department, Fort Lauderdale Police Department, Fort Myers Police Department, Gainesville Police Department, Hialeah Police Department, Hollywood Police Department, Lake County Sheriff's Office, Melbourne Police Department, Orlando Police Department, Palm Beach County Sheriff's Office, Pasco County Sheriff's Office, Plant City Police Department, St.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 8 of 9

Petersburg Police Department, Tampa Police Department, Titusville Police Department, and West Palm Beach Police Department.

* In consideration of the privacy interests of people named in the investigative files produced by several law enforcement agencies, we are releasing only those pages of the files that shed light on Stingray use, and are redacting personally identifiable information.

TAGS National Security Privacy and Surveillance Privacy & Technology Consumer Privacy Location Tracking Internet Privacy Cell Phone Privacy Secrecy

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 9 of 9

Stingray snared him, now he helps write rules for surveillance device

BY KATE MARTIN

Staff writer March 23, 2015

When state Rep. David Taylor proposed a bill that would change how police seek permission to use a controversial cellphone surveillance device, an Arizona resident took note.

Since then, Daniel Rigmaiden has helped refine the bill's definition of a cell site simulator, a device commonly called by its brand name, Stingray. The bill reached its latest milestone Monday, when state senators passed it out of the Law and Justice Committee.

If anyone knows how a cell site simulator works, it's Rigmaiden. He is best known for exposing the existence of Stingrays while defending himself in federal court against 73 counts of fraud, identity theft and conspiracy for filing fake tax returns and depositing hundreds of thousands of dollars in Arizona bank accounts.

In reviewing his case, Rigmaiden discovered the FBI had used the device to find him in his northern California apartment in 2008. He alleged the electronic intrusion into his apartment was an illegal search. A judge ruled against him.

Last April, Rigmaiden pleaded guilty to charges of conspiracy, mail fraud and two counts of wire fraud and was sentenced to 68 months in prison — the time he served while awaiting trial.

Since Rigmaiden's discovery, dozens of police agencies around the country have admitted or been found to possess Stingray-type equipment.

The News Tribune reported last year that the Tacoma Police Department used the surveillance device as early as 2009, the first known instance of a police department deploying the technology in Washington.

Pierce County Superior Court judges said they had no idea the police were using the technology, which can pretend to be a cellphone tower to collect data from everyone in an area. The judges have since demanded that police officers seeking court permission to track a suspect's phone say when they intend to use a cell site simulator.

Taylor's bill would, in part, replicate that Pierce County practice across the state. Amendments suggested by the Seattle office of the American Civil Liberties Union require police to tell judges about the device's capability and get permission from a judge before deploying the device.

"The technology is fairly complicated, and we wanted to make sure the definitions were appropriate in scope," Jared Friend, technology and liberty director for the ACLU, said Monday. "... We have seen judges confused and misinformed about these issues."

The ACLU — which has worked with Taylor, R-Moxee, on several government surveillance issues — also drew on Rigmaiden's suggestions to refine the definition of a cell site simulator to include devices that locate suspects, intercept information, jam signals or install malicious software.

"The reality is he is one of the foremost experts in the field," Friend said of Rigmaiden.

Since his release, Rigmaiden, 34, has continued to investigate surveillance issues. He recently spoke at a privacy, surveillance and technology seminar for Arizona attorneys about police use

Exhibit 1-S

of Stingrays. He also consulted with the ACLU of Northern California on a guide [for criminal defense attorneys](#) on how to tell if a Stingray was used to locate their clients.

Rigmaiden said he wanted to help write the Washington bill because he wanted to set a good standard.

"Other states will grab that law and use it as an example to write their own laws," Rigmaiden said Monday.

Friend said a handful of states have laws aimed at regulating police use of cell site simulators. But if Taylor's passes, it will be the first one to require police to delete information collected from those who are not the target of that police request.

Kate Martin: 253-597-8542 kate.martin@thenewstribune.com @KateReports

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 2 of 2

ELECTRONICALLY FILED
 7/2/2015 12:12 PM
 2014-CH-15338
 CALENDAR: 11
 PAGE 2 OF 2
 CIRCUIT COURT OF
 COOK COUNTY, ILLINOIS
 CHANCERY DIVISION
 CLERK DOROTHY BROWN

Unsealed transcript illuminates TPD 'stingray' use

Jennifer Portman, Tallahassee Democrat

11:54 p.m. EDT June 4, 2014



(Photo: Michael Schwarz, Michael Schwarz/Special to the Democrat)

36 CONNECT TWEET LINKEDIN COMMENT EMAIL MORE

The American Civil Liberties Union says portions of a transcript unsealed this week by a Leon County Circuit judge about the Tallahassee Police Department's use of so-called "Stingray" cellphone-tracking technology show both broad and specific invasions of people's personal privacy rights.

But Police Chief Michael DeLeo says the six-year-old testimony of TPD investigator Chris Corbitt, ordered open to the public Monday by Circuit Judge James Hankinson at the behest of the ACLU,

proves the department is using the technology responsibly and not capturing personal information about citizens.

At issue are comments Corbitt made as part of a 2008 rape case in which the defendant's conviction was overturned last year because an appeals court found his arrest was based on a warrantless search.

"There is definitely some fascinating stuff in the transcript," said Nathan Wessler, the ACLU's Speech, Privacy and Technology Project lawyer. "It provides a really clear window into just how powerful and invasive this technology really is."

As part of his testimony during a 2010 closed hearing, Corbitt explained how he used two types of cellphone simulators — portable devices that imitate cellphone towers and force cellphones to register with them — to track the location of the rape victim's cellphone to a Tallahassee apartment.

After obtaining from Verizon the location of the closest cellphone tower to the woman's phone, Corbitt explained how he drove around the area with a cellphone simulator in his car until he was able to narrow his search to the Berkshire Manor apartment complex. Corbitt said finding the apartment complex was difficult during the day because of interference from other nearby cellphones.

Once he determined which apartment complex the cellphone seemed to be transmitting from — at about 1 a.m. — Corbitt said he switched to a hand-held device and "quite literally stood in front of every door and window" until he was able to locate the exact apartment from which the cellphone was sending its signal.

"The transcript confirms that the Stingray device was forcing every cellphone in range to report back information. It was probably communicating with hundreds of people's phones as police drove around," Wessler said. "Then they switched to a hand-held device and you have a police officer literally lurking outside windows and doors of private dwellings with a powerful tool to obtain private information. This is quite an invasion."

DeLeo disagreed with the ACLU's assertion. He stressed the transcript showed the agency uses the technology solely to determine the location of cellphones as part of legitimate investigations and does not capture personal information or communications of private citizens.

"We aren't capturing anyone's information. It's just searching for that one particular

Exhibit 1-T

cellphone," he said. "All this particular device does is lead us to the cellphone."

In April, after privacy concerns were raised by the ACLU, DeLeo updated TPD's cellphone-tracking policies and procedures to provide greater oversight. The changes call for court orders to be obtained, if possible, before the technology is used, and require an independent supervisor's approval to bypass judicial oversight in emergencies. All uses of cellphone-tracking technology also is now being reviewed quarterly by TPD's attorney.

"We aren't concerned about it," DeLeo said of the transcript release. "I'm comfortable with what we are doing and that extra layer of protections that aren't required, but that we have added."

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 2 of 2

SECTION #5
EMERGENCY PURCHASES

5.1

BID NUMBER:

E1715-PD

Title: Wireless Tracking System, StingRay/Amberjack

Description: To purchase a mobile wireless tracking system.

Department:

MDPD

Allocation:

\$115,500.00

Term of Contract: Upon delivery

Review Committee

Recommendation:

No measure (insufficient availability and emergency).

Review Committee Date: November 12, 2003; Item #2-07

Living Wage: Not applicable, no services contemplated.

Vendor(s):

Harris Corp.

Estimated Contract Usage: \$115,500.00

Justification:

Retroactive authorization to November 1, 2003 is necessary for the purchase of a wireless tracking system. In order to have the system delivered and field tested to provide the level of security commensurate with the (FTAA) Conference, it was necessary to enter into this emergency purchase.

The Miami-Dade Police Department was responsible for providing assistance and support during the Free Trade Area of the Americas (FTAA) Conference held November 16-21, 2003.

Based on the history of these conferences, the department anticipated criminal activities directed at attendees and conference sites facilitated by the use of cellular phones. Wireless phone tracking systems utilized by law enforcement have proven to be an invaluable tool in both the prevention of these offenses and the apprehension of individuals attempting to carry out criminal activities.

MDPD already possessed wireless tracking capability via the Harris Corporation's Triggerfish tracking system. That system was limited in that it provided access to only Cingular and AT&T Wireless carriers. The newly developed Sting Ray/Amberjack system by Harris Corp. provides PCS tracking capability, which includes Metro PCS, Sprint and Verizon carriers. The combination of these two tracking systems, Triggerfish and StingRay/Amberjack provided MDPD the ability to track approximately ninety percent of the wireless industry.

In the performance of market research, MDPD established that the StingRay/Amberjack system is the only transportable Code Division Multiple Access (cellular technology standard) system in the industry offering tracking and location and signal information collection features.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 2 of 2

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
CALENDAR: 11
PAGE 1 of 5
CIRCUIT COURT OF
COOK COUNTY, ILLINOIS
CHANCERY DIVISION
CLERK DOROTHY BROWN

Tacoma police change how they seek permission to use cellphone tracker

BY ADAM LYNN

Staff writer November 15, 2014

Pierce County judges didn't know until recently that they'd been authorizing Tacoma police to use a device capable of tracking someone's cellphone.

Now they do, and they've demanded that police change the way they get permission to use their so-called cell site simulator.

From 2009 to earlier this year, the county's Superior Court judges unwittingly signed more than 170 orders that Tacoma police and other local law enforcement agencies say authorized them to use a device that allows investigators to track a suspect's cellphone but also sweeps cellphone data from innocent people nearby.

In August, the assistant chief of the Tacoma Police Department told The News Tribune that investigators never deployed the device — a cell site simulator, commonly known as a Stingray — without court authorization.

The newspaper since learned police never mentioned they intended to use the device when detectives swore out affidavits seeking so-called "pen register, trap and trace" orders allowing them to gather information about a suspect's cellphone use and location.

That's now changed.

The county's 22 Superior Court judges, who first learned of the police department's cell site simulator from The News Tribune's reporting, now require language in pen register applications that spells out police intend to use the device.

Law enforcement agencies that want to deploy the device also must swear in their affidavits that they will not store data collected from people who are not the target of the investigation, said Judge Bryan Chushcoff, who requested the verbiage during recent meetings with police officials.

"They said they could live with that," Chushcoff said.

Legal experts differ on whether police should have told judges about the cell site simulator when requesting authorization to use it. They also disagree about whether defendants could challenge evidence gathered using the court orders.

They do agree that case law on the matter is evolving.

"This is an area where the law is not very clear," said Mary Fan, Henry M. Jackson professor of law at the University of Washington. "The law is changing really fast."

NEED-TO-KNOW BASIS

The News Tribune learned earlier this year that Tacoma police had a cell site simulator and had sought permission to use it at least 170 times. Police have said they did not deploy the device in all those instances.

Cell site simulators act as mobile cellphone towers, tricking phones in a certain geographic area into connecting to it.

Exhibit 1-V

Police find them useful because they can pinpoint the location of a certain cellphone if police have the number and a general idea of where to look for it.

Privacy advocates find such devices concerning because they trick all cellphones in the area into connecting to them, including those of innocent third parties.

Since August, the newspaper has published a series of stories about the device, the privacy concerns surrounding its use and which local officials outside the Police Department knew about its existence.

One of those stories, published Aug. 28, quoted Tacoma Assistant Police Chief Kathy McAlpine, who said police use their cell site simulator only with a judge's permission.

"We obtain a search warrant under the authority of (state law)," she said.

Several Superior Court judges, who are responsible for reviewing police requests for search warrants and pen registers, said that was news to them.

"People had never heard of it," presiding Judge Ronald Culpepper told The News Tribune at the time.

The court orders police said authorized them to deploy the Stingray and the accompanying documentation had been sealed at the request of police.

On Oct. 2, The News Tribune went to court to request that two of those orders be unsealed. The orders chosen by the newspaper were from 2009, and the underlying criminal cases had been resolved.

Police Department did not object to the orders being unsealed, and Culpepper ordered that they be made available to the newspaper.

Neither the pen register orders nor the affidavits filed by law enforcement mentioned that police used the Stingray or intended to use it.

Instead, detectives used language commonly associated with requesting an order that would force a cellphone company to turn over records for a particular phone, and, where possible, the real-time location of the phone.

The newspaper this month asked police whether all the Stingray order requests failed to inform judges that investigators intended to use a cell site simulator.

Police spokeswoman Loretta Cool said that was the case.

"They all do not have that in there," Cool said.

Investigators did not believe it was necessary to inform judges that the Police Department had a cell site simulator or intended to use it, she said.

Police are required, when requesting a search warrant, to inform judges of what crime they are investigating and what information they seek, Cool said.

"We don't put in there the tactics and techniques we're going to use," she said. "For instance, if we want to search a house, we don't tell them we're going to use the SWAT team or that we're going to use our dogs."

LEGAL QUESTIONS

That argument does not fly with some civil liberty advocates and legal experts.

In 2012, the American Civil Liberties Union and the Electronic Frontier Foundation filed a pleading in a criminal case in which police used a cell site simulator to track down a California man accused of tax fraud.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CR-1538
PAGE 2 OF 5

"Stingrays are highly intrusive and indiscriminate," attorney Daniel Pochoda wrote on behalf of the ACLU and Electronic Frontier Foundation. "Their use implicates the privacy interests of the suspect, as well as untold numbers of third parties as to whom there is no probable cause."

Pochoda said judges should be made aware that police intend to use such devices.

"The government cannot obtain judicial approval for a search using sophisticated, uniquely invasive technology that it never explained to the magistrate," he wrote.

"To construe this order as a valid 'warrant' authorizing the use of a stingray would prevent magistrates from making informed determinations on warrant applications and encourage the government to keep magistrates in the dark."

Bruce Jacob is a law professor at Stetson University in St. Petersburg, Florida.

He told The News Tribune earlier this month he found it troubling that police would not inform judges that they intended to use a cell site simulator in a criminal case.

"I think they're misleading the judges," he said. "They should explain the method that's being used. The court should know what they're seeking and how they're seeking it."

Mary Fan, the UW law professor and a former federal prosecutor, takes a more nuanced view.

Law enforcement agencies must walk a fine line between informing judges about what they're doing and tipping off a criminal as to the tactics and techniques available to them and "jeopardizing their investigations," Fan said.

"That's the challenge," she said.

7/2/2015 12:12 PM 7/2/2015 12:38 PM
7/2014-CHE-13838
PAGE 3 of 5
law enforcement requests to use a cell site simulator often are sealed, defense attorneys have access to such documents through the process of discovery when preparing a case for trial.

Law hasn't been much help, Fan added, with the technologies available to police outpacing a court's ability to clarify how and when they can be legally used.

"This is new terrain," she said. "Law enforcement agencies are the first movers here. You often don't have the definitive last word on new technology."

Still, Fan said, courts in general, and the U.S. Supreme Court in particular, are becoming "more wary of unregulated and unfettered tracking" by law enforcement.

She cited the 2012 case of *United States v. Jones* as a recent example.

In that case, the Supreme Court ruled that placing a GPS tracking device on a suspect's car constituted a search under the Fourth Amendment and that the subject of such a search enjoyed constitutional protections.

Debates such as the one going on in Tacoma can help law enforcement agencies "forge constraints" before the law is clarified by the courts, she added.

Another legal question the courts have yet to answer is whether evidence gathered using such devices can be used against a defendant, especially if the information was obtained either without a court order or one issued by a judge who didn't know a cell site simulator was being used.

"We're looking to see if that's the case for us or not," said Michael Kawamura, director of Pierce County's Department of Assigned Counsel. "With what I know now, I think it would have to be on a case-by-case basis."

Jacob, the Stetson University law professor, said he thinks defendants might have a basis to challenge such evidence, especially if a judge wasn't informed about the tactics police used to get the information.

"If they obtained evidence that was later used in such cases, then, yes, I think there was a

problem," he said.

"MANY CAPABILITIES"

It's impossible to know what exact device Tacoma police are using, its capabilities or, what, if any, evidence local law enforcement gathered using it.

They won't say, and public documents obtained by The News Tribune about the Stingray have been heavily redacted.

Police said they are required by a nondisclosure agreement with the FBI to remain tightlipped. And, as mentioned before, most of the court documents are sealed.

Spokeswoman Cool denied a request by The News Tribune to see the device and photograph it.

"Then it would be a tool we couldn't use," she said.

Ian Smith is a security researcher in the University of Washington Computer Science & Engineering Security and Privacy Lab and has studied cell site simulators and similar devices.

The devices generally can read both the international mobile subscriber identity (the unique number assigned to each cellphone subscriber) and the unique serial number assigned to the actual phone.

"At that point, it would know which devices are in an area and their signal strength, too," Smith said.

Police who have the cellphone number, and therefore the IMSI number of someone, then could use the cell site simulator almost like a metal detector "to follow the signal strength up the gradient" to locate the exact device they're looking for, he said.

Tacoma police have said they use their cell site simulator for that capability alone.

Smith said many of the devices have other applications as well, Smith said.

"They have many capabilities," he said.

Most have the ability to capture and store data of various kinds, including the IMSI and phone identification numbers, Smith said.

Others can break encryption codes a phone sends to a cell tower. That would allow police or others to listen to a person's calls, read their text messages and, in some cases, analyze Internet data, he said.

Cellphone companies have the ability to access that kind of information now, Smith said. Cell site simulators give that capability to anyone who knows how to use them, including the police, he said.

And the technology is rapidly advancing.

There is information on the Internet about so-called ISMI catchers sewn into a vest-like garment that investigators can wear under a coat. There also are hand-held devices the size of a walkie-talkie.

In some countries, authorities have been known to use Stingrays at protest gatherings to assemble lists of the cell phones, and presumably the subscribers, in attendance, Smith said.

"Even the simplest version of these devices can be abused," he said.

JUDGES NOT WORRIED

Pierce County judges Culpepper and Chushcoff told The News Tribune earlier this month that they think Tacoma police most likely are using their cell site simulator legally.

Both said the addition of language to law enforcement requests for pen registers gives the local courts more oversight of the program and the ability to say no if they think the device is being misused.

It also helps to protect the privacy rights of innocent third parties whose data might be captured during a police operation, they said.

"We would have preferred to know about it sooner, but, from what we've been told by police, we have no reason to believe it's being misused," Culpepper said.

Chushcoff said he's seen at least one pen register request in recent weeks in which the limiting language was included.

"I signed it," he said. "I felt it was OK."

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 5 of 5

EMAILS SHOW FEDS ASKING FLORIDA COPS TO DECEIVE JUDGES



POLICE IN FLORIDA have, at the request of the U.S. Marshals Service, been deliberately deceiving judges and defendants about their use of a controversial surveillance tool to track suspects, according to newly obtained emails.

At the request of the Marshals Service, the officers using so-called stingrays have been routinely telling judges, in applications for warrants, that they obtained knowledge of a suspect's location from a "confidential source" rather than disclosing

Exhibit 1-W

that the information was gleaned using a stingray.

A series of five emails (.pdf) written in April, 2009, were obtained today by the American Civil Liberties Union showing police officials discussing the deception. The organization has filed Freedom of Information Act requests with police departments throughout Florida seeking information about their use of stingrays.

“Concealing the use of stingrays deprives defendants of their right to challenge unconstitutional surveillance and keeps the public in the dark about invasive monitoring by local police,” the ACLU writes in a blog post about the emails. “And local and federal law enforcement should certainly not be colluding to hide basic and accurate information about their practices from the public and the courts.”

The U.S. Marshals Service did not respond to a call for comment.

Stingrays, also known as IMSI catchers, simulate a cellphone tower and trick any nearby mobile devices into connecting with them, thereby revealing their location.

When mobile phones—and other wireless communication devices—connect to the stingray, the device can see and record their unique ID numbers and traffic data, as well as information that points to the device’s location. By moving the stingray around, authorities can triangulate the device’s location with greater precision than they can using data obtained from a fixed tower location.



A stingray made by Harris Corp. U.S. Patent and Trademark Office

The government has long asserted it doesn't need a probable-cause warrant to use stingrays because the devices don't collect the content of phone calls and text messages, but instead operate like pen-registers and trap-and-traces, collecting the equivalent of header information. The ACLU and others argue that the devices are more invasive than a trap-and-trace and should require a warrant. By not obtaining a warrant to use stingrays, however, police can conceal from judges and defendant's their use of the devices and prevent the public from learning how the technology is employed.

But the emails released Thursday show police in Florida are going even further to conceal their use of the equipment when they seek probable cause warrants to search facilities where a suspect is located, deceiving the courts about where they obtained the evidence to support their application for the search.

The initial email, which bears the subject line "Trap and Trace Confidentiality," was sent by Sarasota police Sgt. Kenneth Castro to colleagues at the North Port (Florida) Police Department. It was sent after Assistant State Attorney Craig Schaefer contacted police to express concern about an application for a probable cause warrant filed by a North Port police detective. The application "specifically outlined" for the court the investigative means used to locate the suspect. Castro informs his colleague that the application should be revised to conceal the use of the surveillance equipment.

"In the past," Castro writes, "and at the request of the U.S. Marshalls (sic), the investigative means utilized to locate the suspect have not been revealed so that we may continue to utilize this technology without the knowledge of the criminal element. In reports or depositions we simply refer to the assistance as 'received information from a confidential source regarding the location of the suspect.' To date this has not been challenged, since it is not an integral part of the actual crime that occurred."

ELECTRONICALLY FILED
7/2/2015 12:12 PM
CH-138
PAGE 3 OF 3

He then requests that “If this is in fact one of your cases, could you please entertain either having the Detective submit a new PCA and seal the old one, or at minimum instruct the detectives for future cases, regarding the fact that it is unnecessary to provide investigative means to anyone outside of law enforcement, especially in a public document.”

Capt. Robert Estrada, at the North Port Police Department, later confirmed in an email, “[W]e have changed the PCA within the agency after consulting with the [State Attorney’s Office]. The PCA that was already within the court system according to the SAO will have to remain since it has already been submitted. At some point and time the SAO will submit the changed document as an addendum. We have implemented within our detective bureau to not use this investigative tool on our documents in the future.”

ELECTRONICALLY FILED
7/22/2015 12:12 PM
PAGE 4 OF 5

The release of the emails showing interference by a state attorney and the U.S. Marshals Service comes two weeks after agents from the Marshals Service took the extraordinary measure of seizing other public documents related to stingrays from the Sarasota Police Department in order to prevent the ACLU from examining them.

The documents, which were responsive to a FOIA request seeking information about Sarasota’s use of the devices, had been set aside for ACLU attorneys to examine in person. But hours before they arrived for the appointment to view the documents, someone from the Marshals Service swooped in to seize the documents and cart them to another location.

ACLU staff attorney Nathan Freed Wessler called the move “truly extraordinary and beyond the worst transparency violations” the group has seen regarding documents detailing police use of the technology.

The U.S. Marshals Service is not the only entity conspiring with police to prevent the public from learning about the equipment. The Harris Corporation, a Florida-based

company that makes one of the most popular models of stingrays called Stingray, has made law enforcement agencies sign a non-disclosure agreement explicitly prohibiting them from telling anyone, including other government bodies, about their use of the secretive equipment.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 5 of 5

Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program

Dec 31, 2014

WASHINGTON – Senate Judiciary Committee Chairman Patrick Leahy (D-Vt.) and Ranking Member Chuck Grassley (R-Iowa) pressed top Obama administration officials on the use of cell-site simulators, which can unknowingly sweep up the cell phone signals of innocent Americans.

Recent news reports have chronicled the use of such simulators by law enforcement, explaining that the simulators have the potential to capture data about the location of thousands of cell phones in their vicinity. Leahy and Grassley previously pressed the FBI about the use of this technology. In a joint letter sent last week to Attorney General Eric Holder and Secretary of Homeland Security Jeh Johnson, the Senators raised questions about exceptions to a new FBI policy to obtain a search warrant before using a cell-site simulator. The Senators also asked about other agencies' use of the technology.

"It remains unclear how other agencies within the Department of Justice and Department of Homeland Security make use of cell-site simulators and what policies are in place to govern their use of that technology," Leahy and Grassley wrote.

Outlining privacy concerns for innocent individuals, the letter continues: "The Judiciary Committee needs a broader understanding of the full range of law enforcement agencies that use this technology, the policies in place to protect the privacy interests of those whose information might be collected using these devices, and the legal process that DOJ and DHS entities seek prior to using them."

A signed copy of the December 23 letter to Attorney General Holder and Secretary Johnson is available [Here](#).
Text of the letter can be found below.

December 23, 2014

The Honorable Eric H. Holder, Jr.
Attorney General
Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

The Honorable Jeh Johnson
Secretary of Homeland Security
Department of Homeland Security
Washington, D.C. 20528

Dear Attorney General Holder and Secretary Johnson:

In recent months, media reports have detailed the use of cell-site simulators (often referred to as "IMSI Catchers" or "Stingrays") by federal, state and local law enforcement agencies. Most recently a November 14, 2014, Wall Street Journal article ("Americans' Cellphones Targeted in Secret U.S. Spy Program") reported that the United States Marshals Service regularly deploys airborne cell-site simulators (referred to as "DRT boxes" or "dirtboxes") from five metropolitan-area airports across the United States. Like the more common Stingray devices, these "dirtboxes" mimic standard cell towers, forcing affected cell phones to reveal their approximate location and registration information. The Wall Street Journal article reports that "dirtboxes" are capable of gathering data from tens of thousands of cellphones in a single flight.

Exhibit 1-X

We wrote to FBI Director Comey in June seeking information about law enforcement use of cell-site simulators. Since then, our staff members have participated in two briefings with FBI officials, and at the most recent session they learned that the FBI recently changed its policy with respect to the type of legal process that it typically seeks before employing this type of technology. According to this new policy, the FBI now obtains a search warrant before deploying a cell-site simulator, although the policy contains a number of potentially broad exceptions and we continue to have questions about how it is being implemented in practice. Furthermore, it remains unclear how other agencies within the Department of Justice and Department of Homeland Security make use of cell-site simulators and what policies are in place to govern their use of that technology.

The Judiciary Committee needs a broader understanding of the full range of law enforcement agencies that use this technology, the policies in place to protect the privacy interests of those whose information might be collected using these devices, and the legal process that DOJ and DHS entities seek prior to using them.

For example, we understand that the FBI's new policy requires FBI agents to obtain a search warrant whenever a cell-site simulator is used as part of a FBI investigation or operation, unless one of several exceptions apply, including (among others): (1) cases that pose an imminent danger to public safety, (2) cases that involve a fugitive, or (3) cases in which the technology is used in public places or other locations at which the FBI deems there is no reasonable expectation of privacy.

We have concerns about the scope of the exceptions. Specifically, we are concerned about whether the FBI and other law enforcement agencies have adequately considered the privacy interests of other individuals who are not the targets of the interception, but whose information is nevertheless being collected when these devices are being used. We understand that the FBI believes that it can address these interests by maintaining that information for a short period of time and purging the information after it has been collected. But there is a question as to whether this sufficiently safeguards privacy interests.

Accordingly, please provide written responses to these questions by January 30, 2015:

ELECTRONICALLY FILED
7/2/2015 12:12 PM
CH-15338
PAGE 2 of 3

Since the effective date of the FBI's new policy:

a. How many times has the FBI used a cell-site simulator?

b. In how many of these instances was the use of the cell-site simulator authorized by a search warrant?

c. In how many of these instances was the use of the cell-site simulator authorized by some other form of legal process? Please identify the legal process used.

d. In how many of these instances was the cell-site simulator used without any legal process?

e. How many times has each of the exceptions to the search warrant policy, including those listed above, been used by the FBI?

2. From January 1, 2010, to the effective date of the FBI's new policy:

a. How many times did the FBI use a cell-site simulator?

b. In how many of these instances was the use of a cell-site simulator authorized by a search warrant?

c. In how many of these instances was the use of the cell-site simulator authorized by some other form of legal process? Please identify the legal process used.

d. In how many of these instances was the cell-site simulator used without any legal process?

e. In how many of the instances referenced in Question 2(d) did the FBI use a cell-site simulator in a public place or other location in which the FBI deemed there is no reasonable expectation of privacy?

3. What is the FBI's current policy on the retention and destruction of the information collected by cell-site simulators in all cases? How is that policy enforced?

4. What other DOJ and DHS agencies use cell-site simulators?

5. What is the policy of these agencies regarding the legal process needed for use of cell-site simulators?

a. Are these agencies seeking search warrants specific to the use of cell-site simulators?

b. If not, what legal authorities are they using?

c. Do these agencies make use of public place or other exceptions? If so, in what proportion of all instances in which the technology is used are exceptions relied upon?

d. What are these agencies' policies on the retention and destruction of the information that is collected by cell-site simulators? How are those policies enforced?

6. What is the Department of Justice's guidance to United States Attorneys' Offices regarding the legal process required for the use of cell-site simulators?

7. Across all DOJ and DHS entities, what protections exist to safeguard the privacy interests of individuals who are not the targets of interception, but whose information is nevertheless being collected by cell-site simulators?

Please number your written responses according to their corresponding questions. In addition, please arrange for knowledgeable DOJ and DHS officials to provide a briefing to Judiciary Committee staff about these issues following the provision of these written responses, but no later than February 6, 2015.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 3 of 3

Democratic press release from Office of Senate Committee Science and Transportation Committee

Date: Feb. 25, 2015

Nelson: Lawmakers must grapple with privacy questions raised by new surveillance technology

Nelson: Lawmakers must grapple with privacy questions raised by new surveillance
technology#####

Democratic Press Office - (202) 224-8374

WASHINGTON, D.C. - U.S. Sen. Bill Nelson (D-Fla.) said in a speech on the Senate floor today that the proliferation of software and spy devices poses a grave threat to consumers' cellphone and Internet privacy, so much so that lawmakers are going to have to grapple with and find new ways to curb the increasing intrusions.

Nelson also reiterated his call for a Federal Communications Commission (FCC) review of the latest such device to stir controversy, something called a StingRay, which lets police monitor thousands of he calls without a warrant.

"It's time for us to stand up for the individual citizen of this country and their right to privacy," Nelson said in his speech.

Yesterday, Nelson wrote a letter to the FCC asking the agency to review the use of StingRay devices that are now being used by numerous local law enforcement agencies.

The use of the so-called StingRay and other surveillance devices has come under intense scrutiny recently from privacy advocates and also comes during a time when cybersecurity and privacy issues have increasingly become a focal point in Washington.

To view Sen. Nelson's floor remarks, click [here](#). Below is his letter to the FCC.

Feb. 24, 2015

The Honorable Tom Wheeler

Chairman

Federal Communications Commission

445 12th St., S.W.

Washington, D.C. 20554

Dear Chairman Wheeler:

On Feb. 23, The Washington Post published a front-page article "Secrecy around Police Surveillance Equipment Proves a Case's Undoing." That article indicated that the Tallahassee Police Department and other law enforcement agencies around the country have been using a device called the StingRay to collect cell phone call information.

That article and previous others concerning the device reveal the StingRay was certified for use by the Federal Communications Commission (FCC), contingent upon the conditions that StingRay's manufacturer sell these devices

solely to federal, state, and local public safety and law enforcement; and that state and local law enforcement agencies must coordinate in advance with the Federal Bureau of Investigation (FBI) before acquiring or using this equipment. According to the article, these devices now have been purchased by 48 law enforcement agencies in 20 states and the District of Columbia and used in hundreds of cases.

The use of these devices (also known as IMSI catchers) raises a number of potential privacy and constitutional concerns.

Therefore, I am asking that the FCC report to me on its certification process for the StingRay and any other devices that have similar functionality. In particular, I would like information on the following:

- What information the FCC may have had about the rationale behind the restrictions placed on the certification of the StingRay, and whether similar restrictions have been put in place for other devices;
- Whether the FCC inquired about what oversight may be in place to make sure that use of the devices complied with the manufacturer's representations to the FCC at the time of certification; and
- A status report on the activities of the "task force" you previously formed to look at questions surrounding the use of the StingRay and similar devices.

Thank you and I look forward to your response.

Sincerely,
Bill Nelson

ELECTRONICALLY FILED

7/2/2015 12:12 PM
2014-CHE-5338
PAGE 2 of 2

STATE OF NORTH CAROLINA
COUNTY OF MECKLENBURG

IN RE ACCESS TO SEALED COURT
RECORDS CONSTITUTING APPLICATIONS
FOR ORDERS APPROVING USE OF
CELLPHONE SURVEILLANCE
TECHNOLOGY BY CHARLOTTE
MECKLENBURG POLICE DEPARTMENT,
AND RELATED SEALED ORDERS AND
RECORDS

**CONSENT ORDER GRANTING
MOTION AND PETITION FOR
ACCESS TO SEALED COURT
RECORDS**

On October 31, 2014, The Charlotte Observer Publishing Company, d/b/a/ *The Charlotte Observer*, (“*The Charlotte Observer*”), Fred Clasen-Kelly (“Clasen-Kelly”), and WBTV, LLC (“WBTV”) (collectively “Petitioners”) filed a motion and petition seeking access to certain sealed court records maintained by the Mecklenburg County Clerk of Court.

1. The records sought were:

a. Applications during the period 2006 until the present by the Charlotte Mecklenburg Police Department (“CMPD”) to Superior Court or District Court judges in Mecklenburg County for approval to use, in connection with criminal investigations, equipment that simulates a telephone cell tower and allows CMPD to detect and identify serial numbers, location and other information about nearby cellular telephones, laptop computers and tablets that connect to a cellular network (“Cellphone Surveillance Equipment”); and

b. Any orders granting or denying any such applications.

2. Specifically, Petitioners requested that all such applications filed with the Mecklenburg County courts from 2006 until the present seeking approval for CMPD’s

deployment of Cellphone Surveillance Equipment and all orders granting or denying such applications be unsealed and made available to the public for review and copying.

3. In addition, Petitioners requested that the Court order that the Clerk of Court and CMPD make public a list of all such applications for approval to deploy Cellphone Surveillance Equipment and all orders granting or denying such applications for the period 2006 until the present, including the docket numbers for such matters, to the extent such a list exists or can reasonably be compiled by the Clerk of Court or CMPD.

4. Finally, Petitioners requested that the Court order that any search warrant applications, search warrants and return of search warrants related to any applications by CMPD for approval of deployment of Cellphone Surveillance Equipment to the extent they can be determined and any orders granting or denying same, for the period 2006 until the present, which had previously been sealed, be unsealed and be made available to the public for review and copying.

5. CMPD agrees that from approximately 2010 until the present it did submit applications to Superior Court or District Court judges in Mecklenburg County requesting the Court to order certain cell phone service providers to disclose certain information related to a target's phone number in conjunction with criminal investigations. CMPD has informed the Court that it does not object to the unsealing of such applications filed with the Mecklenburg County courts during any part of the time period beginning in 2006 or to the unsealing of orders directed to cellphone service providers directing them to disclose information to CMPD related to a target's phone number in conjunction with criminal investigations. CMPD has informed Petitioners and represents to the Court that the applications submitted and the orders obtained did not specify the specific equipment or the technical functions of any equipment utilized by

CMPD. CMPD represents to the Court that any applications/orders related to cell phone detection, surveillance or “tracking” submitted by CMPD to the Court, would be included in the sealed applications and orders which CMPD agrees should be unsealed.

6. The Charlotte Mecklenburg Police Department, by and through its Chief, Rodney Monroe, has consented to the unsealing of the above-described applications and orders directed to cellphone service providers directing them to disclose to CMPD information related to a target’s telephone number in conjunction with criminal investigations, including sealed applications submitted by CMPD to the Mecklenburg County courts (and related orders), if any exist, regarding cellphone detection, surveillance or “tracking.” CMPD has also consented to the unsealing and disclosure of related search warrant materials (to the extent they can be determined), and to providing the public with a list of such applications and orders for the period 2006 until the present, to the extent such a list exists. CMPD represents to the Court and Petitioners that it does not maintain such a list.

Upon the consent of the Charlotte Mecklenburg Police Department and Petitioners *The Charlotte Observer*, WBTV, LLC and Fred Clasen-Kelly, the Court hereby **ORDERS**, **ADJUDGES AND DECREES** that:

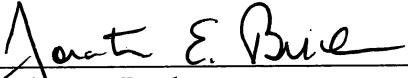
1. The Mecklenburg County Clerk of Court shall unseal and make available to counsel for CMPD and counsel for Petitioners’, the applications and orders described in Paragraphs #5 and #6 above, in order that counsel may conduct an initial limited review of these court records for the purpose of confirming that the records that were sealed are responsive to the Petitioners request. In the event the parties disagree concerning the records reviewed, the records shall be submitted to the Court. Upon completion of this limited review by counsel for the parties, the Clerk shall then make the records available for public review and copying:

- a. Applications during the period 2006 until the present by the Charlotte Mecklenburg Police Department (“CMPD”) to Superior Court or District Court judges in Mecklenburg County requesting the Court to order certain cellphone service providers to disclose information to CMPD related to a target’s telephone number in conjunction with criminal investigations, or regarding cellphone detection, surveillance or “tracking,” and
 - b. Any orders granting or denying any such requests or applications.
2. To the extent the Clerk of Court or CMPD is aware of any search warrant applications, search warrants, and/or return of search warrants related to any such applications by CMPD, and to any such orders granting or denying same, for the period 2006 until the present, which had previously been sealed, such search warrant materials shall be identified and/or unsealed and be made available to the public for review and copying.
3. The Mecklenburg County Clerk of Court make public a list of all such applications and orders (with docket numbers, if any) described in decreltal Paragraph 1 above, to the extent such a list exists.

This the ____ of November, 2014.

Judge Presiding

WE CONSENT:



Jonathan E. Buchan
MCGUIREWOODS LLP
201 N. Tryon St., Suite 3000
Charlotte, NC 28202
Attorney for Movants/Petitioners

Judith Emken
Senior Assistant City Attorney
City Attorney’s Office – Police
601 E. Trade Street
Charlotte, NC 28202
Attorney for Charlotte Mecklenburg Police
Department

LAW & DISORDER / CIVILIZATION & DISCONTENTS

Local judge unseals hundreds of highly secret cell tracking court records

Stingray docs unsealed by North Carolina judge could prompt wave of new appeals.

by Cyrus Farivar - Nov 21, 2014 1:15pm CST

64



Scott

A judge in Charlotte, North Carolina, has unsealed a set of 529 court documents in hundreds of criminal cases detailing the use of a stingray, or cell-site simulator, by local police. This move, which

data:text/html;charset=utf-8,%3Ch1%20id%3D%22archive-head%22%20class%3D%22subheading%20thick-divide-bottom%22%20style%3D%22list-style%3... 1/4

Exhibit 1-AA

took place earlier this week, marks a rare example of a court opening up a vast trove of applications made by police to a judge, who authorized each use of the powerful and potentially invasive device.

According to the *Charlotte Observer*, the records seem to suggest that judges likely did not fully understand what they were authorizing. Law enforcement agencies nationwide have taken extraordinary steps to preserve stingray secrecy. As recently as this week, prosecutors in a Baltimore robbery case dropped key evidence that stemmed from stingray use rather than fully disclose how the device was used.

The newspaper also reported on Friday that the Mecklenburg County District Attorney's office, which astonishingly had also never previously seen the applications filed by the Charlotte-Mecklenburg Police Department (CMPD), will now review them and determine which records also need to be shared with defense attorneys. Criminals could potentially file new claims challenging their convictions on the grounds that not all evidence was disclosed to them at the time.

Relatively little is known about precisely how stingrays are used by law enforcement agencies nationwide, although more and more documents have surfaced showing how they've been purchased and used in limited instances. Last year, Ars reported on leaked documents showing the existence of a body-worn stingray. In 2010, security researcher Kristin Paget famously demonstrated a homemade device built for just \$1,500.

Worse still, local cops have lied to courts (at the direction of the United States Marshals Service) about the use of such technology. Not only can stingrays be used to determine a phone's location, but they can also intercept calls and text messages. While they do target specific phones, they also sweep up cell data of innocents nearby who have no idea that such data collection is taking place.

Neither Senior Resident Judge Richard Boner, nor the Mecklenburg County District Attorney's office, nor the Mecklenburg County Public Defender's office immediately responded to Ars' request for comment. Ars has filed a public records request with the court to obtain the full set of documents.

UPDATE 1:34pm CT: Meghan Cooke, a spokeswoman for the District Attorney's (DA's) Office, told Ars in a statement that the office did not know how long the review process would take.

"As soon as the DA's Office has a list of cases associated with the orders, the office will review those cases individually to determine whether the information was shared with defendants," the statement read. "If prosecutors find that the information was not shared, the office will then work to determine whether the information should have been included in the discovery process. The DA's Office continues to stand by its law enforcement partners as we all work to protect the rights of individuals while also keeping our community as safe as possible."

ELECTRONICALLY FILED
7/2/2015 12:12 PM
1 PAGE

“Sealed at the request of police”

According to the *Observer*, which did not publish the records in full, but summarized some of them, the “CMPD sought permission to use cellphone surveillance more than 500 times since 2010, or about twice a week...Documents and interviews suggest judges rarely, if ever, denied authorization requested by CMPD to use equipment that can intercept cellphone information from criminal suspects and innocent people alike.

"In Mecklenburg County, the documents had remained sequestered in a filing cabinet at the clerk of court's office. They were sealed at the request of police, who have said they were worried about criminal suspects avoiding detection."

The documents apparently include “boilerplate language connected to phone data,” but do not specifically mention a stingray, nor indicate how it would be used, nor what its capabilities are.

It has been very difficult for attorneys and the public alike to fully understand when, where, and how law enforcement has been asking judges to sign off on stingrays. Previously, Brian Owsley, one federal magistrate judge who served in Texas for eight years and is now a law professor at Indiana University, had his efforts thwarted to unseal similar orders.

Owsley is involved in a related situation involving an attempt to reveal the government's actions. Not long before he stepped down from the bench, Owsley tried to unseal more than 100 of his own long-completed judicial orders involving digital surveillance that he himself sealed at the government's request.

But then, a US district judge—who outranks a magistrate—vacated Owsley’s order and resealed them all. That order itself was then sealed. The media company Dow Jones, which publishes *The Wall Street Journal*, filed a motion in federal court in June 2014 to compel the release of those documents. The court has yet to rule on the issue.

"I don't think it's that normal," Owsley told Ars in June 2014.

"I sent in various ways to the government, a number of applications and I said I'm going to unseal these unless you tell me why I shouldn't," he said. These were done in waves. The first wave were completed five years previous, past the statute of limitations, and quite likely are no longer really significant. That was the first wave. The government

did not oppose unsealing of any of them. So I spoke to the court's office and said to upload them to make them available online, and as they were doing that, somehow this district judge found out about it and interjected himself into the process. If the government has said: 'We don't think these things should be unsealed,' that's one thing. But just out of the blue the district judge interjecting himself, that's a little unusual."

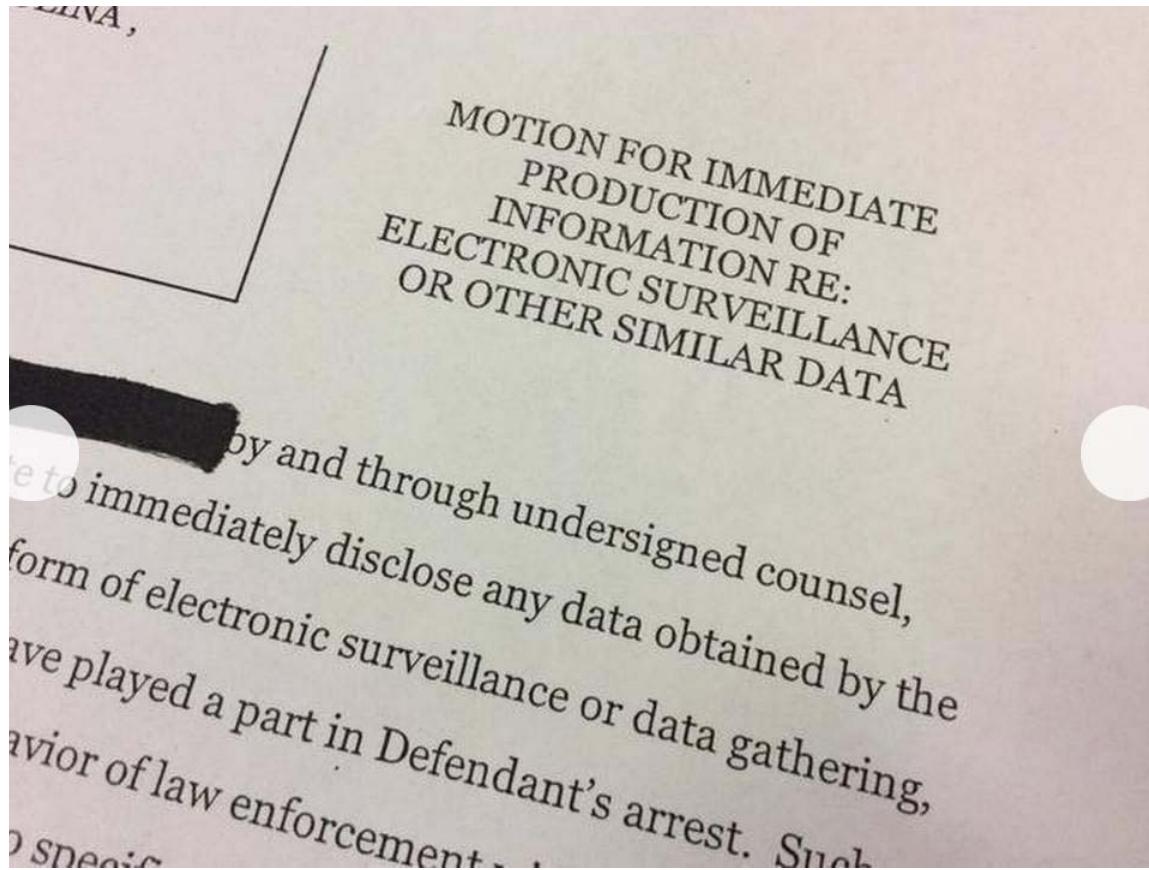
ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 4 of 4

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
CALENDAR: 11
PAGE 1 of 7
CIRCUIT COURT OF
COOK COUNTY, ILLINOIS
CHANCERY DIVISION
CLERK DOROTHY BROWN

New Articles FEBRUARY 15, 2015

Secrecy lifts in CMPD StingRay phone tracking

Charlotte-Mecklenburg police and prosecutors will disclose more details to judges, criminal defendants and the public about a once-secret cellphone surveillance program.



Defense attorneys have started filing motions asking prosecutors to disclose if defendants have been located by the use of cell site simulators or other tracking devices. Prior to the Observer's investigation, lawyers were unaware of their use.

BY FRED CLASEN-KELLY - FRKELLY@CHARLOTTEOBSERVER.COM

Charlotte-Mecklenburg police and prosecutors will disclose more

Exhibit 1-AB

details to judges, criminal defendants and the public about a once-secret cellphone surveillance program.

Defense attorneys and privacy groups had complained that officers gather phone data from both suspects and innocent bystanders without proper oversight.

Among the changes:

- CMPD, for the first time, is disclosing to judges how investigators track cellphones and other wireless devices, a rare step toward transparency for proceedings that take place in judges' chambers.
- People accused of crimes in Mecklenburg County may learn if police used a powerful surveillance device to locate and arrest them.
- The Mecklenburg County District Attorney's Office this spring will reveal results from a review of hundreds of criminal cases it launched after a judge unsealed records about cellphone tracking.

The changes come less than four months after an Observer investigation [revealed](#) that CMPD uses a device called a StingRay that mimics a cellphone tower. The device provides serial numbers, location and other information about nearby phones, laptop computers and tablets that connect to cellular networks.

In response to the newspaper's reporting, Mecklenburg County Senior Resident Superior Court Judge Robert Bell said judges began more closely scrutinizing surveillance requests and asking when officers planned to use a StingRay.

"There is no question they are being upfront," Bell said of police. "You know what they are asking for."

Bell said CMPD's revised documents tell judges when officers want to deploy a StingRay, which he described as a positive move.

Judges also have said that CMPD has discussed a system to routinely unseal the documents after a period of time, a departure from the previous practice. The department said it supports releasing records in closed cases.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
SEARCHED
PAGE 1 OF 1

CMPD and city officials defend how officers conduct cellphone surveillance, saying they do their jobs while respecting privacy rights. The department said that police do not eavesdrop on conversations or store data from innocent people when they use a StingRay.

Permission to track cell phones

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 3 of 7

RESEARCH BY FRED CLASEN-KELLY

INTERACTIVE BY DAVID PUCKETT

But the secrecy surrounding the surveillance has made it difficult for judges and defense attorneys to protect the public from potential police overreach, said George Laughrun, a prominent Charlotte defense attorney.

"Judges probably didn't understand" how the technology worked, Laughrun said. "I didn't understand it. What is it? What does it do? What do you get from it?"

Defendants seek information

Experts said it is rare for local police departments to even acknowledge they own the technology because federal authorities have ordered them not to divulge information. The FBI has said disclosing even minor details could help criminals learn how to avoid

detection.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
JCH-ET
PAGE 4

But some defense attorneys are asking Mecklenburg County prosecutors to turn over evidence gathered from StingRays.

The requests will test North Carolina's open discovery law, which is among the broadest in the country.

To ensure fair trials, the law says defendants should be allowed to examine nearly all evidence used against them.

Defense attorneys said they did not know details about CMPD's cellphone surveillance until an Observer investigation published in October revealed the department had owned a StingRay for eight years.

The Observer and its news partner, WBTV, filed a petition to unseal records related to CMPD cellphone tracking dating to 2006.

Mecklenburg Senior Resident Superior Court Judge Richard Boner later ordered the documents connected to past cases [unsealed](#).

Defense attorneys said the secrecy denied them the chance to challenge evidence in court. Some questioned whether StingRays violate the Constitution's prohibition against unreasonable search and seizures.

Laughrun said he and other lawyers have revised their discovery requests to demand information about cellphone tracking. Now, Laughrun said, prosecutors cannot sidestep the issue by saying defense attorneys failed to request the information.

"The question is, did the police give it to the district attorney's office?" Laughrun said. "It's no excuse. They have a duty to know about it."

Prosecutorial review

In an email, a spokeswoman for Mecklenburg County District Attorney Andrew Murray said the office has always followed discovery laws.

The D.A.'s office has launched an ongoing review into hundreds of cases to determine if the information gathered by phone tracking was used to win convictions. In those cases, officials have said, they would notify defendants and their attorneys.

Prosecutors said they believed that in most cases, cellphone surveillance had been used only to find fleeing suspects who had already been charged, not to build a case against them.

That is why officials said they are confident the convictions should stand.

Charlotte-Mecklenburg police Chief Rodney Monroe has denied vigorously that the department abused discovery laws.

CMPD gave prosecutors court records related to cellphone surveillance in some cases, Monroe has said.

In other instances, he said, officers did not provide documents because the department believed it was not required under the law. In those cases, the use of cellphone tracking was not central to charges against a suspect, Monroe said.

CMPD: More clarity

CMPD told the Observer it has revised court papers that judges review before granting officers permission to track phones in an effort to "improve the effectiveness of the process and provide greater

transparency."

The agency would not provide examples of the new documents, but said the applications more clearly describe investigative tactics, including cellphone tracking.

CMPD says it now includes definitions for each type of equipment officers deploy in its applications to judges. Documents also provide more information in each case about the legal grounds for an officer to make an arrest or search a property.

Jeff Welty, a professor of public law and government at the UNC-Chapel Hill School of Government, said when officers ask for court authorization to perform surveillance they should always make clear what they are seeking permission to do. If the application pertains to technology, he said it should be clear what technology is being used.

In the past, experts told the Observer, applications CMPD submitted to the court were too vague for judges to provide meaningful oversight.

They said that the court orders did not mention StingRays or the more generic term cell-site simulators. Documents also did not spell out how police tracked phones.

Judges most likely had no idea how investigators would monitor phone data, experts said.

More transparency increases the chance that judges will reject requests from CMPD to conduct cellphone surveillance, experts said.

Documents and interviews suggest Mecklenburg judges rarely denied authorization. Monroe said he could only recall one time when a department request has been rejected.

Asked about CMPD's changes to court papers, legal experts said it is impossible to know if the department is now practicing more transparency because officials did not disclose the new wording.

"There hasn't been a lot of candor with the judiciary," Nicole Hardin, a Florida attorney who consults defense lawyers about StingRays. "I

ELECTRONICALLY FILED
7/2/2015 12:12:12 PM
PAGE 1 of 7

find it kind of troubling they won't let anyone see the language."

Anthony Scheer, a Charlotte defense attorney, said the change amounts to a "bare minimum first step" toward transparency.

"If you want to ask a judge to perform an intrusion, you should at the very least be honest with the judge and tell them what the intrusion is," Scheer said. "Telling the judge what you're doing is a basic part of the job."

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 7 of 7



"IMSI catcher"

Web Shopping Images Videos More ▾ Search tools

94 results (0.40 seconds)

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
CALENDAR: 11
PAGE 1 of 12
CIRCUIT COURT OF
COOK COUNTY, ILLINOIS
CHANCERY DIVISION
CLERK DOROTHY BROWN

Acquiring identity parameters by emulating base stations



www.google.com/patents/WO2007010223A1?cl=en

App. - Filed Jul 17, 2006 - Published Jan 25, 2007 - Andrew Paul Pridmore -

M M I Res Ltd

An **IMSI Catcher** is described in Hannes Federrath, Security in Mobile Communications: Protection in GSM networks, mobility management and ...
[Overview](#) - [Related](#) - [Discuss](#)

Special mobile radio telephone supply with inherent access



www.google.com/patents/US8391853

Grant - Filed Mar 23, 2009 - Issued Mar 5, 2013 - Gerhard Kramarz-vonKohout - Deutsche Telekom Ag

Such an **IMSI catcher** represents a virtual wireless cell for a mobile wireless network, the virtual wireless cell taking over parameters of an ...
[Overview](#) - [Related](#) - [Discuss](#)

Acquiring Identity Parameters by Emulating Base Stations



www.google.com/patents/US20080220749

App. - Filed Jul 17, 2006 - Published Sep 11, 2008 - Andrew Paul Pridmore - M.M.I. Research Limited

An **IMSI Catcher** is described in Hannes Federrath, Security in Mobile Communications: Protection in GSM networks, mobility management and ...
[Overview](#) - [Related](#) - [Discuss](#)

Portable cellular base station configuration

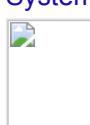


www.google.com/patents/US8606322

Grant - Filed Oct 25, 2010 - Issued Dec 10, 2013 - Eric Sabol - Raytheon Applied Signal Technology, Inc.

2, "IMSI-Catcher," Wikipedia encyclopedia entry,
<http://en.wikipedia.org/wiki/IMSI-catcher>, Oct. 23, 2010. ... 1, 2010. 14,
 Strobel D., "IMSI Catcher ...
[Overview](#) - [Related](#) - [Discuss](#)

System and method for video-assisted identification of ...

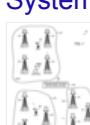


www.google.com/patents/US9025833

Grant - Filed Jul 24, 2011 - Issued May 5, 2015 - Boaz Dudovich - Verint Systems Ltd.

Examples of IMSI catching techniques are described, for example, by Strobel in "IMSI Catcher," Jul. 13, 2007, which is incorporated herein by ...
[Overview](#) - [Related](#) - [Discuss](#)

Systems and methods for identifying rogue base stations



www.google.com/patents/EP2661113A1?cl=en

App. - Filed Apr 30, 2013 - Published Nov 6, 2013 - Ethan Goldfarb - Verint Systems Ltd.

The program configures a cellular phone to detect and report to the subscriber when the phone is being tracked by an **IMSI catcher**.
 SUMMARY ...
[Overview](#) - [Related](#) - [Discuss](#)

System and method for tracking wireless communication ...



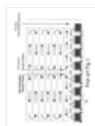
www.google.com/patents/EP2552141A2?cl=en

App. - Filed Jul 26, 2012 - Published Jan 30, 2013 - Ethan Goldfarb - Verint Systems Limited

... International Mobile Station Identifier (IMSI). [0023]. IMSI catching techniques are described, for example, by Strobel in "IMSI Catcher ...
[Overview](#) - [Related](#) - [Discuss](#)

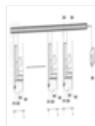
Method of linking a specific wireless device to the ...

Exhibit 1-AC



www.google.com/patents/EP2770692A1?cl=en
 App. - Filed Feb 25, 2014 - Published Aug 27, 2014 - **Roy Glasberg - U-TX Ltd.**
 The method includes installing an International Mobile Subscriber Identity (IMSI) catcher as a surreptitious mobile tower in the midst of the ...
[Overview](#) - [Related](#) - [Discuss](#)

Method of linking a specific wireless device to the ...



www.google.com/patents/US20140242948
 App. - Filed Feb 26, 2013 - Published Aug 28, 2014 - **Roy Glasberg - U-TX Ltd.**
 The method includes installing an International Mobile Subscriber Identity (IMSI) catcher as a surreptitious mobile tower in the midst of the ...
[Overview](#) - [Related](#) - [Discuss](#)

Mobile device and method to monitor a baseband processor ...



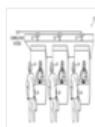
www.google.com/patents/US20140004829
 App. - Filed Jun 14, 2013 - Published Jan 2, 2014 - **Frank Rieger - Gsmk Gesellschaft Fur Sichere Mobile Kommunikation Mbh**
 An IMSI catcher is essentially a false mobile tower acting between the target mobile phone(s) and the service provider's real towers. As such it ...
[Overview](#) - [Related](#) - [Discuss](#)

Stand alone solution for location of a cellular phone



www.google.com/patents/WO2014147627A1?cl=en
 App. - Filed Mar 20, 2014 - Published Sep 25, 2014 - **Roy Glasberg - U-Tx Ltd.**
 ... from a virtual base transceiver station (BTS) 240 (IMSI catcher). In certain embodiments, the virtual base transceiver station is selected from: a ...
[Overview](#) - [Related](#) - [Discuss](#)

System and method for correlation of mobile communication ...



www.google.com/patents/US20120086555
 App. - Filed Oct 5, 2011 - Published Apr 12, 2012 - **Yossi Nelkenbaum - Verint Systems Ltd.**
 Examples of IMSI catching techniques are described, for example, by Strobel in "IMSI Catcher," Jul. 13, 2007, which is incorporated herein by ...
[Overview](#) - [Related](#) - [Discuss](#)

Acquiring identity parameter



www.google.com/patents/US20090023424
 App. - Filed Jan 30, 2007 - Published Jan 22, 2009 - **Paul Maxwell Martin - M.M.I. Research Limited**
 An IMSI Catcher is described in Hannes Federrath, Security in Mobile ...
 The IMSI Catcher behaves like a BTS and like an MS in relation to the ...
[Overview](#) - [Related](#) - [Discuss](#)

Authenticating network elements in a communication system



www.google.com/patents/US8559636
 Grant - Filed Mar 13, 2011 - Issued Oct 15, 2013 - **Gustavo De Los Reyes - AT&T Intellectual Property I, Lp**
 When cellular phones are near an IMSI catcher they generally receive a stronger signal from the IMSI catcher than a cellular base station tower ...
[Overview](#) - [Related](#) - [Discuss](#)

Acquiring identity parameters by emulating base stations



www.google.com/patents/EP1908319B1?cl=en
 Grant - Filed Jul 17, 2006 - Issued Mar 4, 2009 - **Andrew P. M.M.I. Research Limited PRIDMORE - M.M.I. Research Limited**
 An IMSI Catcher is described in Hannes Federrath, Security in Mobile Communications: Protection in GSM networks, mobility management and ...
[Overview](#) - [Related](#) - [Discuss](#)

Authentication method

www.google.com/patents/EP2587429A1?cl=en
 App. - Filed Oct 31, 2011 - Published May 1, 2013 - **Dominic Adenuga - Money and Data Protection Lizenz GmbH & Co. KG**
 Consequently, when an IMSI catcher is installed in the vicinity of a terminal

Methods And Systems For Injecting Wireless Messages in ...



www.google.com/patents/US20140220935

App. - Filed Feb 7, 2014 - Published Aug 7, 2014 - **Jonathan Morgan Peck - Src, Inc.**

This requirement limits the capabilities of an **IMSI catcher** to send messages to mobile stations that decide to move off of the real GSM network ...

[Overview](#) - [Related](#) - [Discuss](#)

Femtocell configuration



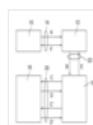
www.google.com/patents/US8588853

Grant - Filed Oct 25, 2010 - Issued Nov 19, 2013 - **Eric Sabol - Raytheon Applied Signal Technology, Inc.**

2, "IMSI-Catcher," Wikipedia encyclopedia entry, <http://en.wikipedia.org/wiki/IMSI-catcher>, Oct. 23, 2010. ... 1, 2010. 14, Strobel D., "IMSI Catcher" ...

[Overview](#) - [Related](#) - [Discuss](#)

Authentication Method



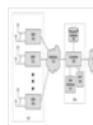
www.google.com/patents/US20140245391

App. - Filed Oct 30, 2012 - Published Aug 28, 2014 - **Dominic Adenuga - Money And Data Protection Lizenz GmbH & Co. Kg**

Consequently, when an **IMSI catcher** is installed in the vicinity of a terminal in order to catch IMSIs of users that make transactions at that ...

[Overview](#) - [Related](#) - [Discuss](#)

Interference detection, characterization and location in a ...



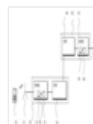
www.google.com/patents/US8138975

Grant - Filed Dec 30, 2008 - Issued Mar 20, 2012 - **Jeffrey F. Bull - Trueposition, Inc.**

A rogue Base Transceiver Station (BTS) (also called an **IMSI-catcher**) is described in European Patent EP1051053 "Method for identifying a ...

[Overview](#) - [Related](#) - [Discuss](#)

Identifiers in a communication system



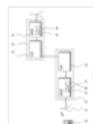
www.google.com/patents/US20080002829

App. - Filed Jun 27, 2007 - Published Jan 3, 2008 - **Dan Forsberg - Nokia Corporation**

This leaves open a possibility that an attacker uses a tracker the to obtain the permanent identity. For example, an **IMSI catcher** are known to ...

[Overview](#) - [Related](#) - [Discuss](#)

Identifiers in a communication system



www.google.com/patents/EP1873998A1?cl=en

App. - Filed Jun 22, 2007 - Published Jan 2, 2008 - **Dan Forsberg - Nokia Corporation**

For example, an **IMSI catcher** are known to have been developed for this purpose. These are typically based on the realisation that it is possible ...

[Overview](#) - [Related](#) - [Discuss](#)

Device and method making it possible to intercept ...



www.google.com/.../WO2009053402A1?cl=en - Translate this page

App. - Filed Oct 22, 2008 - Published Apr 30, 2009 - **Philippe Viravau - Thales Sa**

Devices that use this principle are known as the "**IMSI Catcher**". Il existe aussi des systèmes d'interception passifs permettant d'obtenir ...

[Overview](#) - [Related](#) - [Discuss](#)

Identity acquisition of mobile stations in a mobile ...



www.google.com/patents/WO2011055129A1?cl=en

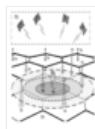
App. - Filed Nov 9, 2010 - Published May 12, 2011 - **Paul Lopez Salzedo - Inpro Limited**

EP-A-1908319 discloses a method of acquiring the identity of two or more mobile devices, by the use of an **IMSI Catcher** device. Issues arise ...

[Overview](#) - [Related](#) - [Discuss](#)

Interference Detection, Characterization and Location in a ...

www.google.com/patents/US20120154213



App. - Filed Feb 28, 2012 - Published Jun 21, 2012 - [Jeffrey F. Bull - Trueposition, Inc.](#)

A rogue Base Transceiver Station (BTS) (also called an **IMSI-catcher**) is described in European Patent EP1051053 "Method for identifying a ...

[Overview](#) - [Related](#) - [Discuss](#)

[Interference detection, characterization and location in a ...](#)



www.google.com/patents/WO2010077790A1?cl=en

App. - Filed Dec 11, 2009 - Published Jul 8, 2010 - [Jeffrey F. Bull - Trueposition, Inc.](#)

[0102] A rogue Base Transceiver Station (BTS) (also called an **IMSI-catcher**) is described in European Patent EP 1051053 "Method for ...

[Overview](#) - [Related](#) - [Discuss](#)

[Identity acquisition of mobile stations in a mobile ...](#)



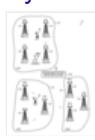
www.google.com/patents/EP2499854A1?cl=en

App. - Filed Nov 9, 2010 - Published Sep 19, 2012 - [Paul Lopez Salzedo - Inpro Limited](#)

EP-A-1908319 discloses a method of acquiring the identity of two or more mobile devices, by the use of an **IMSI Catcher** device. Issues arise ...

[Overview](#) - [Related](#) - [Discuss](#)

[Systems and methods for identifying rogue base stations](#)



www.google.com/patents/US20130344844

App. - Filed Apr 30, 2013 - Published Dec 26, 2013 - [Eithan Goldfarb - Verint Systems Ltd.](#)

The program configures a cellular phone to detect and report to the subscriber when the phone is being tracked by an **IMSI catcher**.

[SUMMARY](#) ...

[Overview](#) - [Related](#) - [Discuss](#)

[Interference detection, characterization and location in a ...](#)



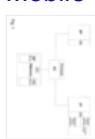
www.google.com/patents/EP2384447A1?cl=en

App. - Filed Dec 11, 2009 - Published Nov 9, 2011 - [Jeffrey F. Bull - TruePosition, Inc.](#)

[0102] A rogue Base Transceiver Station (BTS) (also called an **IMSI-catcher**) is described in European Patent EP 1051053 "Method for ...

[Overview](#) - [Related](#) - [Discuss](#)

[Mobile device and method to monitor a baseband processor ...](#)



www.google.com/patents/EP2680182A1?cl=en

App. - Filed May 8, 2013 - Published Jan 1, 2014 - [Frank Rieger - GSMK Gesellschaft für sichere Mobile Kommunikation mbH](#)

An **IMSI catcher** is essentially a false mobile tower acting between the target mobile phone(s) and the service provider's real towers. As such it ...

[Overview](#) - [Related](#) - [Discuss](#)

[Diversity time and frequency location receiver](#)



www.google.com/patents/CA2746413C?cl=en

Grant - Filed Jun 8, 2010 - Issued Sep 16, 2014 - [Jeffrey F. Bull - Trueposition, Inc.](#)

101091 Figure 8 illustrates an example of the distributed network-based **IMSI-catcher** rogue BTS locator in accordance with the present ...

[Overview](#) - [Related](#) - [Discuss](#)

[Diversity time and frequency location receiver](#)



www.google.com/patents/WO2011011118A1?cl=en

App. - Filed Jun 8, 2010 - Published Jan 27, 2011 - [Jeffrey F. Bull - Trueposition, Inc.](#)

[0109] Figure 8 illustrates an example of the distributed network-based **IMSI-catcher** rogue BTS locator in accordance with the present ...

[Overview](#) - [Related](#) - [Discuss](#)

[Diversity time and frequency location receiver](#)



www.google.com/patents/EP2387725A1?cl=en

App. - Filed Jun 8, 2010 - Published Nov 23, 2011 - [Jeffrey F. Bull - TruePosition, Inc.](#)

[0109] Figure 8 illustrates an example of the distributed network-based **IMSI**-

[Overview](#) - [Related](#) - [Discuss](#)

[Network autonomous wireless location system](#)

www.google.com/patents/EP2422209A1?cl=enApp. - Filed Mar 26, 2010 - Published Feb 29, 2012 - **Jeffrey F. Bull - TruePosition, Inc.****IMSI Catcher.** [0012] European Patent EP 1051053 "Method For Identifying A Mobile Phone User Or For Eavesdropping On Outgoing Calls ...[Overview](#) - [Related](#) - [Discuss](#)

[Network autonomous wireless location system](#)

www.google.com/patents/WO2010123655A1?cl=enApp. - Filed Mar 26, 2010 - Published Oct 28, 2010 - **Jeffrey F. Bull - Trueposition, Inc.****IMSI Catcher.** [0012] European Patent EP 1051053 "Method For Identifying A Mobile Phone User Or For Eavesdropping On Outgoing Calls," ...[Overview](#) - [Related](#) - [Discuss](#)

[Network autonomous wireless location system](#)

www.google.com/patents/CA2755033C?cl=enGrant - Filed Mar 26, 2010 - Issued Jul 29, 2014 - **Jeffrey F. Bull - Trueposition, Inc.****IMSI Catcher** [0012] European Patent EP1051053 "Method For Identifiting A Mobile Phone User Or For Eavesdropping On Outgoing Calls," ...[Overview](#) - [Related](#) - [Discuss](#)

[Method, device and system for detecting a jamming transmitter](#)

www.google.com/patents/EP2733853A1?cl=enApp. - Filed Nov 19, 2012 - Published May 21, 2014 - **Volker Breuer - Gemalto M2M GmbH**It is not necessarily recommended to change to one of these networks, in particular not insecure 2G networks which allow an **IMSI catcher** to ...[Overview](#) - [Related](#) - [Discuss](#)

[Systems and methods for locating communication terminals ...](#)

www.google.com/patents/US8238915Grant - Filed Jul 20, 2010 - Issued Aug 7, 2012 - **Gideon Hazzani - Verint Americas, Inc.**

... IEEE, 2004, 8 pages. 6, Strobel, Daehyun, "IMSI Catcher ...

[Overview](#) - [Related](#) - [Discuss](#)

[Sondermobilfunkversorgung mit eigenem accessmanagemen...](#)

[www.google.com/patents/EP2294775A1?cl... - Translate this page](http://www.google.com/patents/EP2294775A1?cl...)App. - Filed Mar 23, 2009 - Published Mar 16, 2011 - **Von Kohout Gerhard Kramarz - Deutsche Telekom AG**Es ist darüber hinaus bekannt, dass **IMSI-Catcher** in einer Es sei beispielsweise auf die bereits genannten **IMSI-Catcher** verwiesen.[Overview](#) - [Related](#) - [Discuss](#)

[网络自主无线定位系统 Autonomous wireless location system](#)

[www.google.com/patents/CN102405418B?... - Translate this page](http://www.google.com/patents/CN102405418B?...)Grant - Filed Mar 26, 2010 - Issued Jan 21, 2015 - **杰弗里·F·布尔 - 真实定位公司**

一种配置成定位移动设备的网络自主无线定位系统NAWLS，所述移动设备具有用于与无线通信网络WCN通信的无线通信收发机，所述NAWLS包括: ...

[Overview](#) - [Related](#) - [Discuss](#)

[Sondermobilfunkversorgung mit eigenem accessmanagemen...](#)

[www.google.com/.../WO2009152886A1?c... - Translate this page](http://www.google.com/.../WO2009152886A1?c...)App. - Filed Mar 23, 2009 - Published Dec 23, 2009 - **Von Kohout Gerhard Kramarz - Deutsche Telekom Ag**Denkbar wäre auch der Einsatz sogenannter **IMSI-Catcher**, wie sie in EP 10151053 B1 vorgeschlagen werden. Ein solcher **IMSI-Catcher** stellt ...[Overview](#) - [Related](#) - [Discuss](#)

[Improving eavesdropping security of mobile phones](#)

[www.google.com/patents/EP0996303A2?cl... - Translate this page](http://www.google.com/patents/EP0996303A2?cl...)App. - Filed Oct 15, 1999 - Published Apr 26, 2000 - **Michael Wilhelm -**

**Alcatel Alsthom Compagnie Generale D'electricite**

1 ist ein Mobilfunknetz mit mehreren Basisstationen BS1 bis BS5 gezeigt, in dem sich ein Abhörgerät IC (**IMSI-Catcher**) befindet. 1 shows a wireless network ...

[Overview](#) - [Related](#) - [Discuss](#)

Authentication system and method for operating an ...

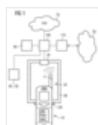
www.google.com/patents/US20130263231 - Translate this page

App. - Filed Apr 1, 2013 - Published Oct 3, 2013 - Manuel Lautenschlager - Bojan Stopic

Mobile phones, used by requesters may be spied using an **IMSI-catcher**.

The various services, which are offered by a service provider, often ...

[Overview](#) - [Related](#) - [Discuss](#)

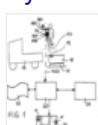
Method and apparatus to identify a user through a mobile ...

www.google.com/patents/EP1424861A1?cl... - Translate this page

App. - Filed Nov 26, 2002 - Published Jun 2, 2004 - Per Vindeby - Siemens Aktiengesellschaft

Verfahren und Vorrichtung werden dadurch gekennzeichnet, dass sich der **IMSI-Catcher** wie ein zwischen ein Endgerät und eine Basisstation ...

[Overview](#) - [Related](#) - [Discuss](#)

System zur elektronischen Verwaltung von mobilen ...

www.google.com/.../DE102013208846A1... - Translate this page

App. - Filed May 14, 2013 - Published Nov 20, 2014 - Peter Polak - logiChip GbR

... a combination of satellite and radio cells assisted positioning system (A-GPS) is formed by a WLAN positioning system or a **IMSI catcher**.

[Overview](#) - [Related](#) - [Discuss](#)

Leakage prevention device for mobile phone

www.google.com/patents/CN101127985A?... - Translate this page

App. - Filed Sep 21, 2007 - Published Feb 20, 2008 - 秦建忠 - 秦建忠

IMSI捕集器干扰周围区域的手机将通话信息通过它来传输，这样某些人就可以窃听你的电话了。 **IMSI catcher** interference area around the phone ...

[Overview](#) - [Related](#) - [Discuss](#)

Device and method making it possible to intercept ...

www.google.com/patents/EP2218237A1?cl... - Translate this page

App. - Filed Oct 22, 2008 - Published Aug 18, 2010 - Philippe Viravau - Thales

... operational for GSM mobile (Global System Mobile). Les dispositifs qui

utilisent ce principe sont plus connus sous le nom de « **IMSI Catcher** ...

[Overview](#) - [Related](#) - [Discuss](#)

Jamming apparatus and method for jamming a target signal

www.google.com/.../WO2010006754A1?c... - Translate this page

App. - Filed Jul 13, 2009 - Published Jan 21, 2010 - Marko Tietz -

Industrieanlagen-Betriebsgesellschaft Mbh

Des Weiteren ist es möglich, den Zentralrechner 21 mit einem **IMSI-Catcher** oder den Basisstationen 30, 30' zu verbinden. Furthermore, it is ...

[Overview](#) - [Related](#) - [Discuss](#)

Jamming apparatus and method for jamming a target signal

www.google.com/patents/EP2301179A1?cl... - Translate this page

App. - Filed Jul 13, 2009 - Published Mar 30, 2011 - Marko Tietz -

Industrieanlagen-Betriebsgesellschaft mbH

Des Weiteren ist es möglich, den Zentralrechner 21 mit einem **IMSI-Catcher** oder den Basisstationen 30, 30' zu verbinden. Furthermore, it is ...

[Overview](#) - [Related](#) - [Discuss](#)

Störvorrichtung und Verfahren zum Stören eines Zielsignals ...

www.google.com/.../DE102008038315A1... - Translate this page

App. - Filed Aug 19, 2008 - Published Jan 28, 2010 - Marko Tietz -

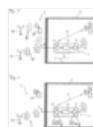
Industrieanlagen-Betriebsgesellschaft Mbh

In verschiedenen Anwendungsbereichen ist es wünschenswert, eine

Störvorrichtung zur Störung von Funksignalen zu haben, die ...

[Overview](#) - [Related](#) - [Discuss](#)

Repeater Repeater



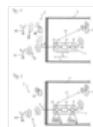
www.google.com/.../DE202009018797U1... - [Translate this page](#)

Grant - Filed Jan 29, 2009 - Issued Jun 6, 2013 - [Andrew Wireless Systems GmbH](#)

Bevorzugt umfasst daher die Steuereinheit eine Untereinheit, die auf einem sogenannten „IMSI-Catcher“ basiert. Preferably, therefore, the ...

[Overview](#) - [Related](#) - [Discuss](#)

Repeater and method for operating such a repeater



www.google.com/patents/EP2180605B1?cl... - [Translate this page](#)

Grant - Filed Jan 29, 2009 - Issued Jan 9, 2013 - [Arndt Pischke - Andrew Wireless Systems GmbH](#)

Bevorzugt umfasst daher die Steuereinheit eine Untereinheit, die auf einem sogenannten „IMSI-Catcher“ basiert. Therefore, preferably the ...

[Overview](#) - [Related](#) - [Discuss](#)

Repeater and method for operating such a repeater



www.google.com/patents/CN102246431A?... - [Translate this page](#)

App. - Filed Oct 6, 2009 - Published Nov 16, 2011 - [托马斯·库梅茨 - 安德鲁无线系统有限公司](#)

Therefore, the control unit preferably includes a sub-unit based on the so-called "international mobile subscriber identity trap (IMSI-Catcher)" a.

[Overview](#) - [Related](#) - [Discuss](#)

Repeater und verfahren zum betrieb eines solchen repeaters



www.google.com/.../WO2010049054A1?c... - [Translate this page](#)

App. - Filed Oct 6, 2009 - Published May 6, 2010 - [Thomas Kummetz - Andrew Wireless Systems GmbH](#)

Bevorzugt umfasst daher die Steuereinheit eine Untereinheit, die auf einem sogenannten „IMSI-Catcher“ basiert. Durch diese hat der Repeater ...

[Overview](#) - [Related](#) - [Discuss](#)

在无线通信或广播系统中的干扰检测、表征以及定位 Interfere...



www.google.com/patents/CN102272617A?... - [Translate this page](#)

App. - Filed Dec 11, 2009 - Published Dec 7, 2011 - [杰弗里·F·布尔 - 真实定位公司](#)

[0157] malicious base transceiver stations (BTS) (also known as **IMSI catcher**) in European Patent EP1051053 "Method for identifying a mobile ...

[Overview](#) - [Related](#) - [Discuss](#)

Device and method for observing, in a spatially limited ...



www.google.com/.../WO2012004074A1?c... - [Translate this page](#)

App. - Filed Jun 7, 2011 - Published Jan 12, 2012 - [Georg Gunzelmann - Thales Defence Deutschland](#)

The means of identification are colloquially referred to as **IMSI catcher**. Die Identifikation der Endgeräte 14, 15 bzw. deren Nutzer erfolgt ...

[Overview](#) - [Related](#) - [Discuss](#)

Device and method for observing, in a spatially limited ...



www.google.com/patents/EP2589239A1?cl... - [Translate this page](#)

App. - Filed Jun 7, 2011 - Published May 8, 2013 - [Jürgen KROKER - Thales Defence Deutschland GmbH](#)

Die Identifikationsmittel werden umgangssprachlich auch als **IMSI-Catcher** bezeichnet. The means of identification are colloquially referred to ...

[Overview](#) - [Related](#) - [Discuss](#)

Einrichtung und Verfahren zur räumlich begrenzten ...



www.google.com/.../DE102010026039A1... - [Translate this page](#)

App. - Filed Jul 3, 2010 - Published Jan 5, 2012 - [Georg Gunzelmann - Thales Defence Deutschland GmbH](#)

Die Identifikationsmittel werden umgangssprachlich auch als **IMSI-Catcher** bezeichnet. The means of identification are colloquially referred to ...

[Overview](#) - [Related](#) - [Discuss](#)

Systems and methods for automated wireless authorization ...



www.google.com/patents/CN101523940B?... - [Translate this page](#)

Grant - Filed Oct 5, 2006 - Issued Jul 11, 2012 - [A·莫迪阿诺 - 尤利卡股份有限公司](#)



In general, by adjusting and optimizing the **IMSI catcher** to create the IMEI catcher, systems and methods disclosed herein allow automatic ...

[Overview](#) - [Related](#) - [Discuss](#)

System and method for secure transaction of data between ...



www.google.com/patents/CN102118387A?cl=en - Translate this page
App. - Filed Dec 30, 2010 - Published Jul 6, 2011 - V·纳塔拉詹 - Tata咨询服务有限公司

[0154] 6) EAP use AES-CTR-192 bit / 3-DES algorithm node address, the base station address is encrypted, so that **IMSI catcher** attack is not ...

[Overview](#) - [Related](#) - [Discuss](#)

Method, device and system for detecting a jamming transmitter



www.google.com/patents/WO2014076283A1?cl=en
App. - Filed Nov 18, 2013 - Published May 22, 2014 - Volker Breuer - Gemalto M2M GmbH

It is not necessarily recommended to change to one of these networks, in particular not insecure 2G networks which allow an **IMSI catcher** to ...

[Overview](#) - [Related](#) - [Discuss](#)

[Help](#) [Send feedback](#) [Privacy](#) [Terms](#)

United States Patent [19]

Easterling et al.

[11] Patent Number: 5,428,667
 [45] Date of Patent: May 27, 1995

[54] MULTI-CHANNEL CELLULAR COMMUNICATIONS INTERCEPT SYSTEM

[75] Inventors: Scott D. Easterling; Michael O. Linden; John C. Voelkel, all of Palm Bay, Fla.

[73] Assignee: Harris Corporation, Melbourne, Fla.

[21] Appl. No.: 29,751

[22] Filed: Mar. 11, 1993

[51] Int. Cl. 6 H04Q 7/34

[52] U.S. Cl. 379/59; 379/34; 455/33.1

[58] Field of Search 379/33, 34, 59, 63, 379/67, 85; 455/33.1, 67.1, 67.2, 95, 99, 100

[56] References Cited

U.S. PATENT DOCUMENTS

3,906,166	9/1975	Cooper et al.	379/59
5,023,900	6/1991	Tayloe et al.	379/59
5,031,204	7/1991	McKernan	379/59
5,289,526	2/1994	Chymek et al.	379/63

Primary Examiner—Curtis Kuntz

Assistant Examiner—Dwayne D. Bost

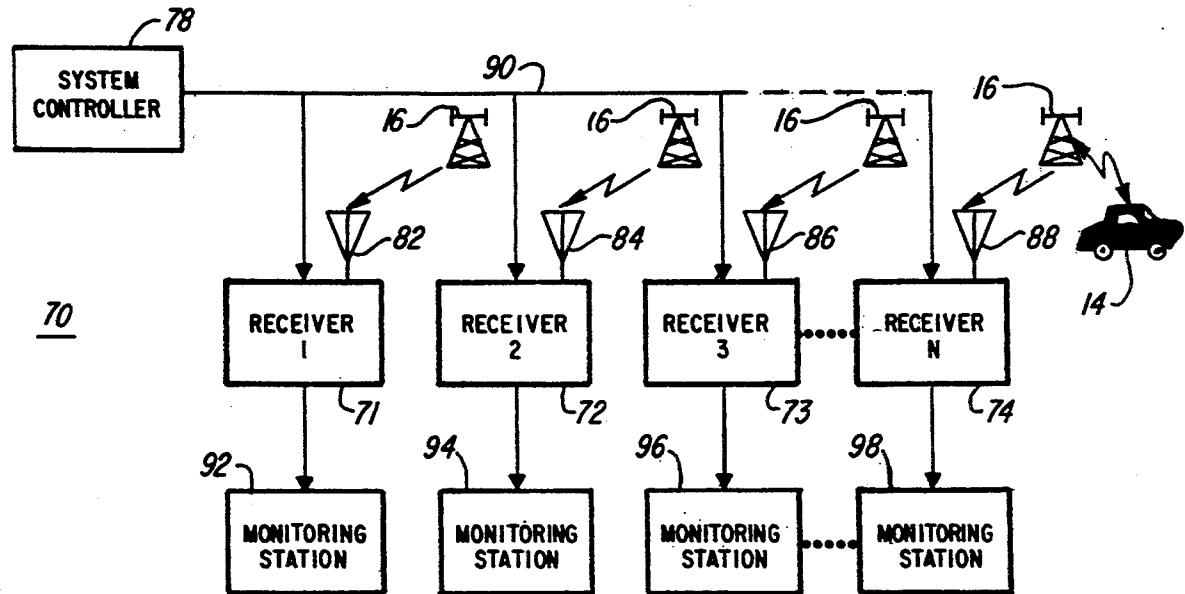
Attorney, Agent, or Firm—John L. DeAngelis, Jr.

[57]

ABSTRACT

A multi-channel cellular communications intercept system for monitoring and then intercepting communications between a mobile unit and a base station in one cell of a cellular telephone system. The system includes a controller and a plurality of receivers with each receiver monitoring the forward control channel from a different cell within a geographical area of interest. When a global page for a target mobile unit is received, one of the receivers in the system is retuned to the forward voice communication channel on which the target mobile unit will be broadcasting for the purpose of monitoring and/or recording the conversation. The remaining receivers are retuned to the strongest forward control channels in the area.

10 Claims, 7 Drawing Sheets



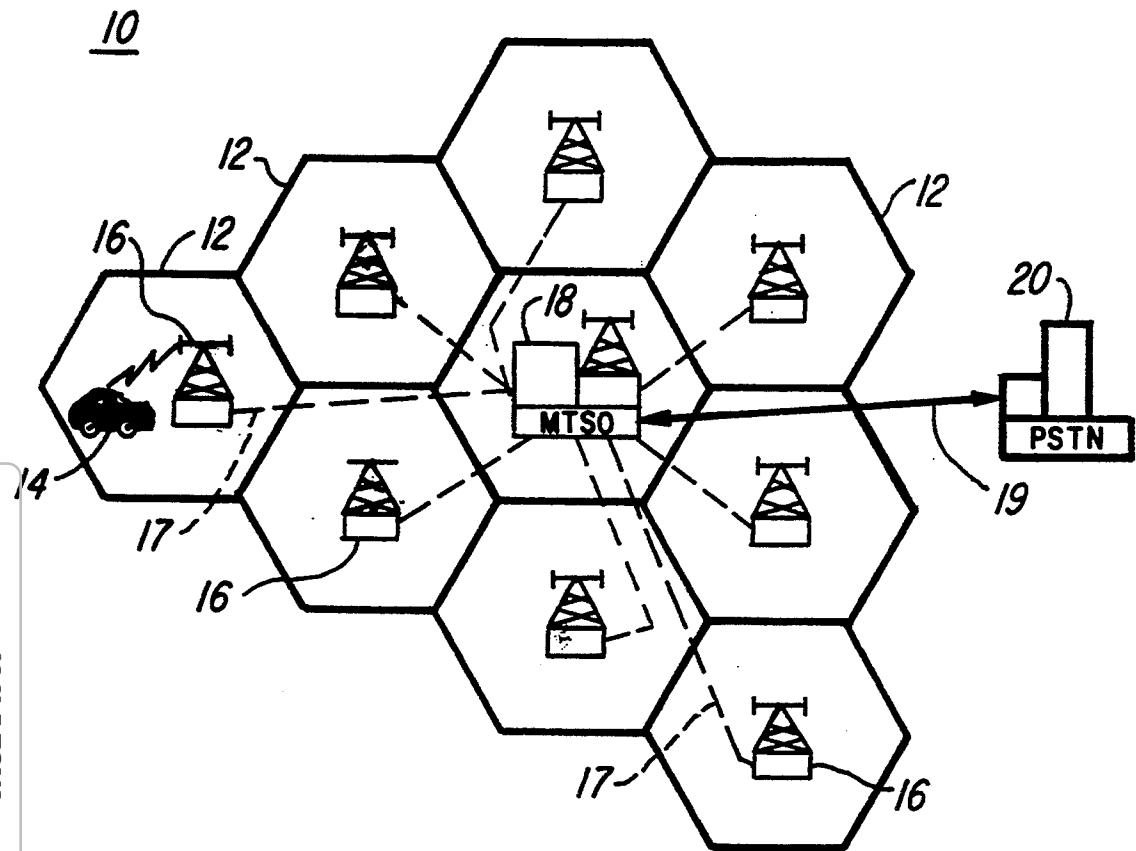


FIG. 1
PRIOR ART

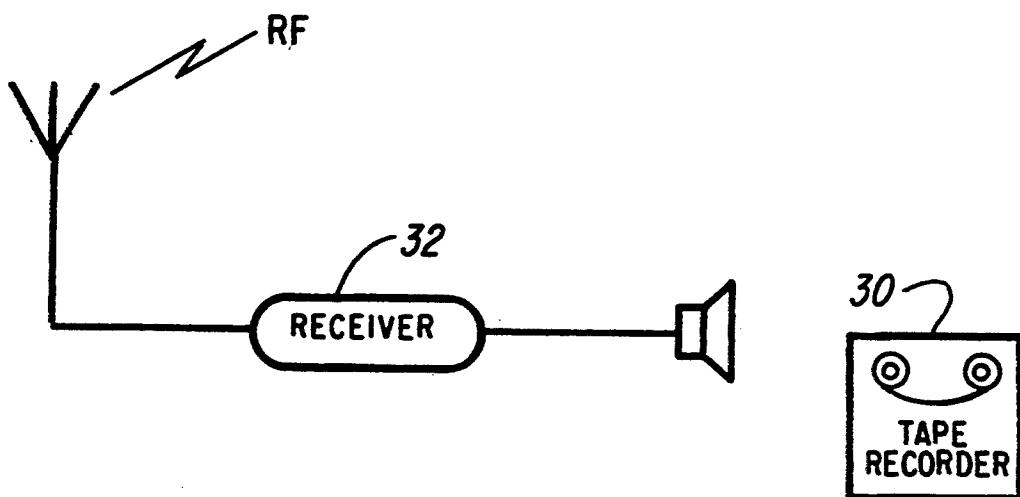


FIG. 2
PRIOR ART

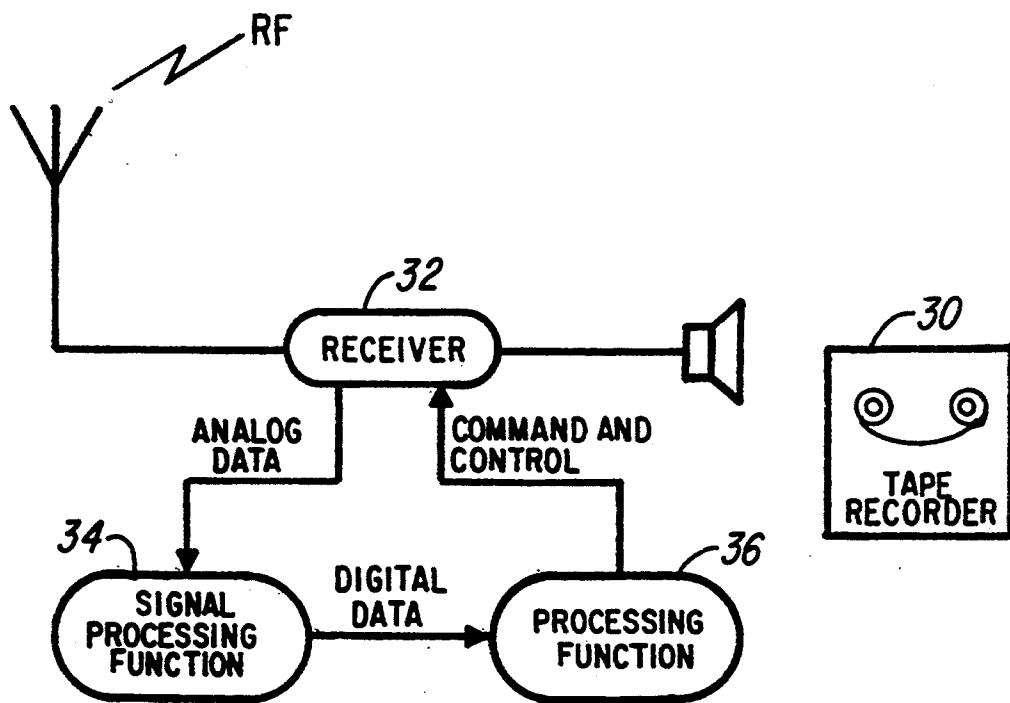


FIG. 3
PRIOR ART

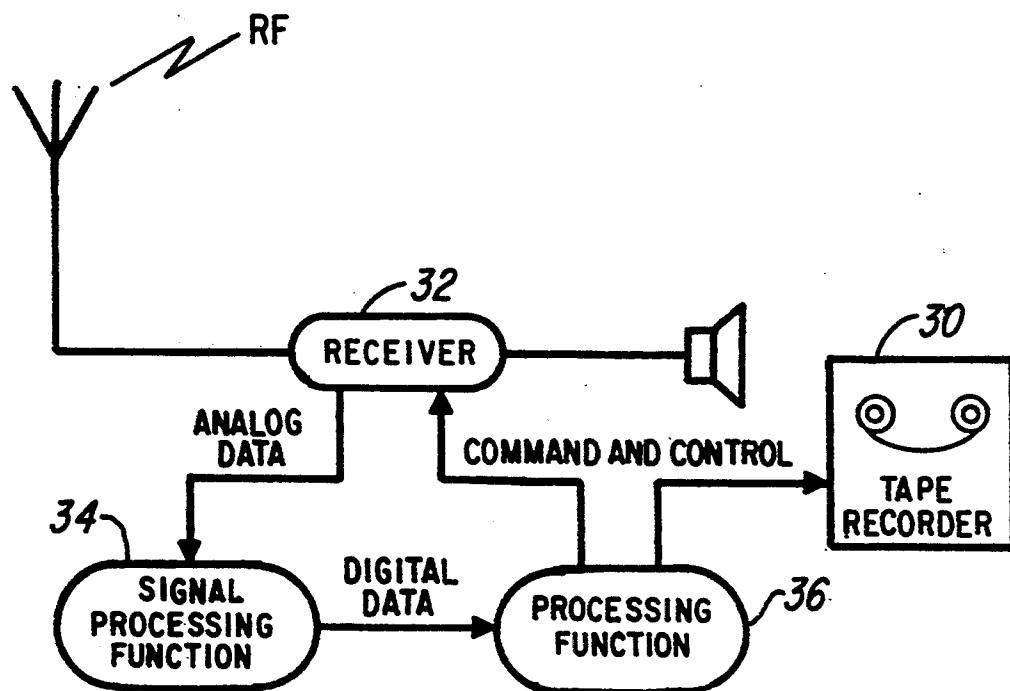
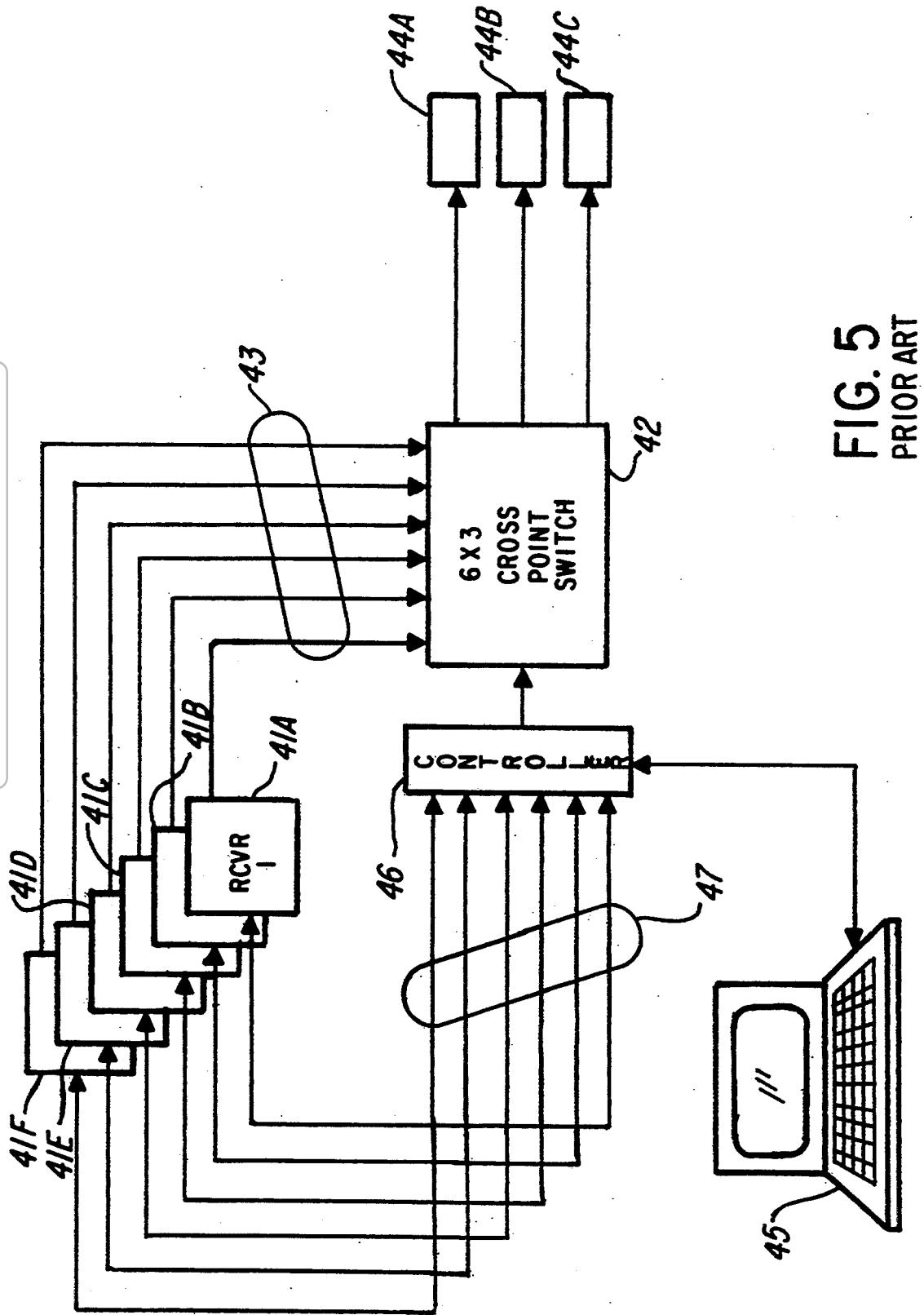


FIG. 4
PRIOR ART

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 3 of 16

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 4 of 16



ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 5 of 16

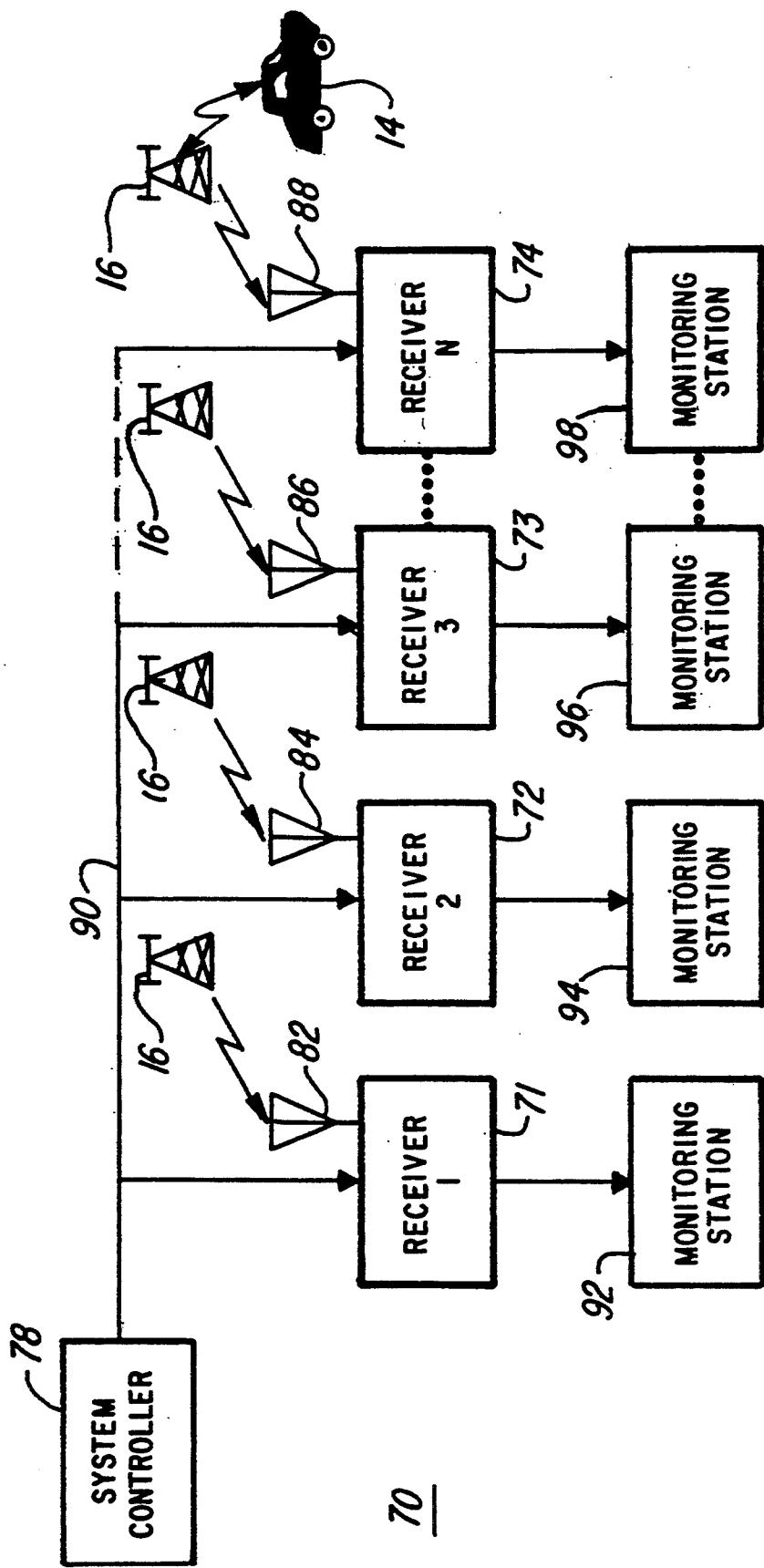
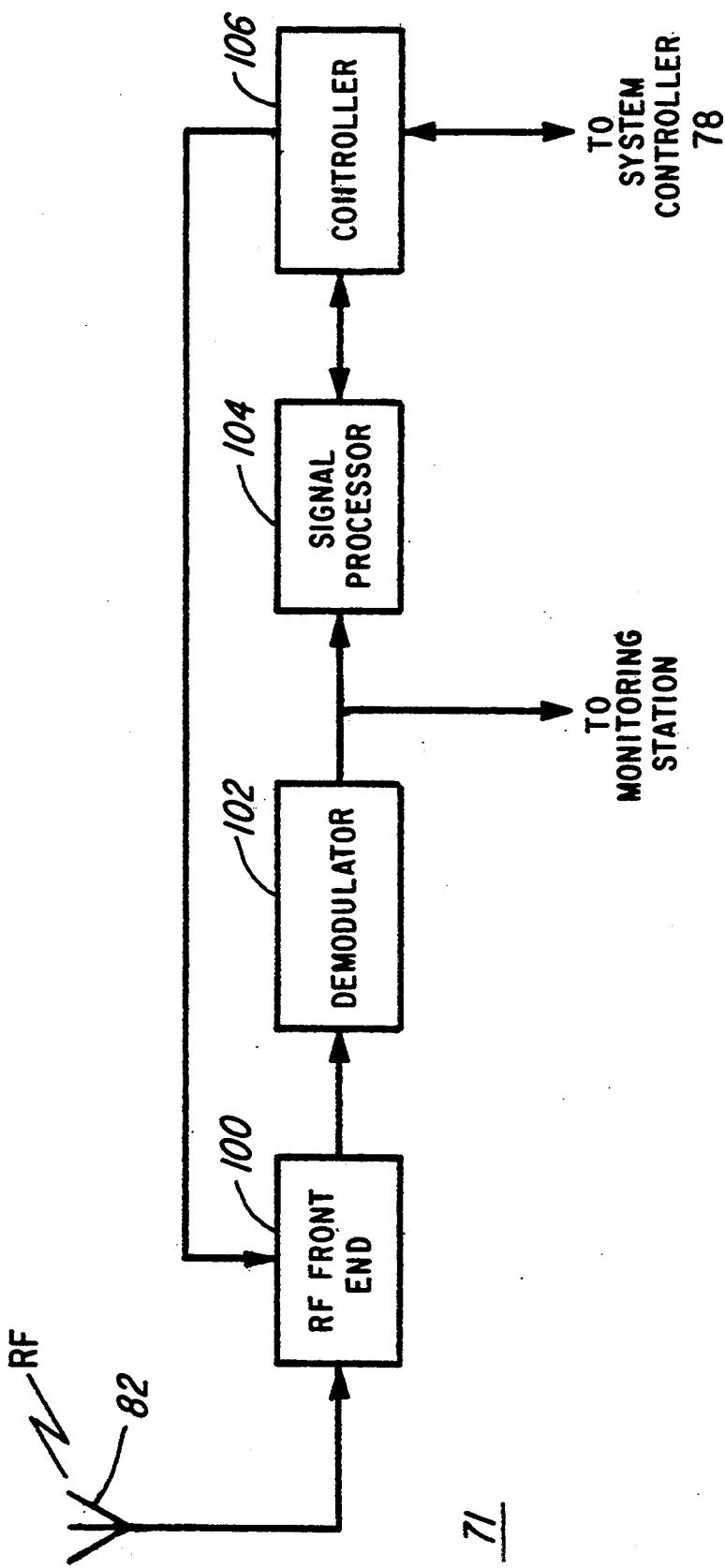
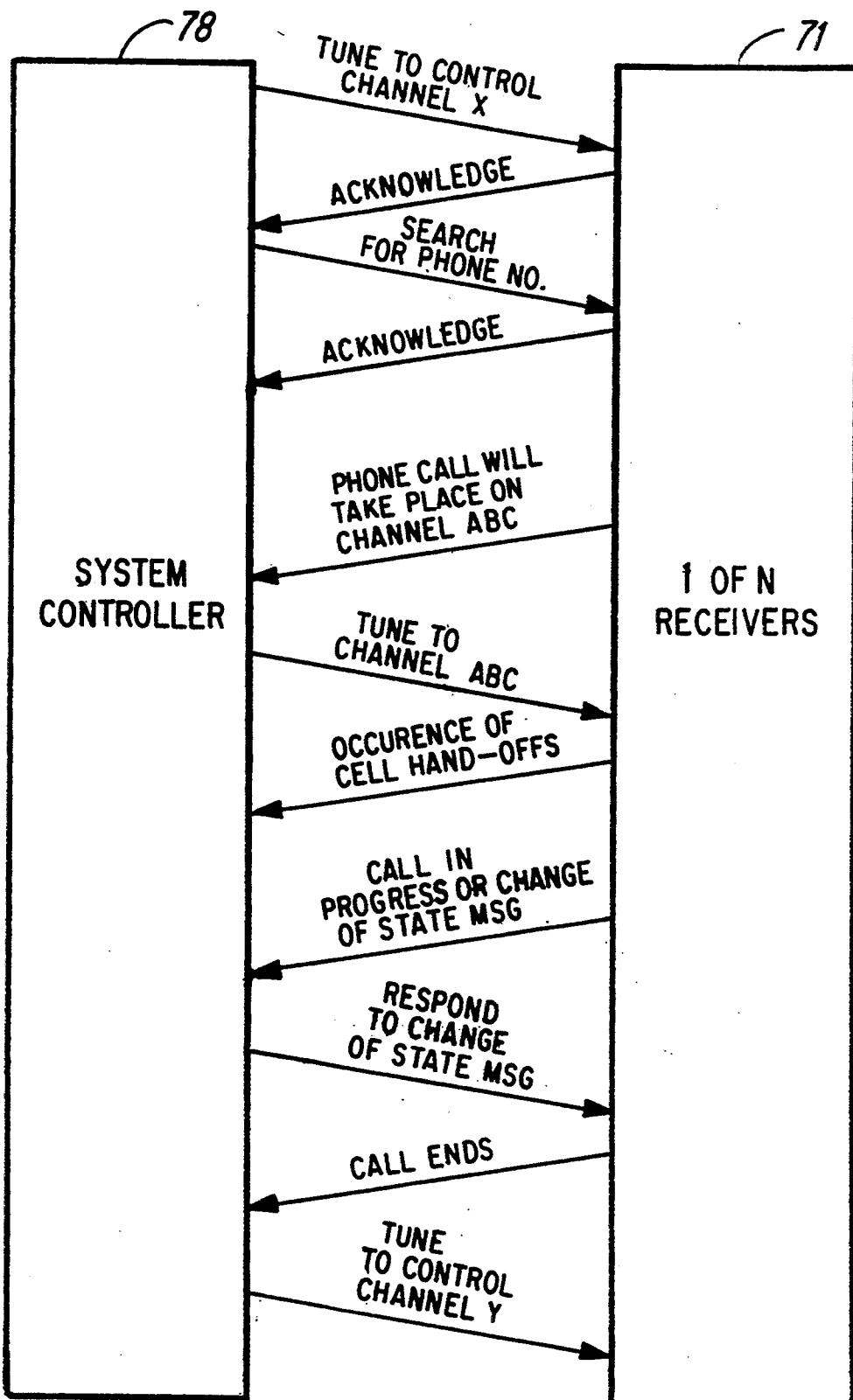


FIG. 6



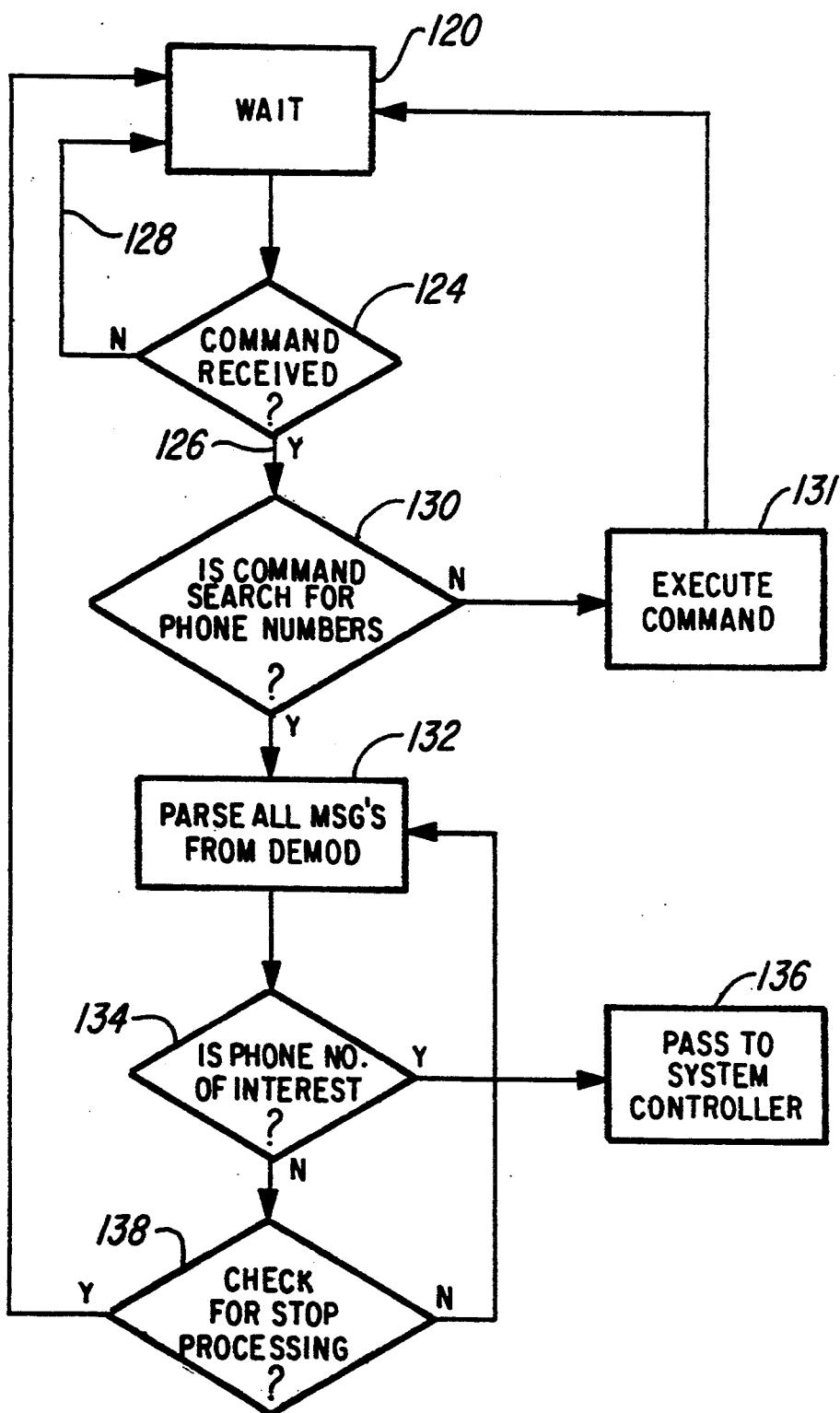
71

FIG. 7



ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 7 of 16

FIG. 8



ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 8 of 16

FIG. 9

MULTI-CHANNEL CELLULAR COMMUNICATIONS INTERCEPT SYSTEM

FIELD OF THE INVENTION

This invention relates to a cellular communications intercept system including a plurality of receivers under control of a system controller for intercepting, monitoring and/or recording cellular telephone conversations.

BACKGROUND OF THE INVENTION

Recent advances in communications technology have created a burgeoning telephony market, both in terms of the availability of new services and new forms of equipment. Cellular telephone technology is one of those new services now being routinely offered in many locations across the country. While cellular telephony is a powerful and efficient new medium, it has also become an important tool for carrying out illegal activities. The mobility and perceived privacy of cellular mobile communications holds significant appeal to those engaged in illegal activities. In fact, in many areas drug dealers routinely use cellular telephony to conduct their day-to-day illegal drug deals.

A prior art cellular system 10 is illustrated in FIG. 1. The cellular system 10 consists of a frequency-modulation (FM) radio network covering a series of geographical areas referred to as cells and identified by reference character 12 in FIG. 1. The two-way radios in each mobile unit, commonly referred to as cellular telephones, operate within the cells 12 by communicating between the mobile unit 14 and a base station 16 within each cell 12. The cellular system 10 is defined by a plurality of base stations 16 distributed over a geographical area of system coverage and managed and controlled over links 17 by a centralized switch referred to as the mobile telephone switching office 18 (MTSO). The base station 16 within each cell 12 has the responsibility for controlling and communicating with all mobile units 14 within the cell and for relaying voice traffic between the mobile units 14 and the mobile telephone switching office 18. The MTSO 18 then relays the voice traffic to the public service telephone network 20 (PSTN) over a link 19.

There are four frequencies used between each base station 16 and any mobile unit 14. Two forward frequencies are used for communication from the base station 16 to the mobile unit 14 and two reverse frequencies are for communications from the mobile unit 14 to the base station 16. One forward frequency is paired with one reverse frequency for communicating control and status information between any mobile unit 14 and the base station 16. A second forward frequency is paired with a second reverse frequency for communicating voice and data between the base station 16 and the mobile unit 14. By convention, these various frequencies are referred to as the forward control channel, the forward voice channel, the reverse control channel, and the reverse voice channel, respectively. Each cell 12 has a single forward control channel and a single reverse control channel for all control and status messages between mobile units 14 within the cell and the base station 16 of the cell. Each cell 12 has a number of forward and reverse voice channels for assignment by the base station 16 as required to meet the communications traffic demands. The forward voice channel is for communicating voice and data from the base station 16 to the mobile unit 14, while the reverse voice channel is

the frequency on which voice/data is passed from the mobile unit 14 to the base station 16.

The following is an example of the technique for setting up an external call in the cellular system 10. 5 When the user of the mobile unit 14 first turns on his cellular telephone, the unit scans all forward control channels to determine the strongest one. Recall that each cell 12 has a base station 16 and each base station has a unique forward control channel. The mobile unit 10 14 then locks onto the strongest received forward control channel, presumably the forward control channel for the cell 12 in which the mobile unit 14 is located, and continues to monitor it.

When a call is placed to a mobile unit 14 from the conventional telephone network, a global page message (or MTSO page), which includes the telephone number or electronic serial number of the called mobile unit, is generated at the mobile telephone switching office 18. 15 The global page is then transmitted in digital format to the base station 16 of every cell 12 that is within the mobile telephone switching office 18. This multiple transmission occurs because the mobile telephone switching office 18 does not know where the target mobile unit 14 is, or if it is within the range of the mobile telephone switching office 18. Each base station 16 then transmits the global page on its unique forward control channel. When the activated mobile unit 14 identifies its own telephone number within the global page, it responds to the base station 16 on the reverse control channel, basically saying, "Here I am". The called mobile unit 14 responds on the dedicated reverse control channel that is unique to the cell 12 in which it is located, and therefore none of the other base stations 16 will see a response to the global page. The base station 16 that is tuned to that reverse control channel sees the response and selects a forward voice channel/reverse voice channel assignment for the mobile unit 14. A command (referred to as a base station page) is then transmitted to the mobile unit 14 from the base station 16 in the form of a voice channel assignment, "I hear you, and please tune to channel x to execute your call". Upon receiving this message, the mobile unit 14 tunes its receiver to the designated forward voice channel to hear the called party and tunes to the paired reverse voice channel to transmit.

This technique for call set up is further complicated as the mobile unit 14 passes from one cell to another during the conversation. The controlling base station 16 continually monitors the strength of the signal from the mobile unit 14 and if that strength diminishes significantly (perhaps indicating that the mobile unit 14 has entered a different cell) then a cell hand-off occurs. To accomplish this, a data message is transmitted from the base station 16 on the forward voice channel telling the mobile unit 14 to tune to a different voice frequency, one that is controlled by a neighboring cell. The mobile unit 14 retunes and the conversation continues on the new frequency. Many cell hand-offs may occur during a single conversation as the mobile unit 14 exits and enters cells.

When the call is completed, the mobile unit 14 scans and locks onto the strongest forward control channel, which again indicates the cell 12 in which the mobile unit 14 resides and listens for a global page that contains its telephone number or electronic serial number.

As discussed above, the mobile unit 14 receives on the forward voice channel and transmits on a different

frequency, the reverse voice channel. This would imply that one would have to monitor both frequencies to hear both sides of the conversation. Such is not the case, however. Because it is unnatural for the telephone user to speak into the telephone and not hear himself in the earpiece. The telephone company transmits the user's voice back for reproduction by the earpiece. This technique is used in the cellular telephony system so that both sides of a conversation can be heard by monitoring only the forward voice channel.

While legal wiretaps can be performed on cellular telephones, where the tap itself is located at the mobile telephone switching office, this type of wiretap is not a complete solution to the problem of monitoring these conversations. If the target mobile telephone is used outside the coverage area of the tapped MTSO coverage is lost. This problem is especially troublesome in areas that are located on the boundaries between adjacent MTSO's. It is obvious that a "fixed site" wiretap on a mobile telephone system cannot be very effective. Therefore, an approach using the mobile communications medium, namely radio frequency reception, has significant advantages. The present invention, as will be described further herein, uses such a radio frequency approach.

One prior technique for monitoring cellular telephone conversations is simply to tune a single scanner or receiver to a forward voice channel and listen to the cellular conversation on that frequency (See FIG. 2). Clearly, this is a hit and miss technique as it requires continuous scanning of the forward voice channels to find a specific target mobile unit. This simple approach provides no way of: (a) following the call during a hand-off; (b) knowing who is talking unless names are spoken; (c) knowing what phone number is being used, other than the fact that it is a cellular telephone; and (d) linking target telephone numbers with cellular conversations (i.e., finding the telephone conversations of the target mobile unit when you know the target's telephone number or electronic serial number). The tape recorder 30 must be controlled manually and the receiver 32 must be manually tuned. These limitations prevent effective use of this technique for legal wiretaps by law enforcement agencies.

A second prior art scheme (FIG. 3) provides the additional feature of following the cellular telephone conversation as it shifts from one voice channel frequency to another, as the target mobile unit passes from one cell to another. This embodiment increases the complexity of the listening device by the addition of the ability to receive and decode the digital data bursts that identify the new voice channel assignment occurring on the existing voice channel frequency. These digital data bursts tell the receiver which frequency to tune to next. The two additional functions required to accomplish this task are identified as the signal processing function 34 and the processing function 36 in FIG. 3. The signal processing function 34 converts the frequency shift keyed (FSK) tone bursts (analog) into digital data by performing a simple FSK demodulation. The digital data representing the new voice channel frequency is communicated to the processing function 36. Here it is decoded and the processing function 36 then commands the receiver 32 to tune to the new frequency. In this embodiment the processing function 36 is manually tuned to establish the initial voice channel frequency to which the receiver 32 is to be tuned. The disadvantage with this embodiment is the inability to find a mobile

unit having a particular telephone number or electronic serial number. Also this technique does not provide the telephone numbers (called or calling) associated with any call that is being monitored. Another limitation of this technique is its ability to only monitor a single forward control channel.

The choice of which single forward control channel to monitor is critical to the probability of intercepting a particular target due to the unique control channel allocation scheme that is based on geographical location. Recall that each cell in a cellular telephone system operates at only one forward control channel frequency. If the mobile target is not located within the coverage area of the cell using the monitored forward control channel, then the voice channel assignment to that target unit will not be available to the intercept system. Therefore, the user of such an intercept system needs prior knowledge of the cell in which the target mobile unit is operating. In those few situations where the correct forward control channel is the one monitored and the voice channel assignment is therefore received, then the intercept unit retunes its receiver to the commanded forward voice channel. The interceptor can now monitor the data on the forward voice channel and is prepared for a cell hand-off when it occurs, as described above.

In yet another embodiment (See FIG. 4) more processing power is included in the processing function 36, providing the ability to store a telephone number that the user is looking for. In this embodiment additional receiver control is added so that the receiver can first be tuned to the forward control channel for receiving telephone numbers and electronic serial numbers. Once the target number is located, the receiver locks onto that target mobile unit, starts the tape recorder, and follows the telephone conversation, including cell hand-offs. This embodiment requires the entering of the target telephone number and then tuning the receiver 32 to the desired forward control channel. This target telephone number information is input to the processing function 36. The processing function 36 also activates the tape recorder 30 when there is a match between the target telephone number and the telephone number picked up by the receiver 32.

If the target mobile unit was stationary or at least began its cellular communication in the same cell site every time, the FIG. 4 embodiment would be satisfactory. However, the nature of cellular communications is mobility. The user therefore does not know where a cellular conversation will originate. The best that can be hoped for is the general vicinity of where that conversation will begin. To solve this problem one could simply add many receivers, each having the functions previously discussed in conjunction with FIG. 4. Such a system would include the number of receivers necessary to cover the area that the target mobile unit might be in, with each receiver tuned to a different cellular control channel within that area.

With this extension of the FIG. 4 embodiment the system now has the capability to intercept cellular telephone calls for a fixed number of cell sites over a geographical area. The limitations of this system include: (a) each receiver must be manually tuned to a designated forward control channel and there must be some scheme for determining the forward control channel of choice; (b) if the target mobile unit has moved out of the geographical area, none of the conversations will be captured; (c) in this scheme the voice channel commu-

nlications associated with a particular target are handled by only that receiver that was monitoring the forward control channel containing the voice channel assignment for the target mobile unit, and (d) since there is one tape recorder for every receiver, the tape recorder can only record those conversations that the receiver with which it is associated is monitoring. As a result of this last stated disadvantage, if the cellular intercept user is trying to gather evidence on a particular person or group of people, that evidence would be spread over several or all the tape recorders. For evidentiary purposes, law enforcement officials must have all conversations related to a particular person or case originally recorded on the same machine. For example, a first call of a target mobile unit is monitored by receiver A, the receiver that was monitoring the forward control channel when the target's call was established. Sometime after terminating that call, the target makes or receives another call, but this time, because the target has moved, receiver B is monitoring the forward control channel for the target's new location and therefore receiver B monitors the call. Since receivers A and B have separate recorders, these two intercepted calls are recorded on-different recorders.

Another prior art system, shown in FIG. 5, allows simultaneous monitoring of multiple targets by a single system, having a plurality of receivers and a baseband switching matrix. The receivers are designated with reference numerals 41A, 41B, 41C, 41D, 41E, and 41F in FIG. 5. A switching matrix 42 provides a path to route the audio signal from each receiver over independent audio signal lines 43 to a separate dedicated monitoring station, identified with reference characters 44A, 44B, and 44C. Control signals from a computer 45 via a controller 46 are input to the switching matrix 42. Control signals are also sent to each receiver from a controller 46 over control lines 47. The computer 45 controls the switching matrix 42 and the receivers 41A through 41F. The capabilities of this system are limited by the current configuration for the computer 45, which usually include no more than six serial ports, with a single port required to control each receiver. Thus only six such receivers can be controlled by the computer 45. Also, the receivers 41A through 41F and the computer 45 must be collocated to reduce signal deterioration due to line length over the control lines 47.

In this FIG. 5 prior art system the audio signal from any receiver can be routed via the switching matrix 42 to any one of separate dedicated monitoring stations 44A through 44C. In practice, the switching matrix 42 is controlled so that the audio from the receiver that identifies the target mobile unit is recorded on a designated monitoring station and then all subsequent conversations that are also related to that target are also recorded on the same monitoring station. In this way the intercept system provides a single tape on which is located all conversations that are relevant to a specific case, where a case is all the telephone conversations relevant to a single wiretap authorization. The disadvantage, however, is that hardware limitations associated with the switching matrix 42 limit the number of recording apparatuses to approximately three. If the system is tracking more than three targets or cases, there will be multiple case recordings on at least one of the recorders. In practical implementation, the switching matrix 42 and its control are highly complex as any of the receivers 41A through 41F may at anytime be switched to any of the monitoring stations 44A through

44C. The complexity of this prior art system grows exponentially more cumbersome with the addition of each receiver and monitoring station.

SUMMARY OF THE INVENTION

The present invention overcomes the limitations discussed above by dynamic reallocation of receiver resources, by interconnection of the receivers with a network, and by including a processing function in each receiver. The system offers judicious use of data exchange between the system controller and each receiver over a high bandwidth local area network and a scheme for dynamically reallocating the receiver resources. With sufficient network bandwidth and controller processor horsepower, the intercept system of the present invention can be expanded to twenty or more channels, as many or few as are needed to cover the entire city or just a part of it. In addition, each of these channels can be a monitoring station for a unique target so that twenty or more targets can be separately monitored and recorded. This expansion also does not require any architecture modifications or hardware reconfiguration, it simply requires adding more receivers to the pool with the necessary software to control them. By putting processing capabilities in each receiver, the load on the system controller is reduced, thus allowing the use of a simpler and less costly controller.

The inventive solution to the disadvantages identified in the prior art systems above involves adding to the plurality of receivers a common point of data entry that has intelligence to know which receiver is tuned to which frequency, which tape recorder is handling which cellular telephone numbers, the ability to query a device in the system to learn what forward control frequencies are available to listen to, and to act as a central collection point for all data coming in from the receivers regarding voice assignments. With this single-point control capability the user can route cellular conversations pertaining to a particular person or group to a specific tape recorder by retuning a specific receiver to the voice channel of the target mobile unit so that conversation can be recorded on the tape recorder identified with that target. Further, this system can follow the target mobile unit through different cell areas by querying the device for active forward control channels on a regular basis and retuning receivers to one of those new control channels as required.

In addition to the single point of data entry and control, a cellular intercept system of the current invention incorporates a network architecture. By using this method of connecting the receivers several advantages are gained. The number of receivers to be connected is unlimited. If the user is targeting a small cell area only a few receivers are needed, but if the targeting area is large, like a large city, the user can connect as many receivers as there are cell sites. The network architecture, with its predefined standards and protocols, allows the receivers to be remotely located from the controller, which is a necessity for covering large areas due to the reuse of certain frequencies within the cellular system as the area of interest grows. The use of a token passing network also allows the receivers to initiate communications with the controller. This is an important distinction from simple wire connections or a bus architecture where the controller must query each receiver to get data from that receiver. A bus architecture also has the disadvantage of limiting the number of

receivers and the distance those receivers can be located away from the controller.

In the present invention the system controller communicates with the plurality of receivers, where several (or all) of the receivers are also connected to monitoring apparatuses, for example a recorder. Each receiver monitors a different cell, or more specifically, the base station page from a different cell in the geographical area of interest, and decodes the telephone number or electronic serial number in the page. The decoded information is input to the controller and when a page identifies a target mobile unit (by telephone number or electronic serial number), the system controller recognizes this and commands one of the receivers to retune to the forward voice channel that was just assigned to the target mobile unit in the page. The retuned receiver is that receiver which is physically connected to the monitoring (e.g. recording) station dedicated to that particular target, i.e., the monitoring station for all communications related to a particular case. Once retuned, the receiver is removed from the pool of receivers monitoring forward control channels. The retuned receiver monitors the forward voice channel of the target mobile unit and follows cell hand-offs as they occur. The system controller may then retune one of the other receivers in the pool to cover monitoring of the forward control channel that the recently retuned receiver had been monitoring. This retuning would be based on a pre-programmed priority scheme. For instance, the highest priority target monitoring station may be physically connected to the receiver that is assigned to monitor the lowest priority cell's forward control channel.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention can be more easily understood and the further advantages and uses thereof more readily apparent, when considered in view of the description of the preferred embodiments and the following figures in which:

FIG. 1 is a diagrammatical presentation of a cellular telephone system;

FIGS. 2-5 are block diagrams of prior art cellular intercept systems;

FIG. 6 is a block diagram of a cellular intercept system constructed according to the teachings of the present invention; and

FIGS. 7, 8, and 9 are diagrams of details of the cellular intercept system of FIG. 6.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

As discussed above, in a cellular telephony system many discrete, limited coverage base transceivers (base stations 16 in FIG. 6) are networked into a system that provides widespread coverage over a geographical area. The connection between the mobile unit 14 and the base station 16 is established by a global page from each base station 16, on its unique forward control channel, in the MTSO network. This global page identifies the called mobile unit 14 by either a telephone number or the electronic serial number. Upon receipt of the global page, the called mobile unit 14 responds, on the reverse control channel, to the base station 16 of the cell in which it is located to identify its presence in the cell. The receiving base station 16 then responds on the forward control channel with a base station page that identifies the voice channel assignment for the called mobile

unit. The base station 16 in that cell then handles the traffic on the forward and reverse voice channels.

Intercepting telephone conversations of a particular target mobile unit can be accomplished by first intercepting the voice channel assignment. Since this channel assignment is available only by intercepting the base station page to the mobile unit 14, the cellular intercept system needs to know the location of the mobile unit 14 and thus the proper cell 12 to monitor. Alternatively, the intercept system must monitor multiple cells to cover a large geographical area, which increases the likelihood of intercepting the appropriate base station page. To monitor several cells in a geographical area requires multiple receivers, where each is capable of identifying the control data associated with a target mobile unit and the voice channel assignment for that target mobile unit. This feature is one of the key aspects of the present invention.

FIG. 6 is a block diagram of a cellular intercept system 70 including receivers 71, 72, 73 and 74 under the control of a system controller 78. While FIG. 6 shows four receivers, it is to be understood by those skilled in the art that the cellular intercept system 70 can be increased in size and coverage area to include any number of receivers, as many as twenty or more given the current processing power associated with the system controller 78.

Each receiver 71, 72, 73 and 74 is connected to an antenna 82, 84, 86 and 88, respectively, for receiving communications from one of the base stations 16 and from mobile units 14. The system controller 78 communicates with each receiver 71 through 74 via an interconnect 90. In the preferred embodiment this interconnect is a token-passing local area network having a bandwidth greater than approximately 200 kb/s, e.g., Ethernet or Appletalk. Access is gained to the network by the well-known token-passing scheme. Each receiver is also connected to a monitoring station, shown in block diagram form in FIG. 6 and identified by reference characters 92, 94, 96 and 98. A monitoring station 40 may include a listening device, e.g., headphones, and/or a recording apparatus. Each monitoring station may also be preassigned to a specific target or case. For example, the monitoring station 92 may be designated to monitor and/or record conversations associated with target A, independent of which receiver 71 through 74 receives the base station page intended for target A. To accomplish this, the system controller 78 controls the receiver 71 to always assign that receiver and its associated monitoring station 92 to all telephone conversations involving target A.

FIG. 7 shows a block diagram of the receiver 71. This block diagram is typical for all receivers in the cellular intercept system 70. Radio frequency signals collected by the antenna 82 are serially processed by an RF front-end 100 and a demodulator 102. The RF front-end 100 and the demodulator 102 incorporate the well-known classical circuitry for performing these functions. The demodulator 102 is capable of demodulating narrow-band frequency modulated signals used in the cellular system. The baseband signal from the demodulator 102 is input to the monitoring station 92 for monitoring and/or recording, as shown in FIG. 7. Immediately prior to a cell hand-off, the new voice channel assignment for the target mobile unit is transmitted over the existing voice channel in the form of audio tones. These audio tones, after passing through the RF front-end 100 and the demodulator 102, are input to a signal processor 104 for decoding. The digital representation of that new

voice channel frequency is input to a controller 106. The controller 106, which is for example a microprocessor, signals the RF front-end 100 to retune to the new voice channel assignment so that monitoring of the cellular telephone conversation can continue on the new voice channel. Information regarding this change in receiving frequency is also sent to the system controller 78 over the interconnect 90. The system controller 78, which is also a microprocessor for example, checks the new voice channel assignment to be sure it is a valid voice channel frequency within the geographical area. The system controller 78 also determines whether other conversations are already being monitored on that same voice channel frequency, and if the other conversations have a higher priority, can command the receiver 71, via the controller 106, to discontinue monitoring activities on that voice frequency.

The basic intent of the communications intercept system 70 is the use of intelligent receivers to minimize network traffic between the system controller 78 and the receivers 71-74. Further, receiver pooling devotes a quantity of n receivers to monitor the base station pages from n cells, with receivers individually removed from the pool, as needed, to monitor conversations of target mobile units. Although only four receivers are illustrated in FIG. 6, it is understood that the system can be increased to include as many as twenty (or more) receivers for increased monitoring capabilities. In setting up the communications intercept system 70, the cells to be monitored are chosen so as to form a coverage net around a target mobile unit's most likely geographic location. The global pages from each receiver 71, 72, 73 and 74 are passed to the system controller 78. Further, after the called mobile unit 14 responds to a global page, the base station 16 transmits a base station page containing the voice channel assignment for the call. This channel assignment will also be received by the receiver monitoring pages in that cell 12, demodulated, decoded, and sent to the system controller 78. Further, prior to system operation, the telephone numbers (or electronic serial numbers) of the target mobile units are entered into the system controller 78 so that a comparison can be made between the target telephone numbers and the telephone numbers received in the global pages. When a match occurs between these telephone numbers, the system controller 78 designates one of the receivers, for example receiver 71, as the intercept receiver. The receiver 71 is then commanded by the system controller 78 to retune to the forward voice channel that had been identified in the base station page. Once retuned, receiver 71 demodulates the telephone conversations of the target mobile unit (as carried on the forward voice channel). The conversation can be monitored and/or recorded at the monitoring station 92, which is dedicated to the receiver 71. In one embodiment, once a receiver is removed from the receiver monitoring pool, the remaining receivers are retuned to always monitor the strongest forward control channels.

The basic aspects of the operation of the cellular intercept system 70, especially the interaction between the receivers 71 through 74 and the system controller 78, are shown diagrammatically in FIG. 8. All signal/commands from the system controller 78 shown in FIG. 8 are input to the controller 106 (See FIG. 7) of the receiver 71. The controller 106 then commands the various functions of the receiver 71 to accomplish the intended result.

The system controller 78 first commands one or more of the n receivers (in this example receiver 71) to tune to a control channel x for the purpose of receiving global pages. All the commands illustrated in FIG. 8 as passing between the system controller 78 and the receiver 71 are passed over the interconnect 90. The receiver 71 responds with an acknowledgement and then the system controller 78 identifies one or more specific telephone numbers that the receiver 71 is to be searching for. The receiver 71 parses large quantities of data in the global pages in search of the specified telephone number. Turning to FIG. 7, this is accomplished by the reception and demodulating of the RF signal in which the called telephone number is encoded. This analog information is decoded in a signal processor 104 and then sent to the controller 106. The controller 106 compares the transmitted or called telephone numbers that are received from the signal processor 104 with the contents of its memory, i.e., the list of target telephone numbers sent from the system controller 78. Note that the system controller 78 can send a different list of telephone numbers to be searched for to each receiver, in this way expanding the capabilities of the system.

When a match is found the receiver 71 acknowledges this by sending a message from the controller 106 to the system controller 78. If the target mobile unit having the specified telephone number received the global page, the same global page that receiver 71 received, the mobile unit will respond, and then the base station 16 in the affected cell 12 will transmit a base station page providing the voice channel frequency assignment. The receiver 71 will also receive the base station page and signal the system controller 78 that the "phone call will take place on channel ABC." With this information in hand, the system controller 78 commands the receiver 71, or any of the other n receivers in the pool, to tune to channel ABC for the purpose of monitoring the target's cellular telephone conversation. As described earlier, the receiver 71 also follows the cell hand-offs as they occur and informs the system controller 78 of these occurrences.

The receiver 71 also informs the system controller 78 that the monitored telephone call continues in progress and whether any state changes have occurred. Examples of such state changes include the occurrence of a cell hand-off or a change in transmitted power level of the target mobile unit. The base station 16 continually monitors the power level of each mobile unit 14 and commands that mobile unit to either increase or decrease the transmitted power level as required to maintain efficient communications. As the need arises, the system controller 78 responds to the receiver 71 with change of state message responses, confirming, for example, a cell hand-off. When a call ends, a message to this effect is sent to the system controller 78, followed by a response to the receiver 71 to tune to a control channel y for receiving global pages and starting the process over again.

FIG. 9 is a diagrammatic representation showing operation of the controller 106, i.e., a controller within one of the receivers 71 through 74. At power up the controller 106 enters a wait state 120. If a command is received, as shown by step 124, processing continues via path 126. If no command is received the controller remains in wait state 120 via the return path 128. Following path 126, there is a step 130 where the command is filtered to determine whether it is a "search for a telephone number" command. If it is not such a com-

mand, then processing moves to step 131 where the command is processed.

If the command is a "search for telephone numbers" command processing moves to a step 132 where the controller 106 parses all the messages from the demodulator 102, decodes them, and passes them to the signal processor 104. As discussed above, the signal processor 104 accepts the analog signal from the demodulator and converts it to a digital signal representing the telephone numbers received. At step 134 query is made as to whether the received telephone number is one of interest. This function is accomplished in the controller 106, where the received telephone number is compared with target numbers received from the system controller 78 and stored in the controller 106. If a match occurs, processing moves to a step 136 where the received telephone number is passed to the system controller 78. Otherwise, processing moves to a step 138. If a stop processing command has been received by this time then processing moves back to the wait state 120. If a stop processing command has not been received, then the controller 106 continues to parse the received telephone numbers and determine whether one is a telephone number of interest at the step 134.

As mentioned above and as represented by step 131 in FIG. 9, there are other commands that the controller 106 processes. The reset or power up command is used to mute the receiver 71 at the beginning of a session, for example. At this time the RF front end 100 can be set to a predetermined frequency or the system controller 78 may issue a command identifying the initial frequency. The receiver 71 can also be commanded to listen to information on various frequencies, including the forward control channel, the forward voice channel, and the reverse control channel. With respect to the forward control channel, the receiver 71 can also be further commanded to listen only to page data or only to voice channel assignment frequencies. The system controller 78 can also issue commands to change the audio output level from the demodulator 102 or to mute that output altogether. On command from the system controller 78, the signal processor 104 can decode power level information obtained from any mobile unit 14.

As previously discussed in conjunction with FIG. 8, at this point the system controller 78 responds to the 45 telephone numbers received and the follow up voice channel assignment by tuning one of the receivers to that voice channel for the purpose of intercepting the cellular telephone conversation.

One key feature of the present invention is the pooling of n receivers to receive both the global pages and the base station pages and the designation of one of those n receivers as the telephone traffic intercept receiver for a particular target. In fact, this designation can be made before any receiver receives page data for that target mobile unit. In any case, when one of the receivers is removed from the pool to monitor and/or record the telephone conversations of the target mobile unit, the remaining receivers continue monitoring global pages in search of telephone numbers for other target mobile units, as illustrated by the example in FIG. 8. In this way, the system operation is optimized so that the maximum number of receivers is always monitoring global pages and as each target mobile unit is found, one receiver drops out of the pool to monitor/record conversations of that target mobile unit.

In the communications intercept system 70 note that the system controller 78 can choose any receiver 71

through 74 to be the monitoring receiver for conversations from any target mobile unit, and thus in effect can have that target mobile unit conversation monitored on any one of the monitoring stations 92, 94, 96, and 98. 5 This is especially helpful in establishing a case for the wiretap authorities in that all conversations for a particular target unit can be routed to a designated monitoring station so that all those conversations are monitored and recorded in sequence.

The system controller 78 can also command any receiver, for example receiver 71 via the controller 106, to tune to a reverse data channel in search of a called telephone number. Once such a called number is identified, the system controller 78 can command any receiver, for example the receiver 71 via the controller 106, to tune to the base page frequency for the cell in which the calling mobile unit is located. The voice channel assignment for the cellular telephone conversation will be transmitted on the base station page frequency and received by the receiver 71. The controller 106 can then retune the receiver 71 to that voice channel frequency and also advise the system controller 78 of this frequency assignment.

As can be seen, the architecture of the communications intercept system 70 easily allows for the expansion of the number of monitoring receivers. Also, if certain receivers are designated as traffic intercept receivers, the number of these can also be expanded. The only limitations on the expansion of the communications intercept system 70 are the capacity of the interconnect 90 and the processing power of the controller 78.

In another embodiment of the present invention each receiver 71 through 74 would broadcast to all other receivers on the network 90 that a telephone number match has occurred between the telephone number transmitted in the global page and the list of target telephone numbers in that receiver's memory. The receiver on the network 90 that is identified as the monitoring and/or recording receiver for that telephone number would then respond back to the initiating receiver with a message that the identified receiver will retune to the voice channel frequency for that cellular telephone conversation and record it. This would be followed by a message to the system controller 78 as to what has occurred. In this embodiment the system controller 78 is relegated to a data entry, display, and overall system configuration role because the receivers 71 through 74 are capable of controlling their own sub-systems and communicating with the other receivers in the cellular intercept system 70. Such a system of distributed control further reduces traffic carried on the interconnect 90.

While we have shown and described embodiments in accordance with the present invention, it is understood that the same is not limited thereto but is susceptible to numerous changes and modifications as known to a person skilled in the art, and we therefore do not wish to be limited to the details shown and described herein, but intend to cover all such changes and modifications as are obvious to one of ordinary skill in the art.

What is claimed is:

1. A cellular communications intercept system for intercepting cellular telephone communications on a cellular network between a base station and a target mobile unit, wherein the cellular network includes a plurality of cells with each cell having a base station, wherein all mobile units communicate with the base station on an assigned voice channel, and wherein each

mobile unit has a preassigned unique identification number, and wherein a global page on a forward control channel from each base station to all mobile units in the cellular network includes the identification number of the called mobile unit, and wherein a base station page on the forward control channel of the base station for the cell in which the called mobile unit is located identifies the voice channel for the called mobile unit, said cellular communications intercept system comprising:

a plurality of tunable receivers, wherein each receiver is tuned to the forward control channel of one base station for receiving the base station pages and the global pages transmitted on that forward control channel;

wherein each of said plurality of receivers includes decoder means responsive to each received global page for extracting therefrom the identification number of the called mobile unit;

wherein each of said decoder means is responsive to each base station page for extracting therefrom the voice channel assignment for the call to the mobile unit;

storage means for storing target mobile unit identification numbers;

comparator means responsive to the identification number of the called mobile unit and responsive to the stored target mobile unit identification numbers and for producing a match signal when the identification number of a called mobile unit matches one of the stored target mobile unit identification numbers;

controller means for controlling said plurality of receivers and responsive to said match signal and said voice channel assignment;

wherein one receiver of the plurality of receivers is designated as the primary receiver for at least one predetermined target mobile unit, and wherein the controller means, in response to the match signal, commands said identified receiver to tune to the assigned voice channel for said at least one predetermined target mobile unit, such that voice communications for said at least one predetermined target mobile unit are received by said identified receiver; and

a monitoring station connected to each one of the plurality of receivers for monitoring all communications intercepted by said connected receiver.

2. The cellular communications intercept system of claim 1 wherein the remaining receivers of the plurality of receivers are retuned, as may be required, to the highest priority forward control channels in the geographic area.

3. The cellular communications intercept system of claim 1 wherein the identification number is the telephone number of the target mobile unit.

4. The cellular communications intercept system of claim 1 wherein the identification number is the electronic serial number of the target mobile unit.

5. The cellular communications intercept system of claim 1 wherein under control of the controller means each of the plurality of receivers can be tuned to a different voice channel assignment such that the communications intercept system can simultaneously monitor the communications of more than one target mobile unit.

6. The cellular communications intercept system of claim 1 wherein the system controller and the plurality of receivers are interconnected by a local area network.

7. The cellular communications intercept system of claim 6 wherein each of the plurality of receivers is located at a site remote from the controller means.

8. The cellular communications intercept system of claim 1 wherein the monitoring station includes a recording device.

9. A cellular communications intercept system for intercepting cellular telephone communications on a cellular network between a base station and a plurality of target mobile units, wherein the cellular network includes a plurality of cells with each cell having a base station, wherein each one of said plurality of target mobile units communicates with a base station on an assigned voice channel, and wherein each one of said plurality of target mobile units has a preassigned unique identification number, and wherein a global page on a forward control channel from each base station to all mobile units in the cellular network includes the identification number of the called mobile unit, and wherein a base station page on the forward control channel of the base station for the cell in which the called mobile unit is located identifies the voice channel assignment for the called mobile unit, said cellular communications intercept system comprising:

a plurality of tunable receivers, wherein each receiver is tuned to the forward control channel of one base station in the cellular network for receiving the global page on that forward control channel;

wherein each of said plurality of receivers includes decoder means responsive to each received global page for extracting therefrom the identification number of the called mobile unit;

wherein the identification number of at least one of said plurality of target mobile units is stored within each of said plurality of receivers;

wherein one receiver of said plurality of receivers is designated as the monitoring receiver for each target mobile unit;

wherein when any one of said plurality of receivers identifies a match between the identification number of the called mobile unit and the identification number of one of said plurality of target mobile units, said identifying receiver produces a match signal that is communicated to each of the other plurality of receivers;

wherein in response to said match signal said receiver of said plurality of receivers having been designated as the monitoring receiver for the identified target mobile unit responds thereto and retunes to the voice channel for the identified target mobile unit for the purpose of monitoring the communications associated with the identified target mobile unit.

10. A cellular communications intercept system for intercepting cellular telephone communications on a cellular network between a base station and a target mobile unit, wherein the cellular network includes a plurality of cells with each cell having a base station, wherein all mobile units communicate with the base station on an assigned voice channel, and wherein each mobile unit has a preassigned unique identification number, and wherein a call is placed by a mobile unit by transmitting the called telephone number on the reverse control channel to the base station of the cell in which the mobile unit is located, and wherein when the call is set up the base station transmits to the calling mobile unit a base station page on its forward control channel

that identifies the assigned voice channel for the call, and wherein in response to the base station page, the calling mobile unit uses the assigned voice channel for the call, said cellular communications intercept system comprising:

a plurality of tunable receivers, wherein each receiver is tuned to the reverse control channel of one base station for receiving the called telephone numbers transmitted on that reverse control channel;

wherein each of said plurality of receivers is responsive to a base station page for extracting therefrom the voice channel assignment for the call; storage means for storing target telephone numbers;

5 15

controller means for controlling said plurality of receivers; wherein the called telephone numbers are input to said controller means; wherein the voice channel assignments are input to said controller means; wherein one receiver of the plurality of receivers is designated as the primary receiver for at least one target mobile unit; and wherein when the called telephone number matches a target telephone number, said controller means causes said primary receiver to tune to the voice channel assignment for the call for monitoring the telephone call.

* * * * *

20

25

30

35

40

45

50

55

60

65

US005870029A
CALENDAR: 11

PAGE 1 of 7

5870029

[11] Patent Number **5870029**
 [45] Date of Patent **May 11, 1999**
 CIRCUIT COURT OF COOK COUNTY, ILLINOIS
 CHANCERY DIVISION
 CLERK DOROTHY BROWN

United States Patent [19]**Otto et al.**

[54] **REMOTE MOBILE MONITORING AND COMMUNICATION SYSTEM**

[75] Inventors: **James C. Otto**, Indian Harbor Beach; **Brian P. Holt**, Melbourne; **Arthur L. Stewart**, Melbourne Bch., all of Fla.

[73] Assignee: **Harris Corporation**, Melbourne, Fla.

[21] Appl. No.: **676,503**

[22] Filed: **Jul. 8, 1996**

[51] Int. Cl.⁶ **G08B 5/22; G08B 23/00**

[52] U.S. Cl. **340/825.36; 340/825.31;**
340/825.49; 340/573; 379/38

[58] Field of Search **340/825.36, 825.31,**
340/573, 825.06, 825.54, 825.49, 572, 539,
568, 525; 379/38

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,918,432	4/1990	Pauley et al.	340/573
5,369,699	11/1994	Page et al.	379/38
5,396,227	3/1995	Carrol et al.	340/825.31

5,414,432	5/1995	Penny et al.	342/357
5,461,390	10/1995	Hoshen	340/825.49
5,568,119	10/1996	Schipper et al.	340/825.37
5,627,526	5/1997	Belcher et al.	340/825.49
5,742,233	4/1998	Hoffman et al.	340/573
5,751,245	5/1998	Janky et al.	340/993

Primary Examiner—Edwin C. Holloway, III

Assistant Examiner—Edward Merz

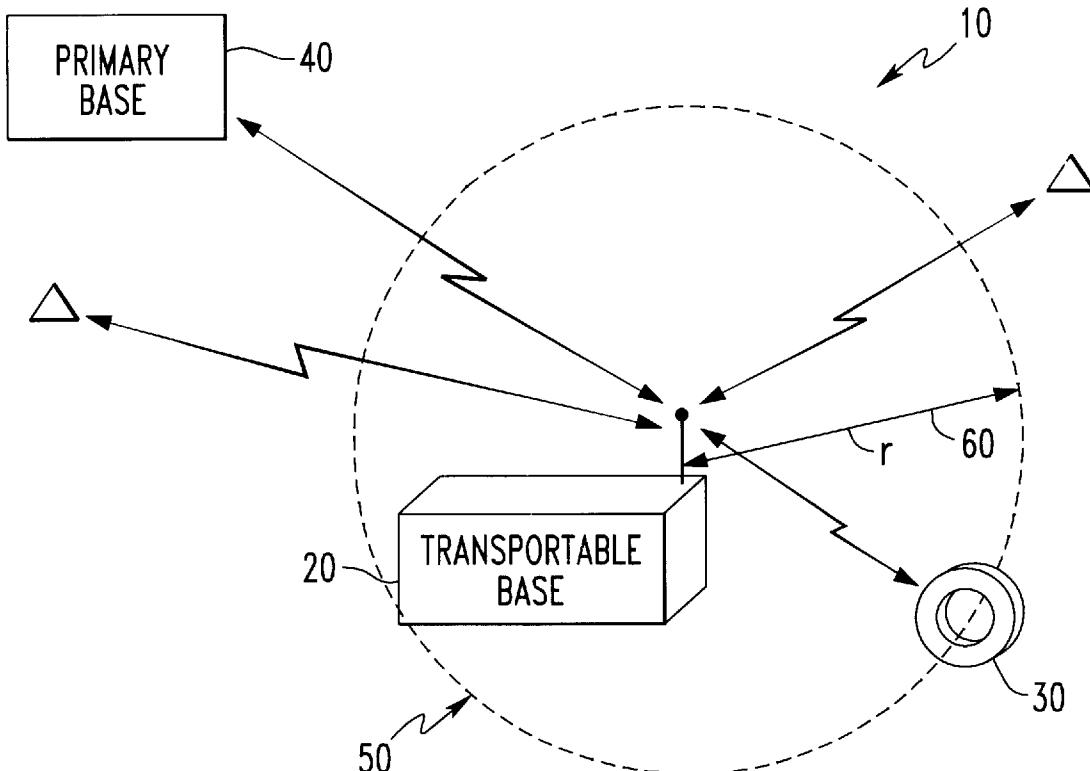
Attorney, Agent, or Firm—Rogerst Killeen

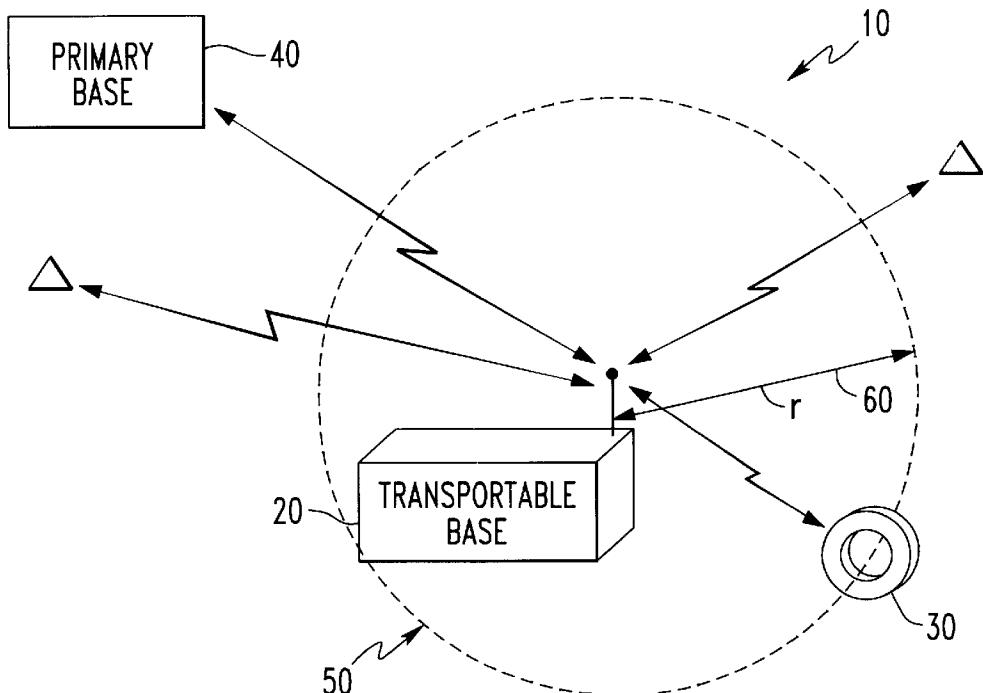
[57]

ABSTRACT

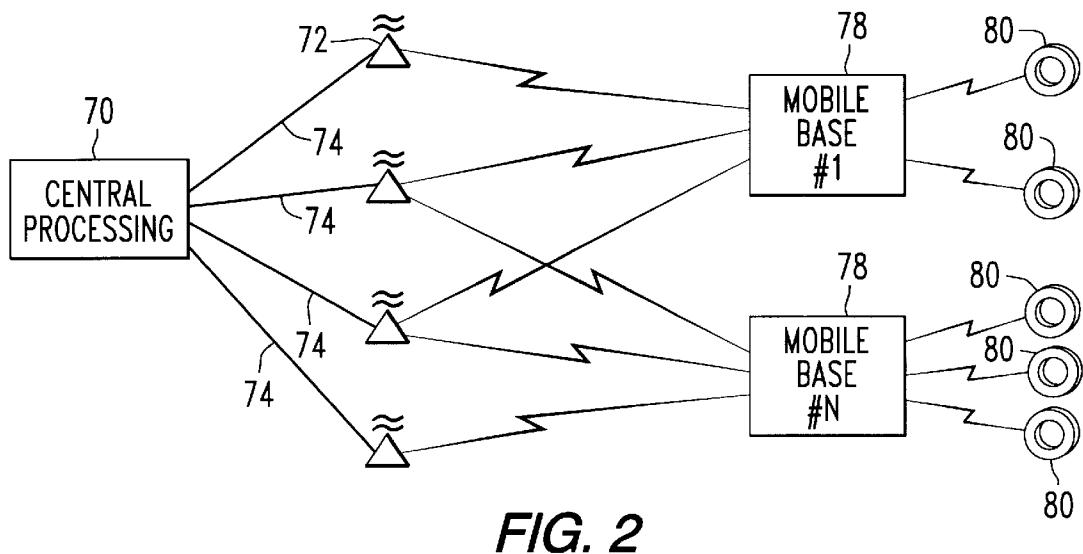
A system and method for monitoring the location and/or presence of an object/person within a desired area includes a mobile base station, a central control center, a mobile signaling device carried by the monitored object/person, and a geolocating means. The mobile base station may be transported to an arbitrary site and retains the monitored object/person within a desired area. The central control center determines the acceptability of the location of the monitored object/person and may raise an alarm condition when the monitored object/person is not within the desired area.

26 Claims, 1 Drawing Sheet





ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 2 of 7



1

REMOTE MOBILE MONITORING AND COMMUNICATION SYSTEM

BACKGROUND OF THE INVENTION

The present invention relates generally to systems for communication with and for monitoring the locations of mobile, remote objects, including people. More particularly, the present invention relates to a system for locating and communicating with the objects (including people) without burdening the monitored object with heavy or bulky communications equipment.

Prior art systems illustrate the various needs for the present invention and that those efforts only partially meet these needs. For example, house arrest systems continuously monitor persons sentenced to remain within a defined, restricted area to assure they do in fact remain within the permitted area. These systems offer continuous oversight but suffer from being able to monitor the offender only at a single fixed location, e.g., his home.

Other prior art prisoner monitoring systems attempt to accommodate the offender sentenced to remain principally within one area but is allowed to travel to a second area during limited times, e.g., the offender must remain at her home except during working hours when she may travel to her place of business. However, these systems are not able to continuously monitor the offender and have limited monitoring areas or distances.

Another type problem exists regarding the need to quickly recover stolen vehicles. Certain type vehicles or assets, known as favorite targets of car thieves, may have installed vehicle tracking systems. These vehicle tracking systems, powered by the vehicle's battery and not unduly limited in size or transmission power capability, allow authorities to track the location of the vehicle over an extended range and for an extended period of time. Such systems, however, do not notify the owner that the vehicle has been stolen and the vehicle is often transported out of the searchable area or disassembled before the theft is discovered and the recovery system activated. A need is therefore present to promptly notify the vehicle owner that the vehicle has been stolen.

In a similar fashion, an automated notification system is needed to notify the proper authorities when an asset has been moved from a given location. For example, in banks it is known to hide a small explosive device coupled with a permanent dye within one or more bundles of currency. When the dye-carrying bundle is removed from the bank, a signal is provided to the explosive device causing it to detonate, spewing the dye upon the currency and persons nearby. One problem with such devices is the fact that innocent passers-by may be injured by the impact from the explosion and the fact that the thief may become more violent in response to the explosion. Accordingly, it is desireable to use a proximity locating device within such currency bundles. The passage of the proximity device outside the range of a base unit could be made to cause an alarm to be signaled at the appropriate authorities and, if desired, to initiate geolocating the locating device within the currency bundle, all without alerting the thief or causing explosions in the vicinity of potentially innocent persons.

U.S. Pat. No. 4,918,432 to Pauley, et al. for a "House Arrest Monitoring System" illustrates a prior art system wherein the monitored individual's movement is limited to a single fixed area. Pauley, et al. discloses a system comprising an small transmitter in the form of an identification tag which is worn by the monitored individual and which transmits a periodic signal directly to a Field Monitoring

2

Device (FMD) or, if the fixed area has communication dead spots, via a repeater to the FMD. The FMD then communicates to a central, fixed location, e.g., by modem and telephone line, to notify the central location when the monitored individual leaves or re-enters the monitored area. If the monitored individual leaves the fixed area, the central location is not aware of the individual's location. Disadvantageously, no provision is made for the central location to communicate with the individual or the individual to communicate with the central location. Such features are necessary if the system is being used to monitor and communicate with an individual who is under protective custody such that they must be able to freely move about without carrying heavy, bulky equipment and such that they must be in ready contact with central monitoring site to transmit or receive a panic signal.

U.S. Pat. No. 5,461,390 to Hoshen for a "Locator Device Useful for House Arrest and Stalker Detection" illustrates a prior art effort to provide intermittent mobile monitoring of an individual by periodically contacting and determining the location of a locator device attached to the individual in the form of a small transceiver strapped to the individual's leg. The central location initiates a monitoring cycle by transmitting a polling signal, via a wireless, e.g., cellular, system to the locator. Upon receipt of the polling signal, the locator queries a positioning system to ascertain its current location and transmits the location back to the central computer. The central computer then completes the monitoring cycle by comparing the individual's location against database records to determine if the individual is within an authorized location. While this system offers a degree of mobility for the monitored individual, requirements to keep the locator device small and lightweight, mandate compromises in transmission distances and frequency with which the locator can be polled. Therefore, continuous monitoring by the central location and communications at greater distances from the wireless transmission points between the central location and the locator device are not possible.

SUMMARY OF THE INVENTION

Accordingly, it is an object of the present invention to obviate many of the problems and limitations of the prior art.

It is another object of the present invention to provide a novel monitoring and communication system whereby a primary base location may continuously monitor a remote, mobile individual, affixed with a personal transceiver, through indications that the individual is within a defined area around a mobile but determinable location by supplementing the primary base location with a transportable, remote base operably maintaining communications between both the primary base location and the mobile individual.

It is another object of the present invention to provide a novel monitoring and communication system whereby a fixed base location's continuous monitoring a remote, mobile individual is enhanced by the fixed base location selectively varying the size of the defined area within which the mobile individual is monitored.

It is yet another object of the present invention to provide a novel monitoring and communication system utilizing a principal base operatively in contact with a mobile individual through a remote, transportable base transmitting to the principal base information concerning location and proximity of the mobile individual, the degree of proximity selectively adjustable at the transportable base or by the mobile individual.

It is still another object of the present invention to provide a novel monitoring and communication system wherein a

mobile individual may communicating with a remote fixed base by causing a mobile, transportable base in close proximity to the individual to transmit a signal to the fixed base. The transportable base may be able to self-determine or to provide signals to assist systems to determine the geolocation of the transportable base (and hence of the mobile individual).

It is a further object of the present invention to provide a novel method for a fixed base monitoring location to communicate with a remote, mobile individual by causing a mobile, transportable base in close proximity to the individual to transmit a signal to that individual.

It is yet a further object of the present invention to provide a novel transportable monitoring base which may determine its own geographic location, maintain communications with a mobile entity in nearby proximity, oversee whether the entity remains within a predetermined range, and communicate this information with a remote, fixed location.

It is still a further object of the present invention to provide a novel transportable monitoring base which maintains communication with a mobile transceiver, oversees whether the transceiver remains within a selectable range, provides its information to a remote, fixed location, and relays information from the fixed location to the transceiver.

These and many other objects and advantages of the present invention will be readily apparent to one skilled in the art to which the invention pertains from a perusal of the claims, the appended drawings, and the following detailed description of the preferred embodiments.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a pictorial representation of one embodiment of the system of the present invention.

FIG. 2 is a pictorial representation of an alternative embodiment of the system of the present invention.

DESCRIPTION OF PREFERRED EMBODIMENTS

With reference to FIG. 1, the present invention is illustrated by a preferred embodiment suitable for use as a prisoner monitoring system which monitors the prisoner within a defined area about a mobile but constantly known location and further indicates if the prisoner leaves the monitored area. The system 10 may include three principal, interactive components: a transportable base 20, a prisoner bracelet or tag 30, and a primary control base 40.

The transportable base 20 may include a portable power source which enables the long-term, mobile movement of the transportable base and, accordingly, the prisoner; a geolocating device which enables the system to remain cognizant of the location of the transportable base; a first proximity device cooperatively operating with the prisoner bracelet 30 to monitor whether the prisoner is within the defined monitoring area 50; and a transmitter for continuously communicating with the primary control base its current location and an indication of whether the prisoner is within the defined monitoring area. Thus, by serving intermediate the prisoner bracelet and the primary control base and by remaining in constant communications with both the prisoner bracelet and the primary control base, the transportable base 20 facilitates continuous prisoner monitoring while allowing the prisoner an increased degree of mobility albeit while being electronically tethered to the transportable base.

The prisoner bracelet 30 (or "tag") is affixed to the prisoner in one of several ways known in the art, e.g., by a

form-fitting strap to the leg or by close fitting rigid multi-piece bracelet around a forearm above the wrist. The bracelet 30 includes a second proximity device operable with the first proximity device of the transportable base 20. The transmission characteristics of the first and second proximity devices jointly define a monitoring distance, "r" 60, between the two devices originating at the transportable base. The area circumscribed about the transportable base by the monitoring distance, "r", determines the monitoring area 50. The monitoring distance 60, and hence the monitoring area 50, is desirably set some amount less than the maximum communication range between the transportable base and the prisoner bracelet.

While the preferred embodiment is described as being used with prisoners, the present invention is by no means limited to such situations and may be used to monitor the location of any mobile persons or objects. For example, the unit could be used to monitor the location of school children on a field trip or outing, with the transportable base being carried in a school bus. In another exemplary embodiment, a system of the present invention can be used to ensure that sentries are properly posted within a predetermined range of an object to be protected. Note that the ability of the transportable base to be moved and to geolocate enhances the usefulness of the invention as the transportable system may be readily established around any area needing security (such as the area surrounding a head of state while on tour.)

Note also that although the described embodiments describe the mobile unit as being housed in a bracelet, many different housings are possible which meet the environmental restrictions of a particular system or location.

The transportable base may include conventional means such as signal strength, doppler effects, phase shifting, radio direction finding, Time Difference of Arrival ("TDOA") and radio frequency ranging for determining the set monitoring distance and the actual distance between itself and the bracelet. The means may, for example, include a monitoring system such as that disclosed in U.S. patent application Ser. No. 055,166, entitled "Proximity Detector Employing Sequentially Generated Mutually orthogonally Polarized Magnetic Fields", by Belcher, et al. filed Apr. 30, 1993 and now abandoned, or in U.S. patent application Ser. No. 315,348, entitled "Proximity Detection Using DPSK Waveform", by Belcher, et al., filed Sep. 30, 1994 now U.S. Pat. No. 5,627,526.

The means for determining monitoring distance described above, generally determine a distance from a receiver but not a location with respect to the receiver. In an alternative embodiment, a system in accordance with the present invention may also include a transportable base unit having a monitoring means which can determine more than the distance a monitored object is from the base station but may also provide information regarding the location and/or relative location of the monitored object from the transportable base unit.

In such an alternative system, sentries in a defined area could be monitored to ensure not only that they have not left the defined area but that they are positioned with respect to one another to avoid "holes" in the perimeter of the monitored area. In such a system, each sentry could carry a mobile unit and be monitored by the transportable unit as to position. The transportable unit or the central unit may use the sentry position information to ensure that the sentries remain on post and have not unwittingly converged in one area, leaving another area unprotected.

Similarly, in an alternative embodiment, the system of the present invention may be used to monitor mobile objects

such as automated search equipment. In such an embodiment, the mobile equipment can be affixed, for example, to mobile sensor systems which are used to search a defined territory for a predetermined object. By monitoring the mobile units with the alternative base unit having the ability to locate the mobile units, the user of the system may ensure that the entirety of a given area has been searched.

In a preferred embodiment the transportable base and the prisoner bracelet communicate using an conventional RF scheme and protocol. Alternative means of communications include microwave, radio frequency, spread spectrum, and proprietary RF encoding/decoding schemes.

The primary control base 40, receiving communications from the transportable base, monitors the location of the transportable base and whether the prisoner has left the monitored area. In a preferred embodiment, the transportable base communications, received by the primary control base, consist of a location communication and an affirmative communication that the prisoner is within the monitored area. In an alternative embodiment, the transportable base communications consist of a location communication and a communication only if the prisoner leaves the monitored area. In yet another embodiment, the transportable base only sends location communications when the transportable base is mobile and its location is changing.

Geolocating of the transportable base may use any conventional geolocating technique and may be carried out by the transportable base or by another system. For example, the transportable base may use geolocating navigation satellites, inertial navigation, dead reckoning based on self-contained sensors, or any of the many navigation aids currently available (such as LORAN and/or aircraft systems.) Alternatively, the transportable base may provide a signal or have an identifying characteristic such that other systems can determine the location of the transportable base and communicate the geolocation of the base to the central system. Examples of such systems include the use of a beacon emanating from the transportable unit which can be sensed and geolocated by existing radio receivers such as orbiting satellites or cellular base stations. In such a situation, the sensing unit may use conventional means to report the geolocation of the transportable base to the central location. If needed for a particular application, the transportable unit may be energized while moving, permitting the monitoring system to be operating even though it is not in a fixed location.

In a preferred embodiment the transportable base and the primary control base communicate using RF communications. Alternative means of communications include microwave, radio frequency, spread spectrum, satellite link, computer network, direct digital (ISDN) and/or modulated signals over a telephone link. Generally, it is desirable that such signals between the base unit and the central unit be encrypted or encoded in such a way so that the system cannot be readily fooled or spoofed by intercepting or interfering signals.

As mentioned earlier, in an alternative embodiment, the transportable unit may monitor a plurality of mobile units, such units providing either distance or location information, and each uniquely identifying itself to the transportable unit by conventional means or by the means disclosed in the referenced application by James C. Otto.

The primary control base also includes means for selectively displaying the location of the transportable base and an "out-of-area" alarm for indicating receipt of an indication the prisoner has left the monitored area centered on the transportable base.

Because the bracelet requires only minimal circuitry to communicate with the transportable base and is not burdened with other functions such as geolocating or transmissions back to the primary control base, its power requirements are greatly reduced permitting long battery life in a small and unobtrusive package. Since the transportable base may be located at a convenient distance from the prisoner and may be concealed within an unobtrusive container such as an automobile trunk or a briefcase, the size and power consumption of the transportable base are less critical. The portable power supply may therefore be of convention design and sized to meet monitoring/transmission distance and duration requirements consistent with the specific prisoner monitoring application.

In an alternative embodiment, some of the components described as being in the transportable base may be included in the mobile unit and vice versa and still come within the scope of the present application. For example, the geolocating capability may be contained in the mobile units which relay a relatively low power signal with the geolocation information to the transportable base unit. Because the mobile units communicate with a relatively nearby transportable base unit and not with a remote central unit, the power requirements for this embodiment of a mobile unit may be kept minimal to reduce the need for and weight of a large battery to be carried around by the mobile user.

The afore-described preferred embodiment of the present invention can be modified to accommodate other uses where an individual is desirably monitored from a distant location and additionally communications between the monitored individual and the distant location are necessary.

In such instances, the size of the area may be desirably changed to increase or decrease the distance from the transportable base. The monitored individual would then be allowed to move without setting off an "out-of-area" alarm. As described, by varying the power and transmission characteristics of the first and second proximity devices, the monitoring distance, "r", between the two devices may be varied. To accommodate this, the transportable base may further include means for a local operator to vary the power to or the transmission characteristics of the first proximity device to vary the effective monitoring distance. In this way the monitored individual is provided with either a smaller or larger monitored area. Alternatively, the primary monitoring base may include a transmitter and the transportable base may include a receiving section so that the primary monitoring base may selectively change the monitoring distance by sending a signal to the transportable base.

In another alternative where the monitored individual is provided more information and control, the transportable base may transmit distance information to the bracelet which may include a distance indicator. In this embodiment, the bracelet may include a selector which causes the transmission of signals to the transportable base to selectively change the monitoring distance. The bracelet may further include a "panic button" which, upon depression, transmits a signal to the transportable base, which signal causes the transportable base to send a panic signal to the primary control base. The control base includes an alarm for indicating receipt of the panic signal.

Such a monitoring application may also require that the primary control base quickly contact the monitored individual. The control base may selectively transmit a signal to the transportable base, such signal causing the transportable base to transmit a signal to the bracelet. The bracelet may include a means to receive this signal and an alarm indicating the receipt of the signal.

With reference now to FIG. 2, an alternative embodiment of the present invention may include a central processing unit **70** which communicates with one or more substations **72** via conventional communications links **74**. The substations **72** communicate with one or more mobile base stations **78**, each of which may be communicating with one or more monitored units **80**.

As described earlier, the base stations **78** communicate with the monitored units **80** to ensure that the monitored units **80** remain within a desired proximity to the base station **78**. The mobile base stations may determine their own geolocation (such as by a GPS locator) and send information regarding their location to the substations **72** or may provide a signal by which an external device or system may determine and report the geolocation of the mobile base **78** to the substation **72**. As the mobile base stations **78** travel from one location to another, the base stations **78** may communicate with different substations **72** so that an entire region, covered by plural substations **72**, may be within the permissible travel locations of the base stations **78**. As the mobile stations travel from the area of one substation **72** to another, the control of and information regarding the mobile base stations **78** may be passed from one substation **72** to another, under the control of the central processing unit **70**.

While preferred embodiments of the present invention have been described, it is to be understood that the embodiments described are illustrative only and the scope of the invention is to be defined solely by the appended claims when accorded a full range of equivalence, many variations and modifications naturally occurring to those of skill in the art from a perusal hereof.

What is claimed is:

1. A system for monitoring an entity's location and for indicating that the entity has left a defined area around the location, the system comprising:
 - a mobile base for establishing a center from which the defined area is defined, said base comprising,
 - a portable power source so that said base may be transported,
 - first proximity means for indicating that the entity has left the defined area, and
 - means for transmitting the location of said base determined by a geolocating device and the indication that the entity has left the defined area provided by said first proximity means;
 - a tag for being carried by the entity comprising second proximity means operable with said first proximity means for setting a size of the defined area and determining that the entity has left the defined area; and,
 - said geolocating device for determining a location of said base and for providing the location to said base; and,
 - a control center for monitoring the location of said base and for providing an indication that the entity has left the defined area, said control center comprising,
 - means for receiving transmissions from said base,
 - means for selectively displaying the location of said base, and
 - an alarm for indicating receipt of the indication that the entity has left the defined area.
2. The system of claim 1 further comprising means for selectively varying the size of the defined area set by said first and second proximity means from said control center.
3. The system of claim 1 further comprising means for selectively varying the size of the defined area set by said first and second proximity means from said base.
4. The system of claim 1 further comprising means for selectively varying the size of the defined area set by said first and second proximity means from said tag.

5. The system of claim 1 wherein said means for transmitting and said means for receiving comprise a computer network.

6. The system of claim 1 wherein said base further comprises a means for determining the distance between said base and said tag.

7. The system of claim 6 wherein said base further comprises a means for transmitting the distance between said base and said tag to said tag, and said tag further comprises a means for indicating said distance to allow said entity carrying said tag to monitor the distance between said base and said tag.

8. The system of claim 1 wherein said tag further comprises means for selectively causing said base to transmit to said control center to allow said entity to signal said control center.

9. The system of claim 8 wherein said control center further comprises an alarm for indicating receipt of said signal transmission initiated by said entity and said base further comprises an alarm for indicating the tag has initiated a signal transmission to the control center.

10. The system of claim 1 wherein said control center further comprises means for selectively causing said base to transmit to said tag to allow said control center to signal said entity carrying said tag and

said tag further comprises an alarm for indicating receipt of said signal transmission initiated by said control center.

11. The system of claim 1 wherein said geolocating device is at said mobile base.

12. A system for ascertaining whether an entity is within a defined area centered on a mobile base, said mobile base comprising:

- a portable first power source so that said base may be transported,
- a geolocating device for determining the present location of said base,
- first proximity means for ascertaining whether the entity is within the defined area, said first proximity means being operable with a second proximity means carried by the entity for setting a size of the defined area and ascertaining whether the entity is within the defined area; and
- means for transmitting the location of said base determined by said geolocating device and an indication of whether the entity is within the defined area provided by said first proximity means.

13. The system of claim 12 further comprising a control center for monitoring the location of said base and for providing an indication that the entity is not within the defined area, said control center comprising:

- means for receiving transmissions from said base,
- means for selectively displaying the location of said base, and
- an alarm for indicating receipt of the indication that the entity is not within the defined area.

14. The system of claim 12 wherein said control center further comprises means for varying the size of the defined area set by said first and second proximity means.

15. The system of claim 12 wherein said base further comprises means for varying the size of the defined area set by said first and second proximity means.

16. The system of claim 12 further comprising a second power source to provide said base with an alternative power source.

9

17. The system of claim 12 wherein the base further comprises
an alarm activated upon the first proximity means ascertaining the entity is not within the defined area and a means for transmitting a notification signal to the second proximity means.
18. The system of claim 17 wherein said means for transmitting a notification signal to said second means is responsive to said first proximity means.
19. The system of claim 17 wherein said means for transmitting a notification signal to said second means is responsive to said base.
20. The system of claim 17 wherein said means for transmitting a notification signal to said second means is responsive to said control center.
21. The system of claim 12 wherein said first proximity means includes a means for determining the distance between said mobile base and said second proximity means.

22. A remote monitor operating with a central site and a mobile transceiver to provide supervising and communicating functions, the remote monitor comprising:
a portable power source so that said monitor may be mobile;
a communication section comprising,
means for receiving information concerning the location of said monitor,
means for transmitting information to and receiving information from said central site,
means for transmitting information to and receiving information from said transceiver;
- a processing section comprising,
means for determining the location of said monitor from said information concerning the location of said monitor and for causing said communication section to transmit said location to said central site to allow the central site to supervise said monitor's location,
means for operably transmitting information to and receiving information from said transceiver and therefrom determining the distance between said

10

- monitor and said transceiver in order to supervise the distance between said monitor and said transceiver, means for determining the status of said transceiver from information received from said transceiver in order to permit said transceiver to communicate status reports to said monitor,
means operable with said transceiver for setting a reference distance between said monitor and said transceiver in order to establish a distance of supervision between said monitor and said transceiver, means for establishing whether said transceiver is located within said reference distance and for causing said communication section to transmit said information to said central site so that said monitor may communicate whether said transceiver is within said established distance of supervision with said central site.
23. The monitor of claim 22 further comprising an alarm section operably connected to said processing section, wherein the a first alarm activates responsive to the processor section determining the transceiver is not within said distance of supervision.
24. The monitor of claim 22 wherein the processor section further comprises a selectively enabled means to cause the communications section to send a signal to said transceiver upon determining said transceiver is not within said distance of supervision in order to communicate to said transceiver the distance between said transceiver and said monitor has exceeded said distance of supervision.
25. The monitor of claim 22, wherein the processor section further comprises means for causing the communication section to transmit said transceiver status reports to said central site.
26. The monitor of claim 22, wherein, upon the central site sending a message that it desires to communicate with the transceiver, the processor section further comprises means for determining the nature of said message and for causing the communication section to transmit said nature of said message to said transceiver.

* * * * *

(12) **United States Patent**
Chinoy et al.

(10) Patent No.: US 671969 B1
(45) Date of Patent: MARCH 2006
MURKIN, CHANCERY DIVISION
CLERK DOROTHY BROWN

(54) APPARATUS AND METHOD FOR
TRACKING AND COMMUNICATING WITH
A MOBILE RADIO UNIT

(75) Inventors: **Sharon Chinoy**, Melbourne, FL (US);
Michael LeBlanc, Palm Bay, FL (US)

(73) Assignee: **Harris Corporation**, Melbourne, FL
(US)

(*) Notice: Subject to any disclaimer, the term of this
patent is extended or adjusted under 35
U.S.C. 154(b) by 692 days.

(21) Appl. No.: 09/610,839

(22) Filed: Jul. 6, 2000

(51) Int. Cl.⁷ G08G 1/123; H04Q 7/20

(52) U.S. Cl. 455/456.1; 455/404.2;
455/414.1; 455/457; 340/988; 340/989;
340/990

(58) Field of Search 455/456.1, 428,
455/457, 404.2, 414.1; 340/988, 989, 990;
342/357.1, 557; 701/207

(56) References Cited

U.S. PATENT DOCUMENTS

- | | | | |
|-------------|---------|------------------|-----------------|
| 5,155,689 A | 10/1992 | Wortham | 364/460 |
| 5,243,530 A | 9/1993 | Stanifer et al. | 364/452 |
| 5,428,546 A | 6/1995 | Shah et al. | 364/449 |
| 5,519,760 A | 5/1996 | Borkowski et al. | 379/59 |
| 5,636,122 A | 6/1997 | Shah et al. | 364/449.1 |
| 5,663,720 A | 9/1997 | Weissman | 340/934 |

5,758,288 A	5/1998	Dunn et al.	455/456
5,841,766 A	11/1998	Dent et al.	370/321
5,898,680 A	4/1999	Johnstone et al.	370/316
5,904,727 A	5/1999	Prabhakaran 701/208
5,914,946 A	6/1999	Avidor et al.	370/336
5,922,040 A	*	Prabhakaran 701/117
5,977,913 A	11/1999	Christ 342/465
5,987,011 A	11/1999	Toh 370/331
6,331,825 B1	* 12/2001	Ladner et al.	340/988
6,492,941 B1	* 12/2002	Beason et al.	342/357.1
6,522,265 B1	* 2/2003	Hillman et al.	340/988

* cited by examiner

Primary Examiner—Nay Maung

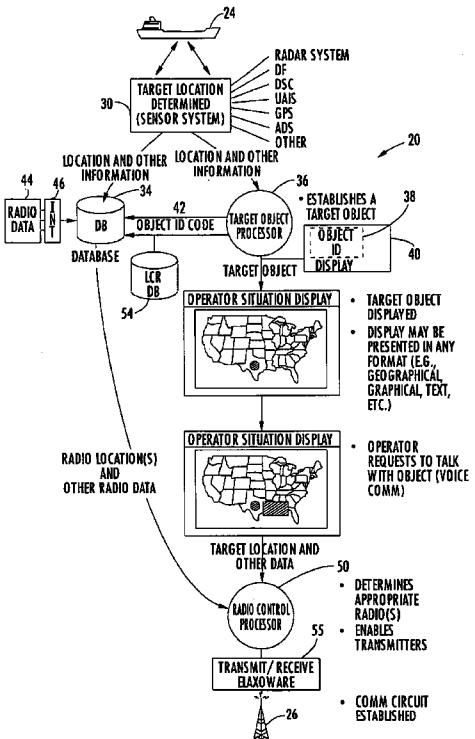
Assistant Examiner—Alan T. Gant

(74) Attorney, Agent, or Firm—Allen, Dyer, Doppelt,
Milbrath & Gilchrist, P.A.

(57) ABSTRACT

An apparatus and method of the present invention establishes a communication link with at least one mobile radio unit as a mobile target by determining the location of the at least one mobile radio unit and displaying on a computer display an object identifier corresponding to the mobile radio unit. A user selects the object identifier and in response to the user selection, establishes one of at least a data or voice communication link with the mobile radio unit. A plurality object identifier corresponding to mobile radio units as different mobile assets are displayed and the object identifier for a displayed mobile radio unit in question is user selected as a mobile target to establish one of at least a data or voice communication link with the mobile radio unit.

45 Claims, 4 Drawing Sheets



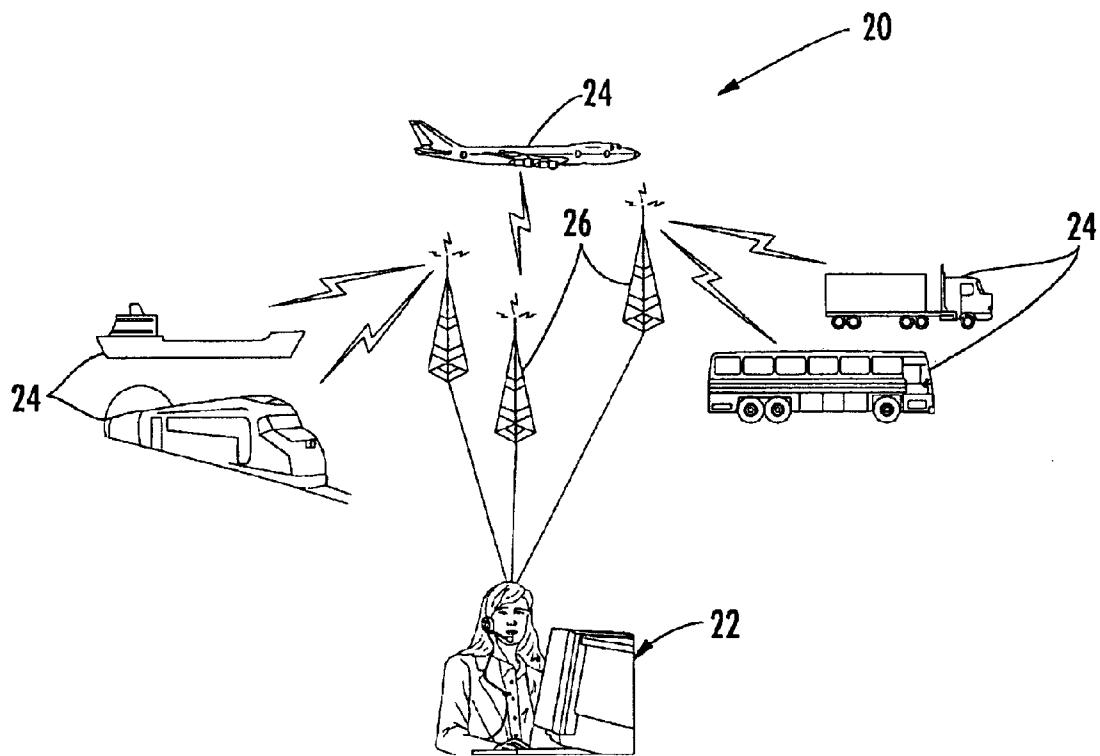
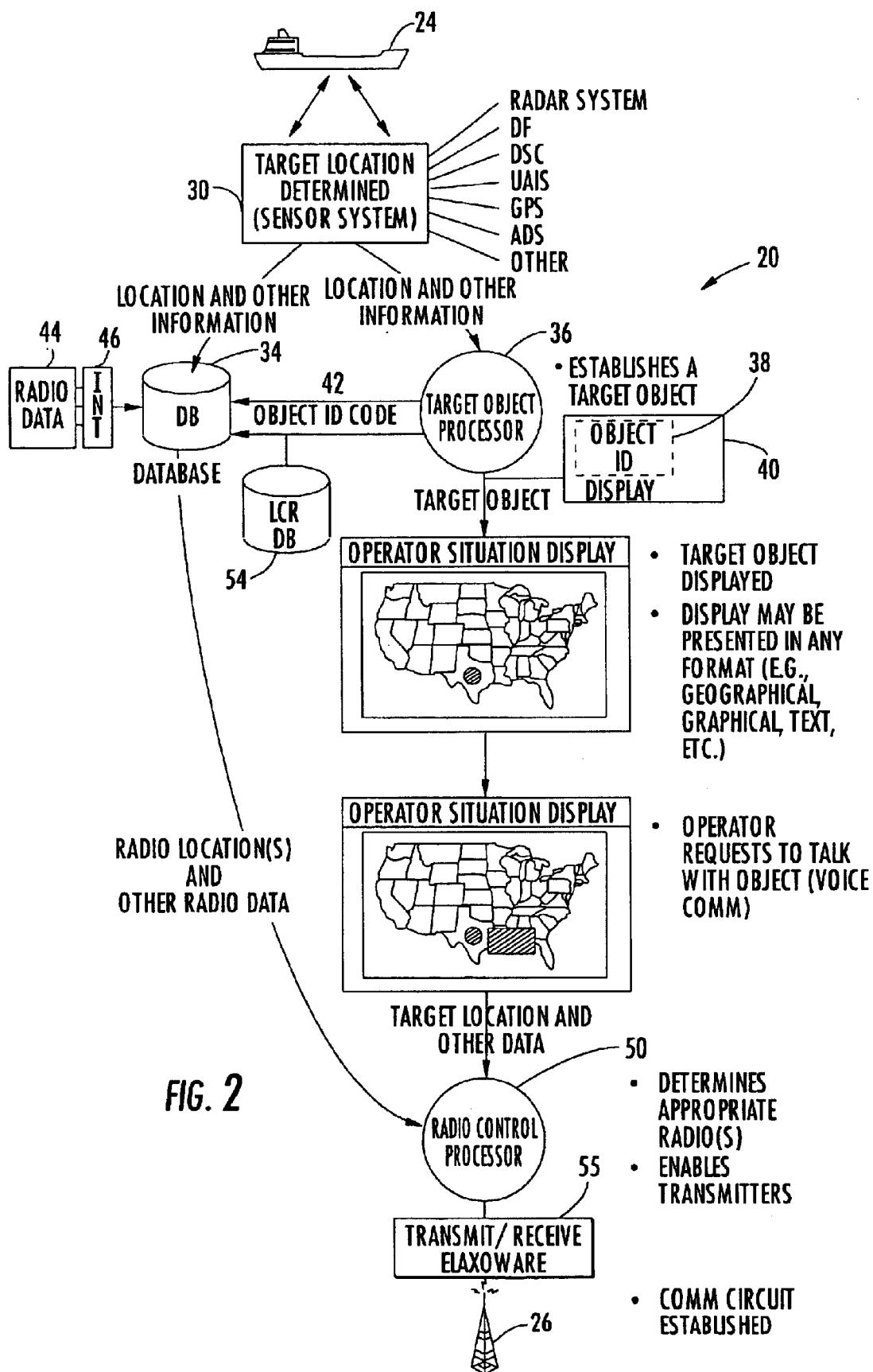


FIG. 1

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 2 of 10



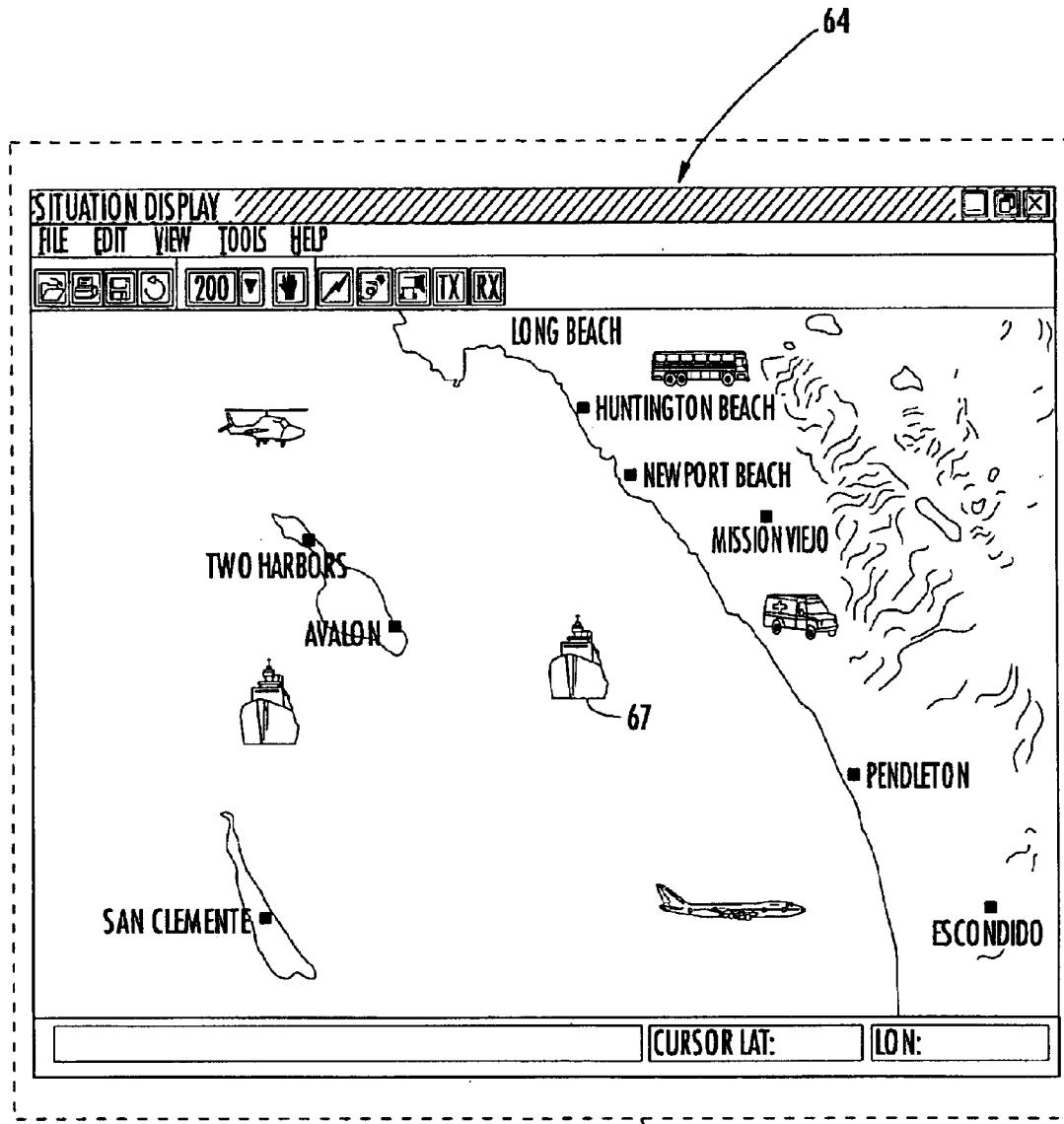


FIG. 3

-62-

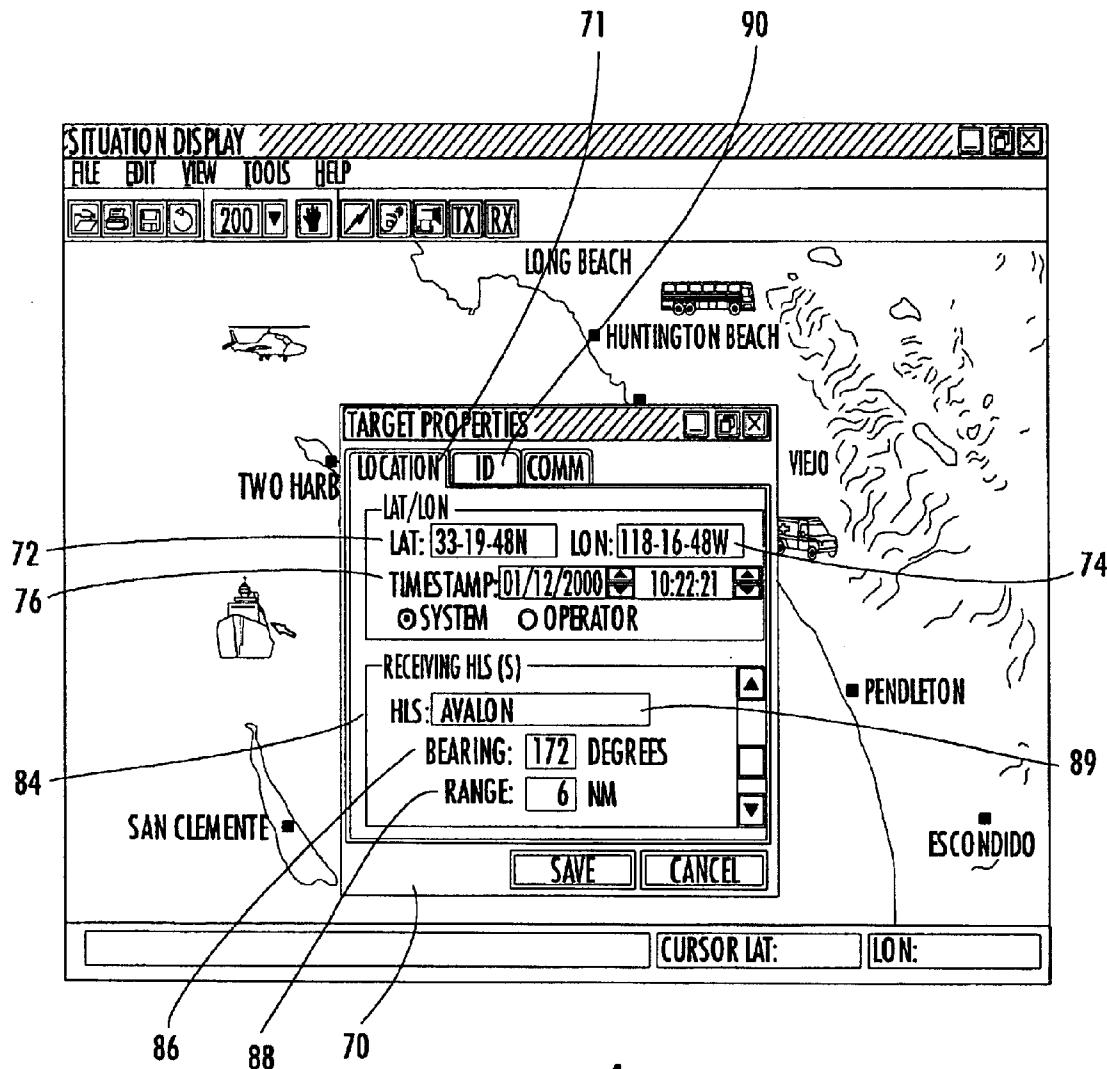


FIG. 4

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 5 of 10

**APPARATUS AND METHOD FOR
TRACKING AND COMMUNICATING WITH
A MOBILE RADIO UNIT**

FIELD OF THE INVENTION

This invention relates to the field of communications and surveillance, and more particularly, this invention relates to the field of communicating with and tracking of a mobile target, such as a mobile radio unit.

BACKGROUND OF THE INVENTION

Current radio frequency radio control systems often require a centralized operator at a control operations center to communicate with a specific mobile target or plurality of mobile targets within a region by selecting a radio's frequency and site button to establish a communications link, i.e., communications channel, with a targeted mobile radio unit representing the mobile target in question. Different examples of mobile targets include an aircraft, ocean going vessel, train, vehicle or other mobile target that contains a mobile radio unit for communication. Thus, a centralized operator working at a control operations center is required to know the location of different radio sites in relation to the mobile target and used in communication links in order to establish voice or data communication with that mobile target. Most of the existing systems in use today do not provide integrated locating and communication, and do not provide increased operator performance and situation awareness.

Historically, control over radio communications was provided by radio control panels that were hard-wired to radios or a switch. These hardware systems evolved prior to the evolution of sophisticated software automation systems. When software solutions were designed for radio communication, they emulated the hardware button approach using software push buttons displayed on a screen forming a graphical user interface. These systems, however, still required the operator to know the frequency and site identifier, i.e., the physical location of a communication linked radio tower when attempting to talk with the mobile target, i.e., mobile radio unit. In addition, separate automation systems displayed location information of the target. For example, in an air traffic control situation, one monitor will be used to display the aircraft location. Another monitor will display information regarding radio control, e.g., the voice switching and control system (VSCS). In a sheriff's or other law enforcement officer's communication center, a typical radio dispatcher position would include a Computer Aided Dispatch (CAD) screen, a status screen, an electronic map, and a radio controller. These elements are not integrated as a whole.

Although there are presently many proposals for emergency 911 procedures where the location of a cellular is determined using GPS or triangulation, there are no integrated solutions for tracking and establishing communication links with one or more mobile targets.

U.S. Pat. Nos. 5,428,546; 5,636,122; and 5,904,727, assigned to Mobile Information Systems, Inc., disclose the use of a monitor that allows the location of a mobile unit to be displayed on the monitor as an icon. Jobs can be assigned to vehicles as part of a database within a computer system and coupled to a vector database. The dispatching system has job icons displayed on a rasterized map. However, there is no integrated solution of both localization information and communication control.

U.S. Pat. No. 5,987,011 to Toh discloses a routing method for supporting ad-hoc mobile communications within a radio communications network, where the stability of various communication links between neighboring mobile hosts are measured. A communications route through the network is selected and based on the stability of the communication links. Thus, the best routing method for a mobile network can be provided.

However, these and other similar proposals do not provide an integrated system having increased operator performance and situation awareness, which also allows the location determination of the mobile radio unit and the tracking of and communication with integrated unit.

SUMMARY OF THE INVENTION

The present invention is advantageous and allows for the establishment of a communication link with a mobile target, i.e., mobile radio unit, by determining first the location of the mobile radio unit, or a plurality of mobile radio units, such as by location determining sensors. The mobile radio unit is displayed on a user interface of a computer display as an object identifier. The user selects the object identifier and in response to the user selection, establishes one of at least a data or voice communication link with the mobile radio unit. Thus, it is possible to track various mobile radio targets, such as emergency vessels, helicopters and ships in distress, aircraft, land-based vehicles, and then establishing communication by the user selecting an icon. The system automatically establishes the appropriate communications link based on pre-established criteria that may include least cost, strongest signal, least path congestion or other. This apparatus and system allow a completely integrated voice and data system.

In accordance with one aspect of the present invention, the apparatus includes a controller for receiving location determining signals from sensors and determining the location of a mobile unit. This determination could be based on the target's location information and mode of radio transmission, and the use of other sensors, as known to those skilled in the art. A computer display is associated with the controller for displaying the mobile radio unit as an object identifier and, in one aspect of the invention, displaying the geographic location. A transceiver is connected to the controller. Upon user selection of the object identifier, at least one of a data or a voice communication link is established with the mobile radio unit.

The object identifier displayed on the computer display can identify the geographic location of the mobile radio unit in latitude and longitude coordinates and altitude, if appropriate. The transceiver can also establish a least cost routing communications link with the mobile radio unit. This information on least cost routing can be contained in a least cost routing database. A database is also associated with the controller for storing data relating to the location or other information of a target containing the mobile radio unit. A unique object identification code is assigned to the mobile radio unit, including the location data stored within the database. This unique object identification code is linked to the displayed object identifier for allowing user selection of the object identifier, while selectively accessing the data stored within the database on the mobile radio unit.

Naturally, the transceiver can be part of the modem of a computer, interface card, or radio unit connected to the processor. A recorder can record any data or voice communications that are established to the mobile radio unit for future reference.

BRIEF DESCRIPTION OF THE DRAWINGS

Other objects, features and advantages of the present invention will become apparent from the detailed description of the invention which follows, when considered in light of the accompanying drawings in which:

FIG. 1 is a general, overall view of the integrated system of the present invention showing communication between an operations control center and mobile targets, i.e., mobile radio units, via wireless radio transmission towers, such that integrated or separate sensors may be used to determine location.

FIG. 2 is a schematic, block and pictorial diagram showing the process flow from the point when a mobile target location is established to the point when the communications link circuit is established with the mobile target.

FIG. 3 is a computer screen representation showing a user interface that displays various mobile radio units as mobile targets and assets on a geographical display.

FIG. 4 shows a computer screen where the icon for a mobile target as a mobile radio unit has been selected and a target properties box has been displayed, indicating location.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention is advantageous, allowing a determination of an appropriate mobile unit location using sensor data about radio location and mode of radio transmission or other means, and provides an integrated voice and data system.

As shown in FIG. 1, the system of the present invention is illustrated generally at 20, and includes an operations control center 22 that communicates with and tracks various mobile assets and targets corresponding to mobile radio units 24, such as transportation vehicles, i.e., the illustrated bus and tractor trailer, the jet aircraft as a commercial airline, or military or emergency management system (EMS) aircraft, a train and ship. Communication is accomplished via the communication links shown as wireless towers 26.

The present invention is especially applicable for use in rescue or surveillance operations, such as with the Coast Guard, police dispatch, air traffic control, fleet management, or other similar organizations, where various mobile radio units can be tracked (e.g., police cars, aircraft rescue ships, and fleet vehicles). Mobile radio units are also referred to as mobile assets when associated with an organization, group base, or administrative center. They are also mobile targets because targets are tracked or their location determined, and communication established with a target in question. A ship, aircraft vehicle, or other mobile target is a mobile radio unit and mobile target that is tracked. Information is updated in a database through appropriate processors that receive information about the particular mobile target, process it, and store it within a database.

As shown in FIG. 2, a sensor system is illustrated generally at block 30 and acquires location data about a mobile target, such as the illustrated mobile radio unit 24. The sensor system could be formed from a plurality of different sensors. These could include a radar system used for location determination, RDE, DSC, UAIS, GPS, ADS or other systems as known to those skilled in the art.

The location data and other information known about the mobile target or mobile radio unit is forwarded to a database 34 and a computer processor 36, also referred to as a target object processor, which establishes through appropriate software a target object for display on a computer screen, i.e., an

object identifier 38 that is displayed on a computer screen of a display 40 associated with the computer processor. The processor has software that assigns a unique object identification code 42 to the mobile radio unit. The processor uses the code 42 for accessing from the database 34 any data about the mobile radio unit that is the selected mobile target, including any location data, identification data, and other data stored within the database about the mobile target. The object identifier 38 is in one aspect of the present invention displayed as a user selectable icon on a graphical user interface as explained below. It could also be user selectable text or other user selectable means.

Radio data 44 is also received in the database through an appropriate radio interface 46 that could include other location data, such as identifying data on the type of mobile target or mobile radio unit that would aid in rescue, determining capacity or work characteristics, or other information. After accessing the database, the processor 36 controls the computer display 40 to place on screen an operator situation display where the object identifier 38 is displayed on screen in almost any desired screen format, such as geographical, graphical, text or other display types known to those skilled in the art. Although a geographical display is shown, it should be understood that the exact geographical location of the mobile radio unit, i.e., the mobile target or other mobile asset, does not have to be known by the operator. The system has determined automatically the mobile target location and operates accordingly.

A user selects the object identifier 38, such by clicking a mouse button, and in response to the object identifier selection, establishes one of at least a data or voice communication link with the mobile radio unit. A radio control processor 50, which could be separate from, associated with, or the same as the target object processor 36, determines what radios or other communication transmitters are activated with transmit/receive hardware 55 to enable transmission and establish a communication link, i.e., circuit, with the targeted mobile radio unit. This step could include accessing a least cost routing database 54 to determine the least cost route to a mobile target in terms of data integrity or actual monetary value. For example, different communications networks could be used or a determination made that part of the communication link may include a land line connection and part can include a wireless network as part of the connection.

Both voice switching and air-ground communication could be used as explained. The system as disclosed allows for a VHF voice communication system (e.g., as used by the Coast Guard, 911 communication center, or air traffic controller) and permits centralized operators at an operations control center to locate a vessel and communicate with it, or communicate with any vessels within a desired region in an integrated fashion.

FIG. 3 illustrates an example of the type of graphical user interface 64 that can be displayed on a computer screen at a workstation terminal 62 or other location station. The interface is a general Windows™ format. Various mobile radio units corresponding to mobile assets are illustrated as a helicopter icon, and ship icon. Various cities are displayed on the geographic display and correspond to different facilities that have administrative centers for monitoring and/or controlling mobile assets, such as helicopters, ships, etc. A mobile target location to be determined is shown by the location of the target icon 67.

FIG. 4 illustrates a computer screen similar to that shown in FIG. 3, where a mobile target is located by sensors, such

as radar or RDF. The data is stored in the database and processed for display as an object identifier. The user clicks on the mobile target 67 and a target properties box 70 is displayed, which shows the latitude, longitude, time, and any other relevant information that is maintained in the database and is desired to be displayed. The system 20 of the present invention works with the controllers 36,50 and sensor system 30 to maintain tracking of the mobile target and other mobile radio units, which can be displayed as icons that periodically change position on the screen corresponding to movement. As shown on the target properties user box 70, the location data area 71 can include the respective latitude and longitude data entry lines 72,74, a time stamp 76, the receiving station data area 84, including information such as its bearing 86 and range 88, and the name area 89 of the unit. Other information could include an ID tab 90 that can be depressed to show the identification information of the target. This information can be modified as necessary and then stored in the database 34. For example, if greater information is found about the mobile target, this information can be stored and later used. It is possible to establish communication by dialing a telephone number automatically when a user clicks an icon.

Many modifications and other embodiments of the invention will come to the mind of one skilled in the art having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is to be understood that the invention is not to be limited to the specific embodiments disclosed, and that the modifications and embodiments are intended to be included within the scope of the dependent claims.

What is claimed is:

1. A method of establishing a communication link with a mobile radio unit comprising the steps of:

determining the location of at least one mobile radio unit;
selecting a desired screen format for a computer display as either a geographical, graphical or text display;
displaying on the computer display an object identifier indicative of the mobile radio unit as either the geographical, graphical or text display as selected by the user; and

user selecting the object identifier and in response to the user selection, establishing one of at least a data or voice least cost route communication link with the mobile radio unit.

2. A method according to claim 1, and further comprising the step of storing least cost routing data within a least cost routing database and accessing the database for determining a least cost route of the communication link.

3. A method according to claim 1, and further comprising the step of storing data relating to the location of the mobile radio unit within a database while also updating periodically within the database any changes reflective of a change in location of the mobile radio unit.

4. A method according to claim 1, and further comprising the step of assigning a unique identification code to the mobile radio unit for accessing from the database any data about the mobile radio unit, including location data of the mobile radio unit.

5. A method according to claim 1, and further comprising the step of displaying the geographic location of the mobile radio unit on the computer display in longitude and latitude coordinates.

6. A method of establishing a communication link with at least one mobile radio unit comprising the steps of:

determining the location of a mobile radio unit;

storing data relating to the location of the mobile radio unit within a database while also updating periodically within the database any changes to the data reflective of a change in location of the mobile radio unit;

assigning a unique object identification code to the mobile radio unit for accessing from the database any data about the mobile radio unit, including the location data stored within the database;

displaying on a computer display an object identifier corresponding to the mobile radio unit, wherein the object identifier is linked to the unique object identification code for accessing from the database the stored data about the mobile radio unit and location data of the mobile radio unit;

user selecting an object identifier and displaying a target properties box having a display of stored data from the database that identifies specific data about the mobile radio unit as retrieved from the database to aid in determining specific applications for the mobile radio unit as a mobile asset; and

selecting the object identifier through the user interface and in response to the object identifier selection, establishing one of at least a data or voice communication link with the mobile radio unit.

7. A method according to claim 6, and further comprising the step of displaying the object identifier as a user selectable icon on a graphical user interface.

8. A method according to claim 6, and further comprising the step of displaying the object identifier as user selectable text on a user interface.

9. A method according to claim 6, wherein the data about the mobile radio unit stored within the database further comprises information relating to communication parameters of the communication link that can be established with the mobile radio unit.

10. A method according to claim 6, and further comprising the step of displaying the geographic location of the mobile radio unit as an object identifier on the computer display in longitude and latitude coordinates.

11. A method according to claim 6, wherein the step of determining the location of the mobile radio unit further comprises the step of receiving a distress signal from the mobile radio unit.

12. A method according to claim 6, wherein the object identifier further comprises a geographic region displayed on a geographic display.

13. A method according to claim 6, and further comprising the step of dialing a telephone number to establish a communication link.

14. A method according to claim 6, and further comprising the step of recording any data or voice communications that are established to the mobile radio unit.

15. A method according to claim 6, and further comprising the step of determining the location of the mobile radio unit by the use of direction finding sensors.

16. A method of establishing a communication link with a mobile radio unit comprising the steps of:

determining the location of the mobile radio unit within a mobile network by the use of direction finding sensors;
storing data relating to the location of the mobile radio unit within a database while also updating periodically within the database any changes to the data reflective of a change in location of the mobile radio unit;

storing least cost routing data in a database for establishing a least cost networked communication link with the mobile radio unit from a controller;

assigning a unique object identification code to the mobile radio unit for accessing from the database the data about the mobile radio unit, including the location data stored within the database;

displaying on a computer display an object identifier corresponding to the mobile radio unit, wherein said object identifier is linked to the unique object identification code for accessing from the database the stored data about the mobile radio unit and location data of the mobile radio unit;

user selecting the object identifier through the user interface and in response to the object identifier selection, determining a least cost communication route to the mobile radio unit; and

establishing one of at least a data or voice networked communication link with the mobile radio unit based on the least cost communication route determination.

17. A method according to claim 16, wherein said least cost communication route is determined by accessing the least cost routing database containing costs of communication routes between the user selected mobile radio unit and controller, and calculating a least cost route.

18. A method according to claim 17, and wherein the step of establishing one of at least a data or voice networked communication link comprises the step of merging a plurality of controller to target communication routes into a least cost communication route.

19. A method according to claim 16, and further comprising the step of updating the least cost routing database at predetermined time intervals.

20. A method according to claim 6, and further comprising the step of displaying the object identifier as a user selectable icon on a graphical user interface.

21. A method according to claim 16, and further comprising the step of displaying the object identifier as user selectable text on a user interface.

22. A method according to claim 16, and further comprising the step of displaying the geographic location of the mobile radio unit as an object identifier on the computer display in latitude and longitude coordinates.

23. A method according to claim 16, wherein the data about the mobile radio unit stored within the database further comprises information relating to communication parameters of the communication link that can be established with the mobile radio unit.

24. A method according to claim 16, wherein the step of determining the location of the mobile radio unit further comprises the step of receiving a distress signal from the mobile radio unit.

25. A method according to claim 16, wherein the object identifier further comprises a geographic region displayed on a geographic display.

26. A method according to claim 16, and further comprising the step of dialing a telephone number to establish a communication link.

27. A method according to claim 16, and further comprising the step of recording any data or voice communications that are established to the mobile radio unit.

28. A method according to claim 16, and further comprising the step of determining the location of the mobile radio unit by the use of direction finding sensors.

29. An apparatus for establishing a communication link with a mobile radio unit comprising:

a controller for receiving location determining signals and determining the location of a mobile radio unit;

a computer display associated with the controller for displaying an object identifier indicative of the mobile

radio unit, wherein said controller is operative for displaying a desired screen format of either a geographical, graphical or text display based on a user selection of the desired display; and

a transceiver connected to the controller, wherein upon user selection of the object identifier, at least one of a data or a voice least cost route communication link is established with the mobile radio unit.

30. An apparatus according to claim 29, wherein said object identifier displayed on said computer display identifies the geographic location of the mobile radio unit in latitude and longitude coordinates.

31. An apparatus according to claim 29, and further comprising a least cost routing database for storing least cost routing data.

32. An apparatus according to claim 29, and further comprising a database associated with said controller for storing data relating to the location of the mobile radio unit, and a unique object identification code assigned to the mobile radio unit, including the location data stored within the database.

33. An apparatus according to claim 32, wherein said unique object identification code is linked to said object identifier for allowing user selection of the object identifier and selectively accessing the data stored within the database about the mobile radio unit.

34. An apparatus for tracking and communicating with a mobile radio unit comprising:

a controller for receiving location determining signals and determining the location of a mobile radio unit;

a database connected to the controller for storing data relating to the mobile radio unit, including the location of the mobile radio unit, said controller assigning a unique object identification code to the mobile radio unit for accessing by the controller the database and retrieving any stored data about the mobile radio unit;

a computer display associated with the controller for displaying an object identifier corresponding to the mobile radio unit, wherein said object identifier is linked to the unique object identification code, wherein said object identifier can be user selected to display stored data in a target properties box that identifies specific data about the mobile radio unit as retrieved from the database to aid in determining specific applications for the mobile radio unit as a mobile asset; and a transceiver connected to the controller, wherein upon user selection of the object identifier, at least one of a data or a voice communication link is established with the mobile radio unit.

35. An apparatus according to claim 34, wherein said object identifier is displayed as a user selectable icon on a graphical user interface.

36. An apparatus according to claim 34, wherein said object identifier is displayed as user selectable text.

37. An apparatus according to claim 34, wherein the data about the mobile radio unit stored within the database further comprises information relating to communication parameters of the communications link that can be established with the mobile radio unit.

38. An apparatus according to claim 34, wherein said object identifier further comprises a geographic region displayed on said computer display.

39. An apparatus according to claim 34, and further comprising a recorder for recording any data or voice communications that are established to the mobile radio unit.

9

40. An apparatus for tracking and communicating with a mobile radio unit comprising:

- a controller for receiving location determining signals and determining the location of a mobile radio unit;
- a database connected to the controller for storing data relating to the mobile radio unit, including the location of the mobile radio unit, said controller assigning a unique object identification code to the mobile radio unit for accessing by the controller the database and retrieving any stored data about the mobile radio unit;
- a least cost routing database connected to the controller for storing least cost routing data for establishing a least cost networked communication link with the mobile radio unit;
- a computer display associated with the controller for displaying an object identifier corresponding to the mobile radio unit, wherein said object identifier is linked to the unique object identification code; and
- a transceiver connected to the controller, wherein upon user selection of the object identifier, at least one of a

20

10

data or a voice communication link is established with the mobile radio unit.

41. An apparatus according to claim **40**, wherein said object identifier is displayed as a user selectable icon on a graphical user interface.

42. An apparatus according to claim **40**, wherein said object identifier is displayed as user selectable text.

43. An apparatus according to claim **40**, wherein the data about the mobile radio unit stored within the database further comprises information relating to communication parameters of the communications link that can be established with the mobile radio unit.

44. An apparatus according to claim **40**, wherein said object identifier further comprises a geographic region displayed on said computer display.

45. An apparatus according to claim **40**, and further comprising a recorder for recording any data or voice communications that are established to the mobile radio unit.

* * * * *

(12) **United States Patent**
Billhartz et al.

(54) **WIRELESS COMMUNICATIONS SYSTEM
INCLUDING A WIRELESS DEVICE
LOCATOR AND RELATED METHODS**

(75) Inventors: **Thomas Jay Billhartz**, Melbourne, FL (US); **Vivek Krishna**, Palm Bay, FL (US); **Steve Kopman**, Melbourne, FL (US)

(73) Assignee: **Harris Corporation**, Mebourne, FL (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 295 days.

(21) Appl. No.: **10/767,794**

(22) Filed: **Jan. 29, 2004**

(65) **Prior Publication Data**

US 2005/0170843 A1 Aug. 4, 2005

(51) **Int. Cl.**
H04B 1/04 (2006.01)

(52) **U.S. Cl.** **455/456.2; 455/456.1;**
455/456.5; 455/456.6; 342/457; 370/328

(58) **Field of Classification Search** **455/422.1,**
455/41.2, 456.1-457, 67.13, 63.4, 67.16,
455/550.1, 562.1, 575.7; 370/328, 352;
342/457-458

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,526,357 A	6/1996	Jandrell	370/95.2
5,550,549 A	8/1996	Procter, Jr. et al.	342/47
5,687,196 A	11/1997	Proctor, Jr. et al.	375/347
5,706,010 A	1/1998	Franke	342/47
6,292,665 B1	9/2001	Hildebrand et al.	455/456
6,680,923 B1 *	1/2004	Leon	370/328
6,865,394 B1 *	3/2005	Ogino et al.	455/456.1
2002/0080759 A1	6/2002	Harrington et al.	370/338
2002/0118655 A1	8/2002	Harrington et al.	370/328

2002/0171586 A1 *	11/2002	Martorana et al.	342/458
2003/0025602 A1	2/2003	Medema et al.	340/568.1
2003/0034887 A1	2/2003	Crabtree et al.	340/539
2003/0043073 A1	3/2003	Gray et al.	342/465
2003/0162550 A1 *	8/2003	Kuwahara et al.	455/456
2003/0182052 A1 *	9/2003	DeLorme et al.	701/201
2003/0191604 A1 *	10/2003	Kuwahara et al.	702/150
2004/0081139 A1 *	4/2004	Beckmann et al.	370/352
2004/0110514 A1 *	6/2004	Kim et al.	455/456.1
2004/0203889 A1 *	10/2004	Karaoguz	455/456.1
2004/0266348 A1 *	12/2004	Deshpande et al.	455/41.2

(Continued)

OTHER PUBLICATIONS

Yellowjacket-A, 802.11a Wi-Fi Analysis System, Berkeley Varitronics Systems.

Primary Examiner—Joseph Feild

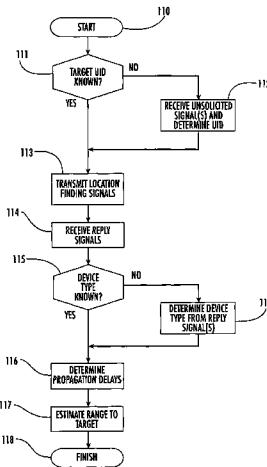
Assistant Examiner—Kamran Afshar

(74) Attorney, Agent, or Firm—Allen, Dyer, Doppelt, Milbrath & Gilchrist, P.A.

(57) **ABSTRACT**

A wireless communications system may include a plurality of wireless communications devices and a wireless device locator. More particularly, the wireless device locator may include at least one antenna and a transceiver connected thereto, and a controller for cooperating with the transceiver for transmitting a plurality of location finding signals to a target wireless communications device from among the plurality thereof. The target device may transmit a respective reply signal for each of the location finding signals. Additionally, the controller may also cooperate with the transceiver for receiving the reply signals, and it may determine a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon a known device latency of the target device. As such, the controller may estimate a range to the target device based upon a plurality of determined propagation delays.

34 Claims, 9 Drawing Sheets



US 7,110,779 B2

Page 2

U.S. PATENT DOCUMENTS

2005/0037775 A1 * 2/2005 Moeglein et al. 455/456.1

2005/0059411 A1 * 3/2005 Zhengdi 455/456.1

* cited by examiner

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 2 of 18

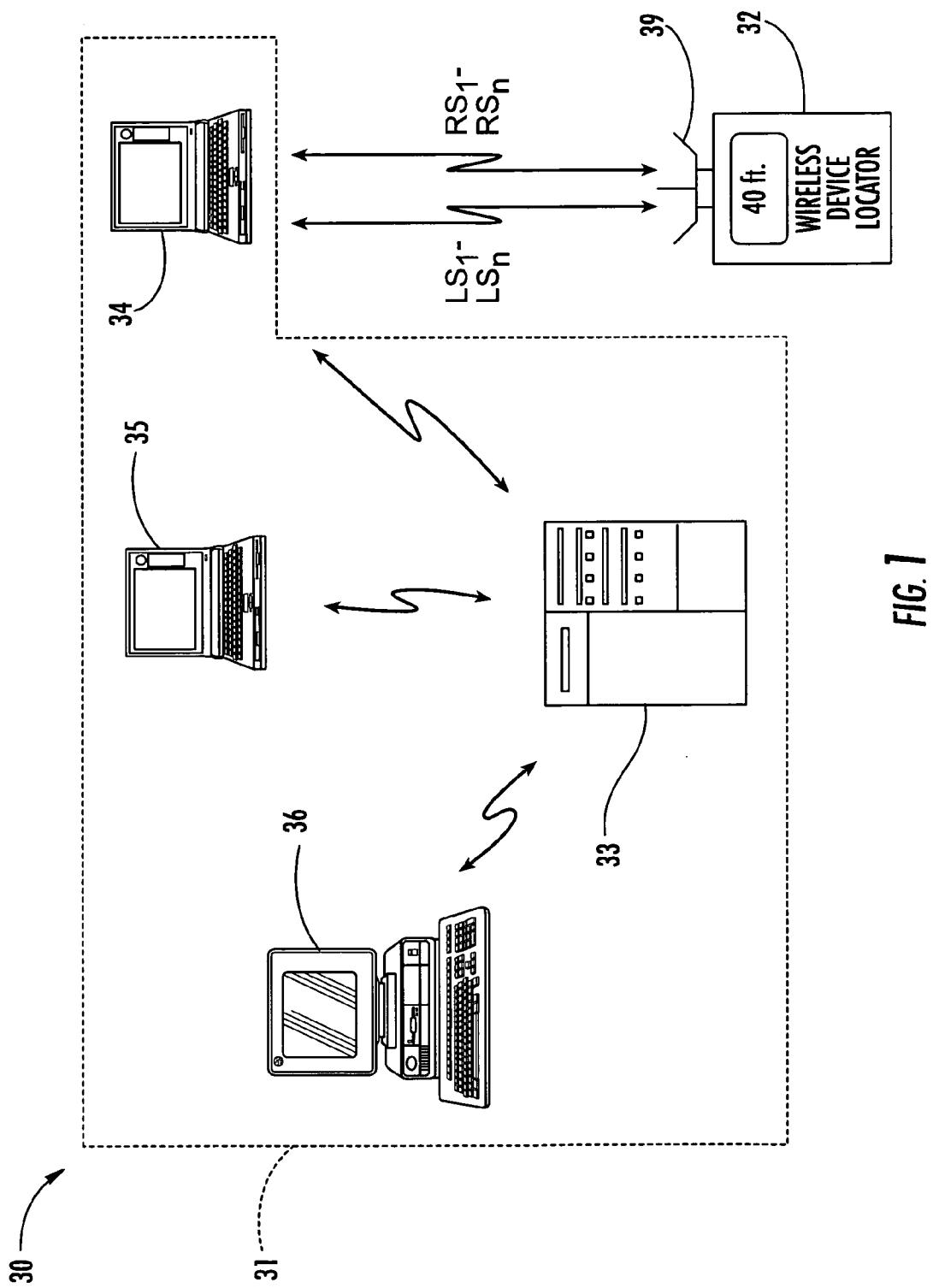


FIG. 1

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 3 of 18

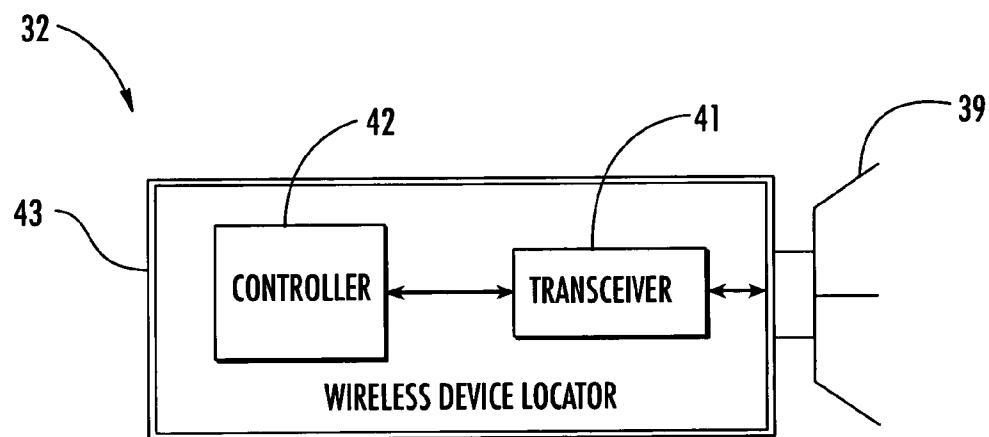


FIG. 2

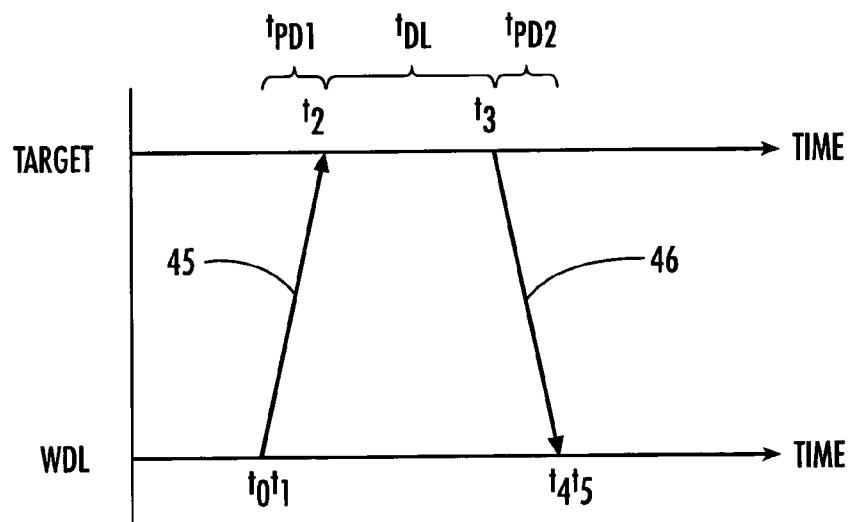


FIG. 3

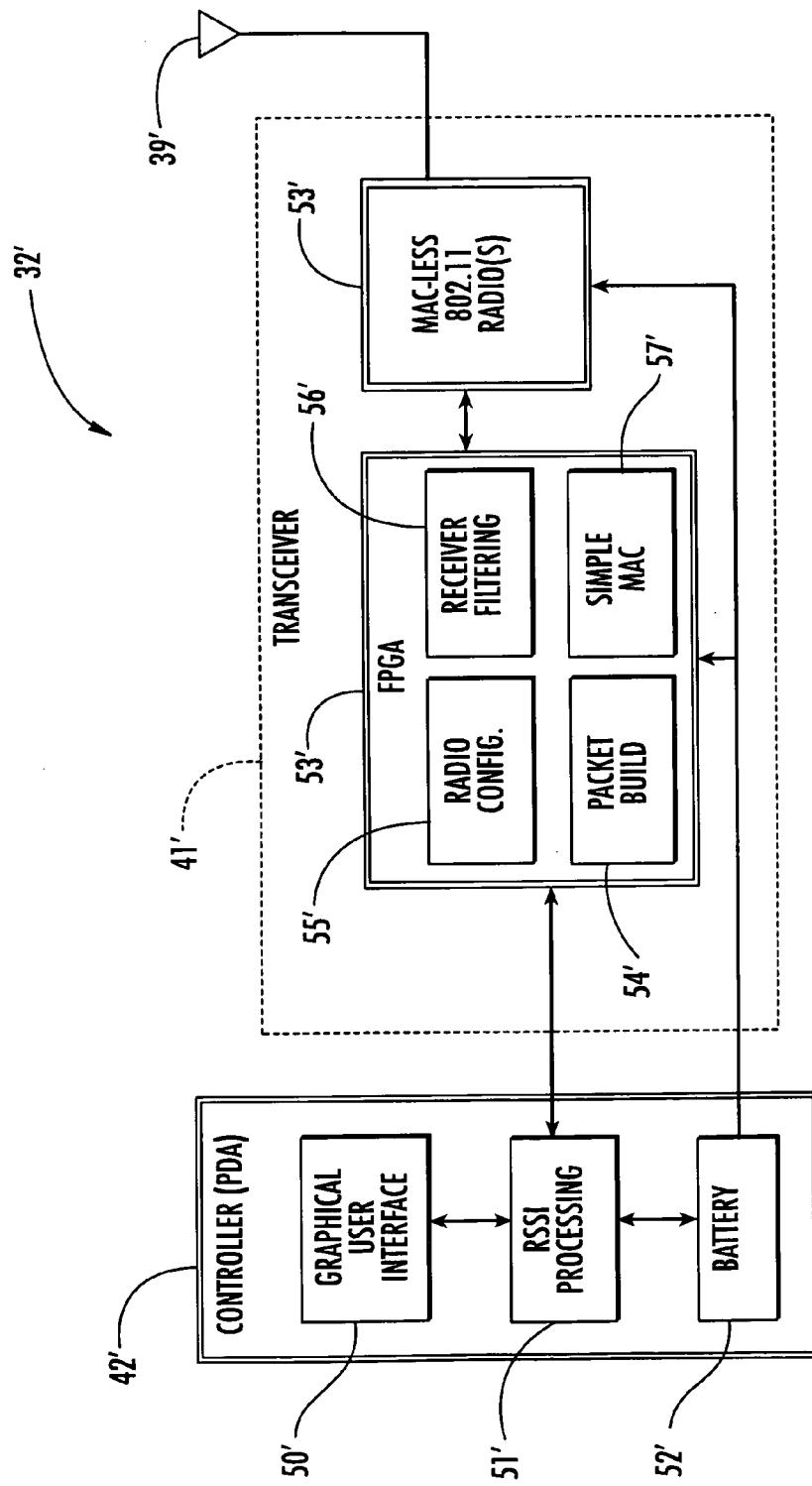


FIG. 4

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 5 of 18

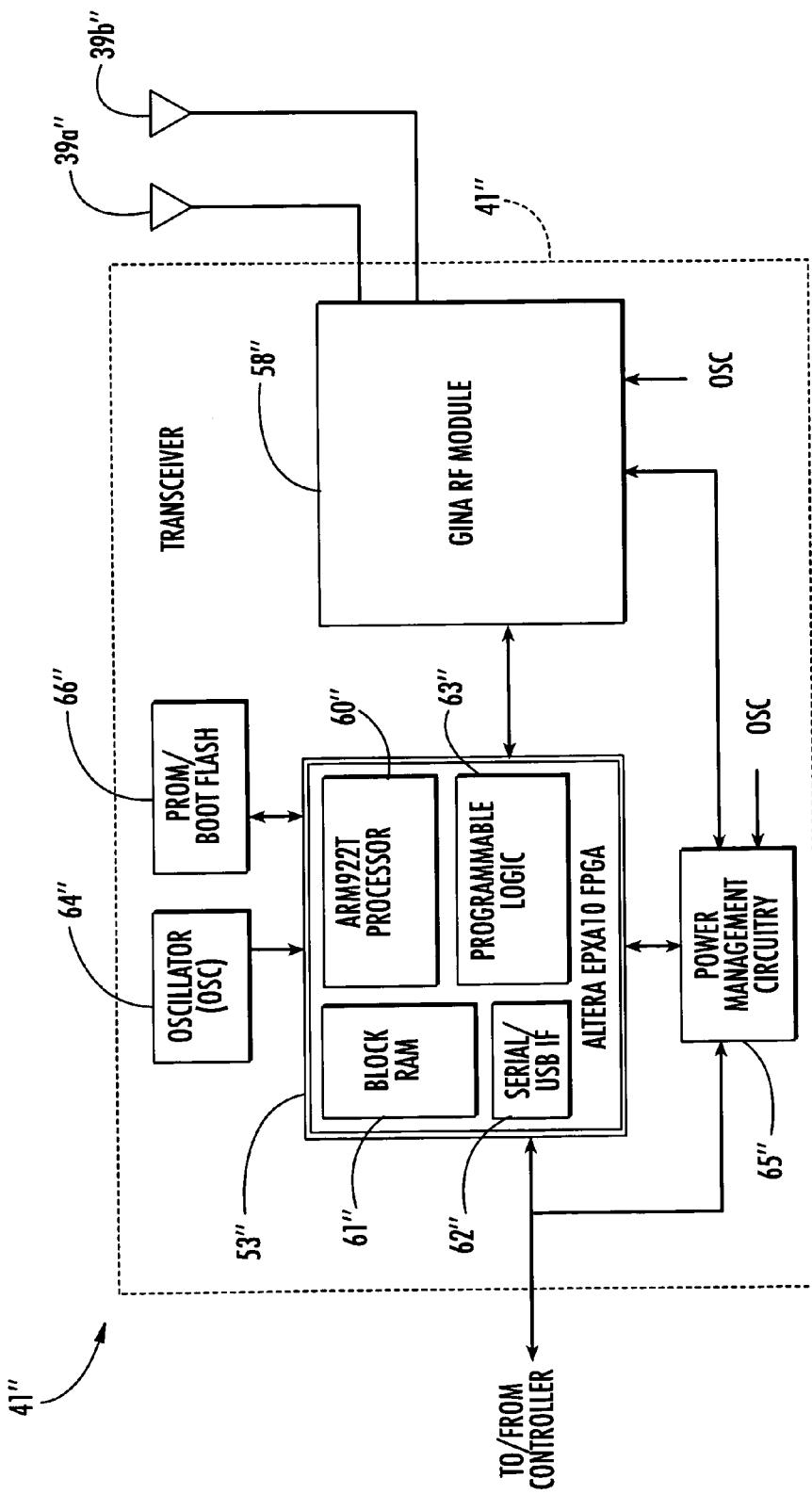


FIG. 5

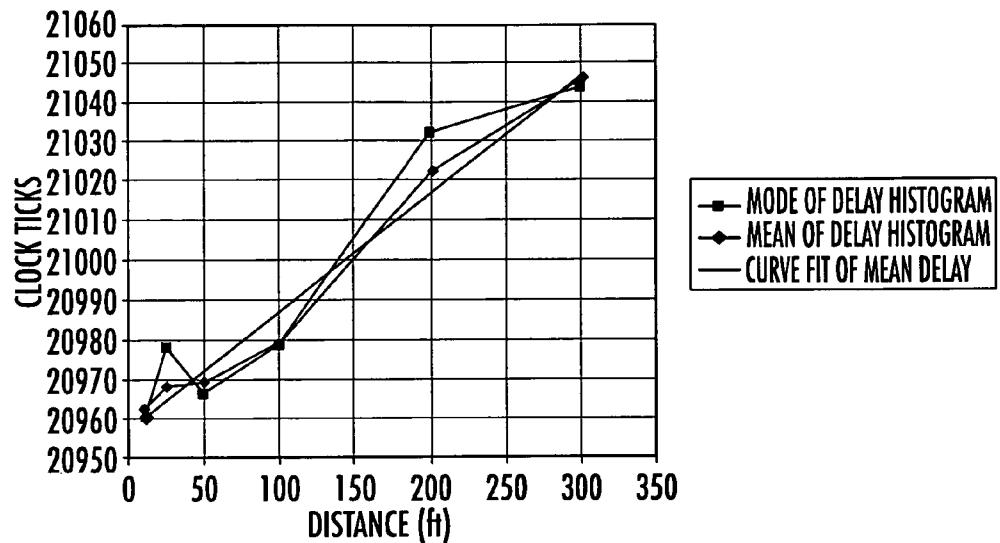


FIG. 6

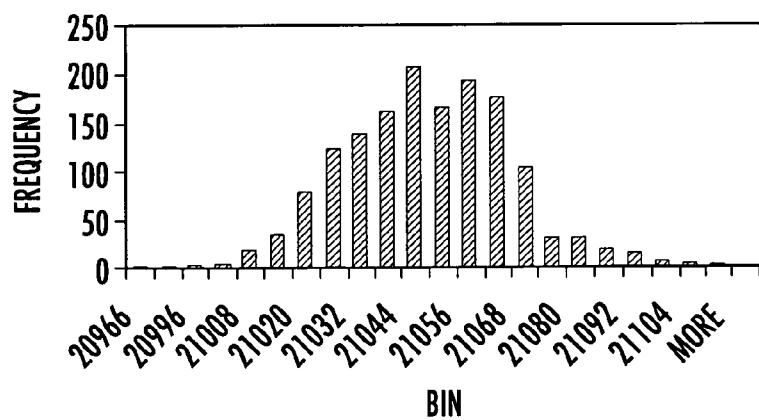
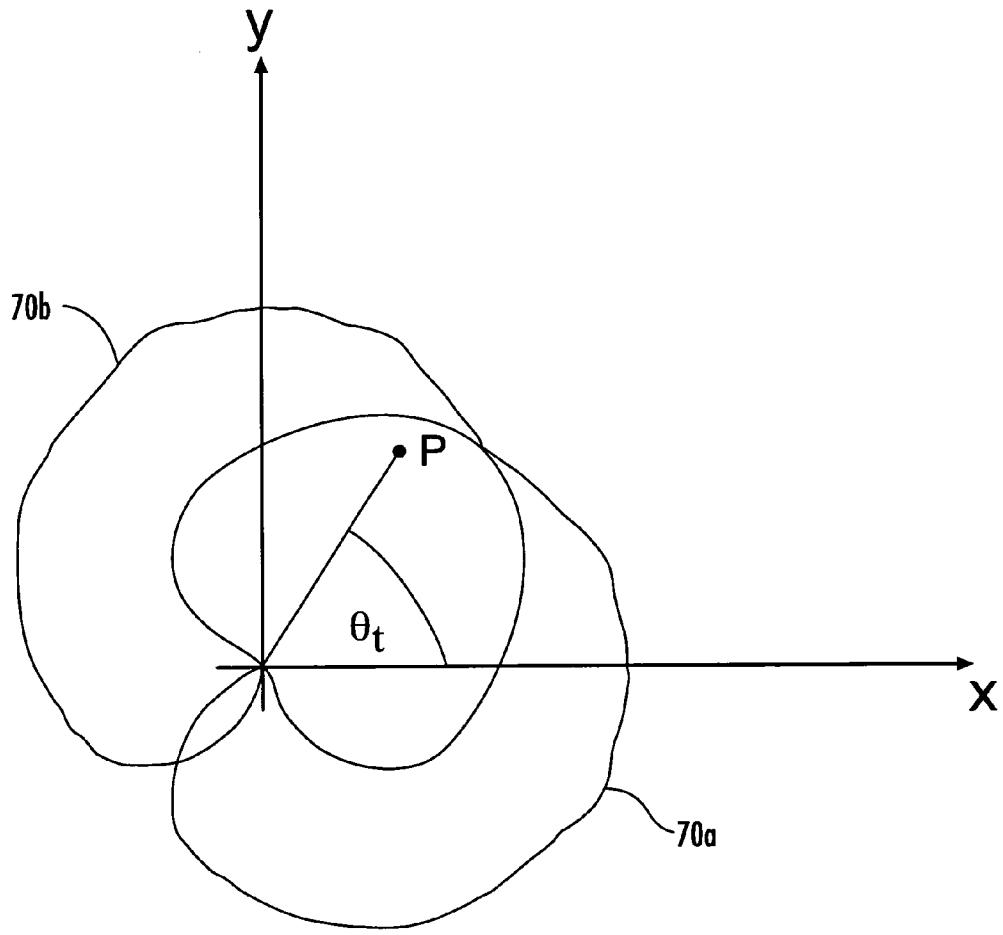


FIG. 7

**FIG. 8**

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 8 of 18

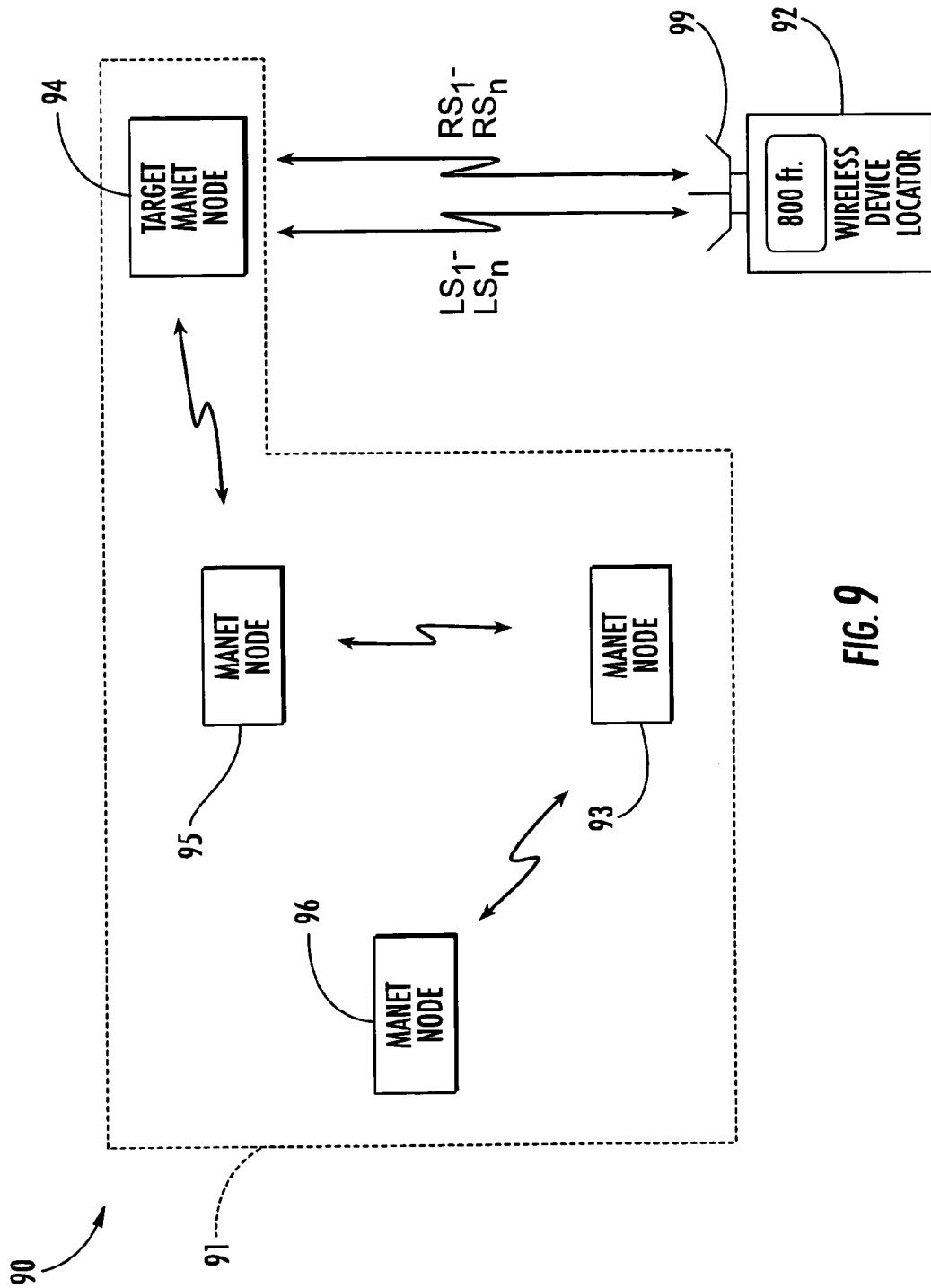


FIG. 9

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 9 of 18

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 10 of 18

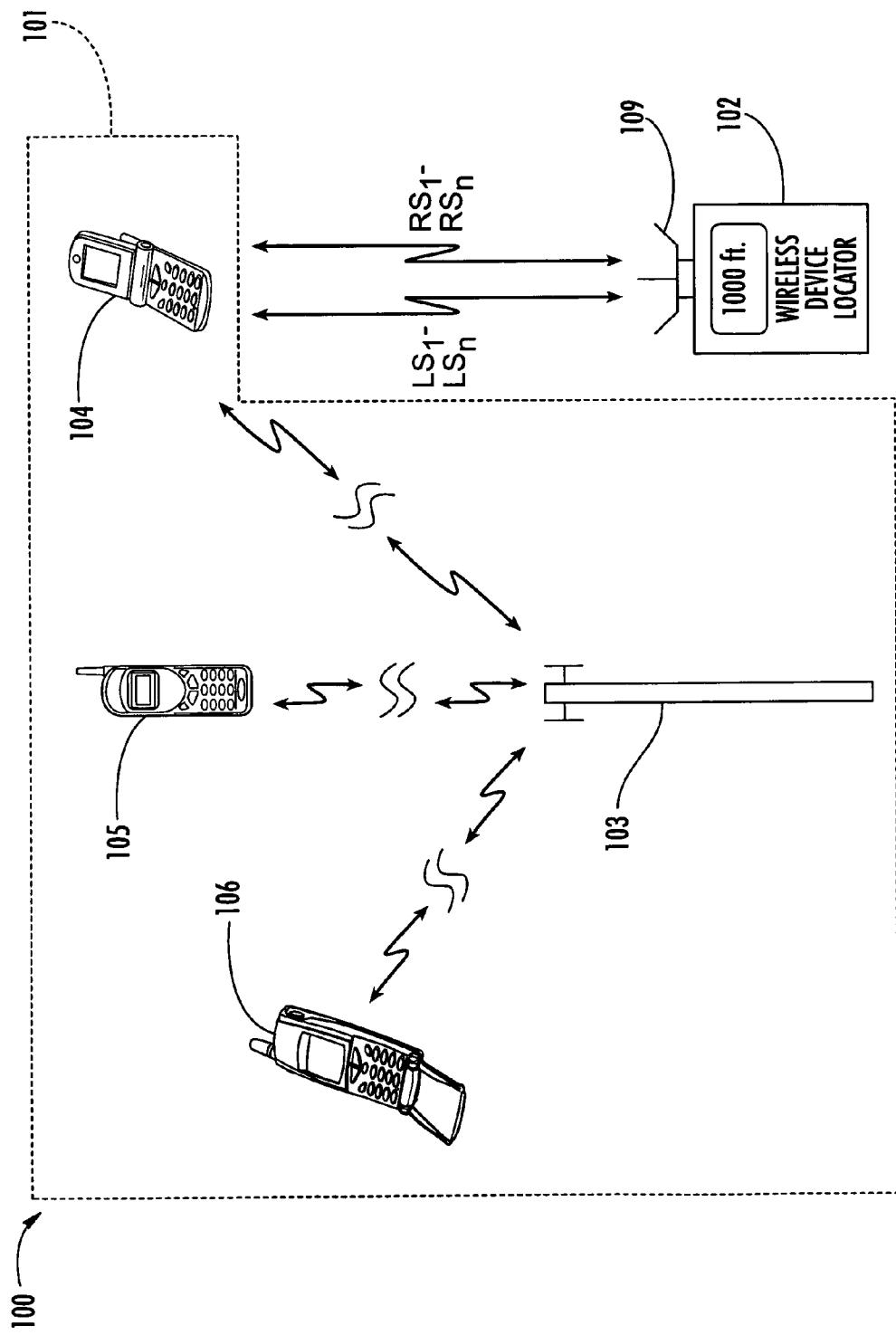


FIG. 10

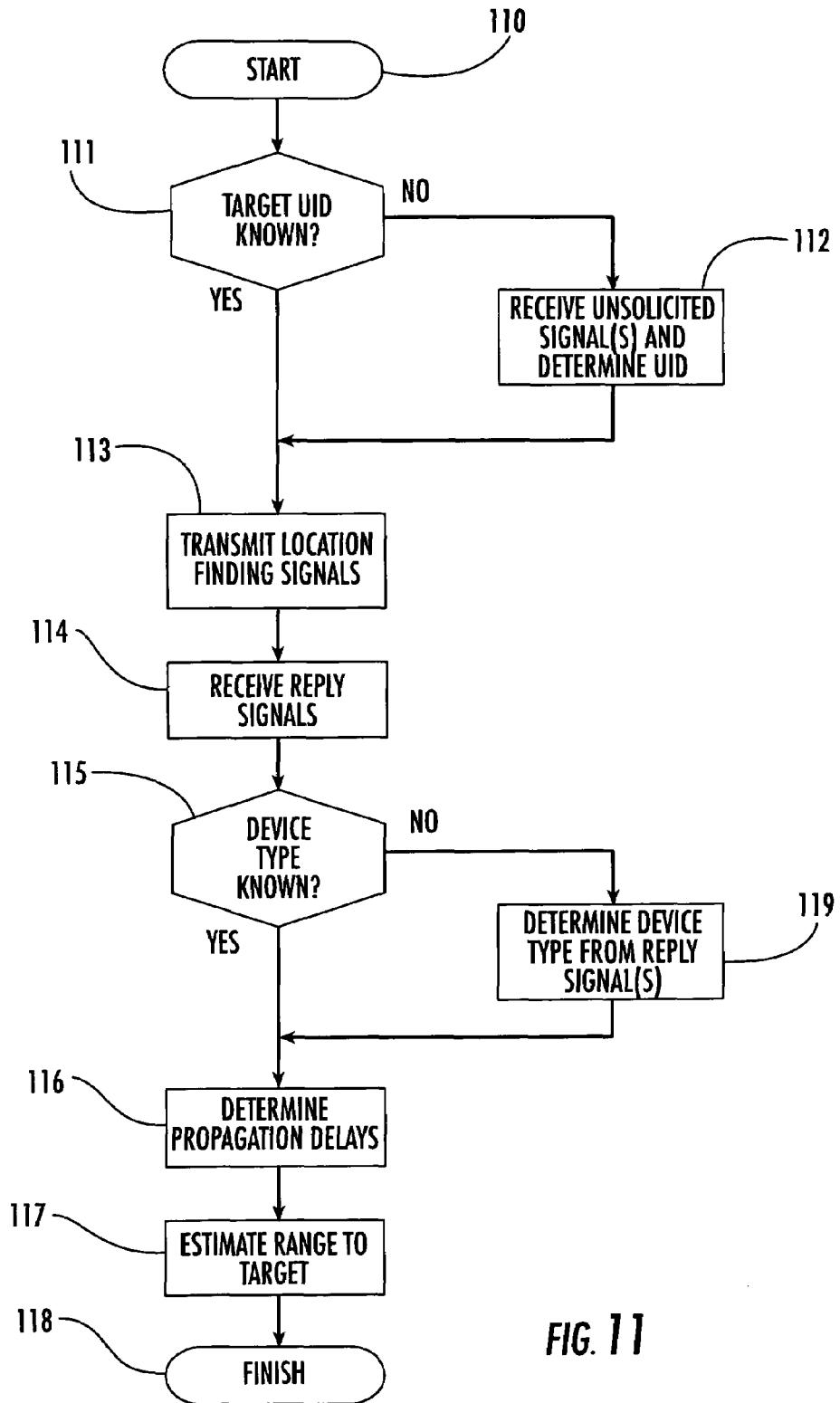


FIG. 11

**WIRELESS COMMUNICATIONS SYSTEM
INCLUDING A WIRELESS DEVICE
LOCATOR AND RELATED METHODS**

FIELD OF THE INVENTION

The present invention relates to the field of wireless communications systems, and, more particularly, to wireless location devices and related methods.

BACKGROUND OF THE INVENTION

Wireless location techniques are used in numerous applications. Perhaps the most basic of these applications is for locating lost articles. By way of example, published U.S. patent application No. 2003/0034887 to Crabtree et al. discloses a portable article locator system for locating lost articles such as glasses, keys, pets, television remotes, etc. More particularly, a wireless transceiver is attached to a person, animal, or other object. A handheld locator transmits a locator signal to the wireless transceiver which includes a unique address code of the transceiver. If the received code matches that stored by the wireless transceiver, it sends a return signal back to the locator device. The locator device uses the return signal to determine the distance and/or direction to the wireless transceiver from the user's location.

The locator device includes an antenna array which includes a plurality of omni-directional antennas. The locator unit determines the bearing to the wireless transceiver by switching between antennas in the antenna array and using Doppler processing to determine a direction of a wireless signal received from the transceiver. The distance to the wireless transmitter is also determined based upon the reception of the wireless signal at each of the antennas of the antenna array. Furthermore, in one embodiment, which is intended to avoid interference between two or more locators in a common area, a plurality of locator signals may be sent from a locator at a standard repetition rate. The locator's receiver then only listens for responses during predetermined windows following each transmission.

In contrast, in some applications it is desirable to determine the location of an unknown signal transmitter. U.S. Pat. No. 5,706,010 to Franke discloses such a system in which a transmitter locator receives a signal from the unknown signal transmitter and processes the signal to determine a bearing to the unknown signal transmitter. The transmitter locator then sends an interrogating signal to the unknown signal transmitter. Upon receiving the interrogating signal, the unknown signal transmitter heterodynes the interrogation signal with its own carrier signal to generate an intermodulation return signal. A processor of the transmitter locator measures the round-trip transit time from the transmission of the interrogation signal to the reception of the intermodulation return signal. A range to the unknown signal transmitter is then calculated based upon the round-trip transit time.

Still another application in which locating a wireless communications device is often necessary is in cellular telephone networks. That is, it may be necessary to locate particular cellular telephone users for law enforcement or emergency purposes, for example. U.S. Pat. No. 6,292,665 to Hildebrand et al., which is assigned to the present assignee, discloses a method for geolocating a cellular phone initiating a 911 call. A base station transceiver transmits a supervisory audio tone (SAT), which is automatically looped back by the calling cellular phone. Returned SAT signals are correlated with those transmitted to determine the

range of the cellular phone. In addition, incoming signals from the cellular phone, such as the returned SAT signals, are received by a phased array antenna and subjected to angle of arrival processing to determine the direction of the cellular phone relative to the base station. The cellular phone is geolocated based upon the angle of arrival and the range information. A correction factor provided by the manufacturer of a given cellular telephone is used to account for the loopback path delay through the phone.

One additional area in which wireless device location can be important is in wireless networks, such as wireless local area networks (WLANs) or wide area networks (WANs), for example. A typical prior art approach to locating terminals within a WLAN includes locating a plurality of receivers at fixed locations within a building, for example, and then determining (i.e., triangulating) the position of a terminal based upon a signal received therefrom at each of the receivers.

Another prior art approach for wireless terminal location is to use a direction finding (DF) device which includes a directional antenna for receiving signals when pointed in the direction of a transmitting node. An example of a portable DF device for WLANs is the Yellowjacket 802.11a wi-fi analysis system from Berkeley Varitronics. This device uses a passive DF technique, i.e., it does not solicit any signals from a terminal but instead waits for the terminal to transmit signals before it can determine the direction of the transmission.

Despite the advantages of such prior art wireless communications device locators, additional wireless location features may be desirable in various applications.

SUMMARY OF THE INVENTION

In view of the foregoing background, it is therefore an object of the present invention to provide a wireless communications device locator which provides enhanced location features and related methods.

This and other objects, features, and advantages in accordance with the present invention are provided by a wireless communications system which may include a plurality of wireless communications devices each having a device type associated therewith from among a plurality of different device types. Further, each device type may have a known device latency associated therewith. The system may also include a wireless device locator. More particularly, the wireless device locator may include at least one antenna and a transceiver connected thereto, and a controller for cooperating with the transceiver for transmitting a plurality of location finding signals to a target wireless communications device from among the plurality of wireless communications devices. The target wireless communications device may transmit a respective reply signal for each of the location finding signals.

Additionally, the controller of the wireless device locator may also cooperate with the transceiver for receiving the reply signals, and it may determine a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor. This may be done based upon the known device latency of the target wireless communications device. As such, the controller may estimate a range to the target wireless communications device based upon a plurality of determined propagation delays.

In other words, the wireless device locator advantageously provides active range finding. In other words, the wireless device locator prompts the target wireless commu-

nications device to send reply signals using the location finding signals, rather than passively waiting until the target wireless communications device begins transmitting. This allows for quicker and more efficient device location.

Furthermore, by estimating the range based upon a plurality of propagation delays, the wireless device locator mitigates the effects of variations in the device latency time. That is, while the target wireless communication device has a known device latency, there will necessarily be some amount of variance from one transmission to the next. Using a plurality of propagation delays associated with different transmissions provides a significantly more accurate approximation of the device latency time and, thus, a more accurate range estimation. By way of example, the controller may estimate the range based upon an average (e.g., mean, median, mode, etc.) of the propagation delays.

In addition, each wireless communications device may have a unique identifier (UID) associated therewith, and the controller may insert the UID for the target wireless communications device in each of the location finding signals. Furthermore, the target wireless communications device may generate respective reply signals based upon the UID in the location finding signals. That is, the target wireless communications device will act upon the location finding signals because these signals include its UID, whereas the other wireless communications device will not.

The target wireless communications device may generate unsolicited signals including the UID thereof. As such, the controller may cooperate with the transceiver to receive at least one unsolicited signal from the target device, and the controller may also determine the UID for the target device from the at least one unsolicited signal. Thus, if the UID of a target wireless communications device is not already known, the wireless device locator may passively “listen” for unsolicited signals therefrom (i.e., signals that the wireless communications device did not solicit) and determine the UID based thereon.

Additionally, the controller may also determine the device type of the target wireless communications device based upon the UID. By way of example, the UIDs may include media access control (MAC) addresses of respective wireless communications devices. Accordingly, the controller may determine the device type of the target wireless communications device based upon the MAC address in some applications.

In accordance with another advantageous aspect of the invention, the at least one antenna may be a plurality of antennas, and the controller may cooperate with the plurality of antennas to determine a bearing to the target wireless communications device based upon at least one of the received reply signals. More particularly, the bearing may be a three-dimensional bearing, which may be particularly useful for locating wireless communications devices within a multi-story building, for example. In particular, the antenna(s) may be one or more directional antennas, for example. Further, the wireless device locator may further include a portable housing carrying the at least one antenna, the transceiver, and the controller.

The wireless device locator may be used with numerous type of wireless communications device. For example, the wireless communications devices may be wireless local area network (WLAN) devices, mobile ad-hoc network (MANET) devices, and cellular communications devices.

A method aspect of the invention is for locating a target wireless communications device from among a plurality of wireless communications devices, such as those discussed briefly above. The method may include transmitting a plu-

rality of location finding signals to the target wireless communications device, and receiving a respective reply signal for each of the location finding signals therefrom. The method may further include determining a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon the known device latency of the target wireless communications device. As such, a range to the target wireless communications device may be estimated based upon a plurality of determined propagation delays.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is schematic block diagram of a wireless communications system in accordance with the present invention including a wireless local area network (WLAN) and wireless device locator for locating WLAN devices thereof.

FIG. 2 is a schematic block diagram generally illustrating the components of the wireless device locator of FIG. 1.

FIG. 3 is a graph illustrating the signal propagation delay and device latency components used by the controller of FIG. 2 to estimate range.

FIG. 4 is a schematic block diagram illustrating an embodiment of the wireless device locator of FIG. 2 for a WLAN implementation.

FIG. 5 is a schematic block diagram illustrating in greater detail an embodiment of the transceiver of the wireless device locator of FIG. 4.

FIGS. 6 and 7 are histograms illustrating range estimation test results performed using the wireless device locator of FIG. 4.

FIG. 8 is a graph illustrating bearing determination in accordance with the present invention.

FIGS. 9 and 10 are schematic block diagrams illustrating alternate embodiments of the wireless communications system of FIG. 1 including a mobile ad-hoc network (MANET) and a cellular network, respectively.

FIG. 11 is a flow diagram illustrating a wireless device location method in accordance with the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout, and prime and multiple prime notation are used to indicate similar elements in different embodiments.

Referring initially to FIGS. 1 and 2, a wireless communications system 30 illustratively includes a wireless local area network (WLAN) 31 and a wireless location device 32. The WLAN 31 illustratively includes an access point 33 (e.g., a server) and a plurality of WLAN devices or terminals which communicate therewith wirelessly, such as the laptop computers 34, 35, and the desktop computer 36. Various WLAN protocols may be used in accordance with the present invention for such wireless communications (e.g., IEEE 802.11, Bluetooth, etc.), as will be appreciated by those of skill in the art. Moreover, it will also be appreciated that additional access points and/or other numbers of wireless communications devices may be used, even though only

a few number thereof are shown for clarity of illustration. Further, numerous other types of WLAN enabled wireless communications devices (e.g., personal data assistants, etc.) may also be used, as will be further appreciated by those skilled in the art.

Each wireless communications device 34–36 in the WLAN 31 has a device type associated therewith from among a plurality of different device types. More particularly, the device type may signify the particular manufacturer and/or model of a given WLAN card or chip set used therein. In some embodiments, it may also signify the standard the device complies with (e.g., IEEE 802.11).

The device type is important in that different device types will have known device latencies associated therewith. For example, different WLAN cards or chip sets will have a certain latency associated with the time they take to process a received signal and generate an acknowledgement reply thereto. These delay times may be fairly consistent across different models from a same manufacturer, or they may vary significantly. Additionally, WLAN protocols such as IEEE 802.11 have a specified interframe spacing associated therewith, as will be appreciated by those skilled in the art. Thus, in circumstances where the interframe spacing requirements are closely adhered to, the latency of a given WLAN card or chip set will be substantially equal to the interframe spacing.

The wireless device locator 32 illustratively includes an antenna 39 and a transceiver 41 connected thereto, as well as a controller 42 connected to the transceiver. These components may conveniently be carried by a portable housing 43 in some embodiments, although they could be implemented in a more stationary embodiment, if desired. In the illustrated example, the antenna 39 is a directional antenna, although omni-directional antennas may also be used, as will be appreciated by those skilled in the art. It will also be appreciated that various antenna/transceiver combinations may be used. As will be discussed further below, more than one antenna may be used in certain embodiments to provide bearing determination capabilities, and separate transceivers may optionally be used for respective antennas, if desired.

Operation of the wireless device locator 32 will now be described with reference to FIG. 3. The controller 42 cooperates with the transceiver 41 for transmitting a plurality of location finding signals to a target wireless communications device to be located from among the plurality of wireless communications devices. In the present example, the laptop 34 is the target device.

As will be appreciated by those skilled in the art, each WLAN device 34–36 in the network 31 will have a unique identifier (UID) associated therewith which is used in signals transmitted between the respective devices and the access point 33. The UID distinguishes the devices 34–36 from one another so that each device only acts upon or responds to signals intended for it, and so the access point 33 knows which device it is receiving signals from.

Depending upon a given implementation, the wireless locator device 32 may or may not know the UID of the target device 34 before hand. For example, in some embodiments the wireless device locator 32 could download the UID from the access point 33 (either wirelessly or over a wired network connection, for example). This may be the case when trying to locate a node in a LAN where the node is already registered with the network. However, if the UID is not known, the wireless device locator 32 may passively listen to the target device 34 for unsolicited signals being transmitted therefrom. This feature may be advantageous for law enforcement applications, or for locating an interfering

node that is not registered with a particular network but causes interference therewith, for example. By “unsolicited” signals it is meant that these signals are not solicited by the wireless device locator 32 itself, although such signals may have been solicited from another source (e.g., the access point 33).

The controller 42 cooperates with the transceiver 41 to receive one or more of the unsolicited signals, and the controller determines the UID for the target device 34 therefrom. Of course, the method by which the controller 42 determines the UID from the unsolicited signal will depend upon the given implementation, and whether or to what degree such signals are encrypted.

Additionally, the controller 42 may also determine the device type of the target wireless communications device 34 based upon the UID thereof. By way of example, the UIDs may include media access control (MAC) addresses of respective wireless communications devices. The MAC addresses may be specific to a particular type of device manufacturer, or indicate a particular operational protocol with which the device is operating, as will be appreciated by those skilled in the art. Accordingly, the controller may determine the device type of the target wireless communications device 34 based upon the MAC address thereof in some applications.

As such, to locate the target device 34, the controller inserts the UID therefor in each of the location finding signals. By way of example, the location finding signal may include the UID of the target device 34 in a header packet and a valid but empty data packet. This will force the target device 34 to generate a reply signal acknowledging receipt of the location finding signal (i.e., an ACK signal). Of course, various other location finding signals could be used to cause the target terminal 34 to generate an ACK signal, as will be appreciated by those skilled in the art. The controller 42 cooperates with the transceiver 41 for receiving the reply signals from the target device 34 via the antenna 39. The location finding signals and reply signals may be radio frequency (RF), microwave, optical, or other suitable types of signals, as will be appreciated by those skilled in the art.

The controller 42 determines the propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor, and it uses this propagation delay to estimate a range to the target device 34. However, the propagation delay has to first be determined based upon the total round trip time from the sending of the location finding signal to the reception of the respective reply signal.

The total round trip time will include several components. Referring more particularly to FIG. 3, the first component is the time associated with transmitting a location finding signal 45, which is illustrated with an arrow. That is, this is the time from the beginning of the location finding signal transmission (time t_0) to end thereof (time t_1). Two time axes are shown in FIG. 3. The top or upper axis represents events that occur at the target device 34, while the bottom or lower axis represents events that occur at the wireless device locator 32.

The second component of the round trip time is the propagation delay or time t_{PD} it takes for the location finding signal 45 to travel from the wireless device locator 32 to the target device 34 (i.e., from time t_1 to t_2). The third component of the round trip time is the device latency t_{DL} of the target device 34 (i.e., from time t_2 to t_3). This is the time it takes the target device 34 to receive, process, and transmit a reply signal 46 responsive to the location finding signal 45. The final components of the round trip time are propagation

delay t_{PD2} of the reply signal 46 (i.e., from time t_3 to t_4), and the reception time thereof by the wireless device locator 32 (i.e., from time t_4 to t_5).

The controller 42 will know the times associated with the transmission of the location finding signal 45 (i.e., from time to t_0 to t_1), as well as the time associated with the reception of the reply signal 46 (i.e., from time t_4 to t_5) for each round trip, since these can be readily measured by the controller. The quantities that the controller 42 will not know are the propagation delays t_{PD1} , t_{PD2} and the actual device latency t_{DL} .¹⁰

Yet, as noted above, the controller 42 will have access to the known device latency (i.e., a mean latency) for the given device type of the target device 34, which provides a close approximation of the actual device latency t_{DL} . The known device latency could be a measured value based upon collected data, it could be provided by manufacturers, or it could be based upon a value set in a communications standard, as discussed above, for example.¹⁵

As will be appreciated by those skilled in the art, the actual device latency will likely vary somewhat from one transmission to the next for any wireless communications device, potentially by as little as a few nanoseconds to a few microseconds, depending upon device configurations, processing loads, etc. Accordingly, a close approximation of the total propagation delay (i.e., time t_{PD1} +time t_{PD2}) may therefore be obtained by substituting the known device latency for the actual device latency t_{DL} , and subtracting this value from the time between times t_1 and t_4 . Dividing the total propagation delay by two (since both propagation delays may be considered equal or substantially equal for a stationary or relatively slow moving target device 34) and multiplying this by the speed of light gives the estimated distance to the target device 39, based upon the single propagation delay associated with the signal pair 45, 46.²⁰

Yet, as noted above, device latencies tend to vary from one transmission to the next. Since the location finding signals and reply signals are traveling at the speed of light, such variances can make a significant difference in the estimated distances. More particularly, light travels approximately 1000 ft. in one microsecond. Thus, if the device latency varies by one microsecond from one transmission to the next, the estimated distance to the target device 34 would similarly vary by 1000 ft. or so, which likely will be an unacceptable accuracy for many applications.²⁵

In accordance with the present invention, the controller 42 advantageously estimates the range to the target device 34 not solely based upon a single measured propagation delay, but rather upon a plurality thereof. More particularly, by estimating the range based upon a plurality of propagation delays, the wireless device locator 32 mitigates the effects of the variations in the actual device latency time. This provides a significantly more accurate approximation of the device latency time and, thus, a more accurate range estimation. By way of example, the controller 42 may estimate the range based upon an average of the propagation delays, though other suitable statistical functions may also be used (e.g., mean, median, mode, etc.). Of course, it should be noted that the average may be taken on the entire round trip delay instead of first subtracting out the known device latency as described above. That is, the same result may be obtained by first taking the average and then subtracting out the known device latency, as will be appreciated by those skilled in the art.³⁰

An exemplary embodiment of the present invention is now described with reference to FIGS. 4 and 5. The wireless device locator 32' may use a personal data assistant (PDA)

as the controller 42', although a personal computer (PC) or other suitable computing device may also be used. More particularly, the PDA 42' illustratively includes a graphical user interface (GUI) 50', and a received signal strength indication (RSSI) processing module 51' for cooperating with the transceiver 41' to perform above-described range estimation processing operations. More particularly, the RSSI module 51' may be implemented as a software module which is run on the PDA 42', as will be appreciated by those skilled in the art, and which cooperates with the GUI to provide range estimates to a user.⁵

The PDA 50' also illustratively includes a battery 52', which may conveniently be used for powering the various transceiver 41' components, as shown. Of course, it will be appreciated that separate batteries may be used, or one or more components of the wireless device locator 32' may be powered by an external (e.g., AC) source. The transceiver 41' operates in accordance with the IEEE 802.11b standard and includes a MAC-less 802.11b radio 58' and a field-programmable gate array (FPGA) 53' connected thereto. The FPGA 53' illustratively includes a packet building module 54', a radio configuration module 55', a receiver filtering module 56', and a simple MAC processing module 57' for processing the location finding signals and reply signals and communicating with the radio 53' in accordance with the 802.11b standard, as will be appreciated by those skilled in the art.¹⁵

More specifically, the MAC-less radio 58' may be a GINA model RF module from GRE America, Inc., and the FPGA 53' may be a module EPXA10 from Altera Corp. The hardware components of the FPGA 53" illustratively include an ARM922T processor 60", block RAM 61" therefor, a serial/universal serial bus (USB) interface 62", and a programmable logic section 63". Additional circuitry including an oscillator 64", power management circuitry (i.e., regulators, microprocessor supervisor, etc.) 65", and a programmable read-only memory (PROM)/boot flash memory 66" are connected thereto as shown, as will be appreciated by those skilled in the art.²⁰

Referring now to FIGS. 6-7, a test was conducted in accordance with the present invention in which approximately 1500 location finding signals were transmitted to a stationary wireless IEEE 802.11 device. The time it took to receive the reply signal was measured by ticks of an internal clock of the controller 42, where each tick represents 7.567 ns. From FIG. 6 it may be seen that the reply signals from the target device were returned within between about 20,960 and 21,045 clock ticks, where the transmission of the respective location signals each began at 0 clock ticks. Moreover, if this range is divided into equal sections or bins, the frequency (i.e., number) of round trip times that fell within each of the bins is shown in FIG. 7.²⁵

Plotting various statistical functions of the measured clock tick samples (such as the mean and the mode) versus the known distance to the target device allowed statistical curve-fitting to take place, as shown in FIG. 6. It was determined from the test results that taking the mean of the samples provided the most accurate range estimation. More particularly, the ranges to several 802.11b target devices at varying distances were estimated using this approach, and the worst case error for the estimated range was never more than 20 ft. Preferably, the location finding signals are transmitted over a relatively short interval (a few seconds or less) so that if the target device is moving the accuracy of the results will not be significantly diminished. Of course, various numbers of location finding signals and transmission

intervals may be used depending upon the particular implementation, as will be appreciated by those skilled in the art.

In accordance with another advantageous aspect of the invention, multiple antennas 39a", 39b" (FIG. 5) may be used to provide target bearing in addition to the estimated range. Referring more particularly to FIG. 8, bearing determination in the case where the antennas 39a", 39b" are directional antennas will now be described. The antennas 39a", 39b" have respective reception patterns 70a, 70b, which may be orthogonal to one another (i.e., the former is directed along the x-axis, while the latter is directed along the y-axis).

The target device is at a point P, which is within the reception patterns 70a, 70b. Each of the antenna gain patterns 70a and 70b can be measured and known to the locator, and represented by gain functions G1(θ) and G2(θ) where θ represents the angle of deviation from a particular reference direction.

As such, to determine the line of bearing to the target device, the received signal strength is measured from each of the antennas 70a, 70b, respectively. Based upon this information, the controller 42' may then find the angle θ, using the relationship $G1(\theta_r) - G2(\theta_r) = P1 - P2$, where P1 and P2 is the received signal power off antenna 1 and antenna 2, respectively. In other words, the difference in the signal strength received between the two antennas (P1-P2) should equal the difference in the antenna gain of the two antennas at the angle of the line of bearing ($G1(\theta_r) - G2(\theta_r)$). Thus, the target line of bearing to the target device is at θ_r. It should be noted that it is possible that more than one angle θ may satisfy the relationship $G1(\theta_r) - G2(\theta_r) = P1 - P2$. These multiple angles represent a line of bearing ambiguity that can easily be resolved by making multiple measurements, as can be appreciated by those skilled in the art.

As noted above, more than one transceiver 41' may be used in certain embodiments, which would allow signal strength measurements to be taken based upon a same reply signal from the target device. However, if only a single transceiver 41' is used, the controller 42' may alternate which antenna 70a, 70b is receiving and measure the received signal strength of successive signals, for example. Moreover, the bearing may be determined in three dimensions, if desired, which may be particularly useful for locating wireless communications devices within a multi-story building, for example, as will be appreciated by those skilled in the art.

While the present invention has been described above with reference to a WLAN wireless device locator 32', it will be appreciated by those skilled in the art that it may also be used in other wireless communications systems with other types of wireless communications devices. Referring more particularly to FIG. 9, a mobile ad-hoc network (MANET) system 90 illustratively includes a wireless device locator 92 including an antenna 99, such as those described above, and a MANET 91. More particularly, the MANET includes MANET nodes or devices 93-96, of which the node 94 is the target node in the illustrated example. Here, the wireless device locator 92 performs range and/or bearing estimation in the same manner described above, except that it will operate in accordance with the appropriate MANET protocol used within the system 90, as will be appreciated by those skilled in the art.

Another embodiment is illustrated in FIG. 10, in which a wireless device locator 102 having an antenna 109 is used within a cellular communications system 100 for locating cellular devices (e.g., cellular telephones) 104-106 in cellular network 101. The cellular devices 104-106 place and

receive calls via a cellar tower 103, as will be appreciated by those skilled in the art. In the illustrated example, the target device is the cell phone 104. Here again, the wireless device locator 102 will communicate using the appropriate operating protocol being used in the cellular network 101 (e.g., code-division multiple access (CDMA), short message service (SMS), etc.), as will be appreciated by those skilled in the art.

Turning now additionally to FIG. 11, a method aspect of the invention is for locating a target wireless communications 10 device from among a plurality of wireless communications devices 34-36. Beginning at Block 110, if the UID for the target device 34 is unknown, the controller 42 may determine the UID from unsolicited signals transmitted by the target device, for example, as described above (Block 112). Of course, in some embodiments, the controller 42 may download the signals from a network access point 33, etc., as also described above.

Once the UID for the target wireless communication device 34 is known, location finding signals are transmitted to the target wireless communications device, at Block 113, and respective reply signals for each of the location finding signals are received therefrom, at Block 114. If the device type (and, thus, the known device latency) are known, at Block 115, then the propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor is determined based upon the known device latency of the target wireless communications device 34, at Block 116. As such, a range to the target wireless communications device 34 is estimated based upon a plurality of determined propagation delays (Block 117), as previously discussed above, thus concluding the illustrated method (Block 118).

Of course, if the device type is unknown, the controller 42 may determine the device type from the reply signal (Block 119), as discussed above, or by other suitable methods which will be appreciated by those skilled in the art. It should be noted that while this step is shown as occurring after the receipt of the reply signals in the illustrated example, the device type determination may be performed prior thereto, such as while determining the UID, for example.

Many modifications and other embodiments of the invention will come to the mind of one skilled in the art having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is understood that the invention is not to be limited to the specific embodiments disclosed, and that modifications and embodiments are intended to be included within the scope of the appended claims.

That which is claimed is:

1. A wireless communications system comprising:
a plurality of wireless communications devices each having a device type associated therewith from among a plurality of different device types, each WLAN device having a unique identifier (UID) associated therewith, and each device type having a known device latency associated therewith; and
a wireless device locator comprising
at least one antenna and a transceiver connected thereto, and
a controller for cooperating with said transceiver for transmitting a plurality of location finding signals to a target wireless communications device from among said plurality of wireless communications devices and inserting the UID for said target wireless communications device in each of the location finding signals;

11

said target wireless communications device transmitting a respective reply signal for each of said location finding signals based upon the UID in the location finding signals;
 said controller of said wireless device locator also for cooperating with said transceiver for receiving the reply signals,
 determining a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon the known device latency of said target wireless communications device, and
 estimating a range to said target wireless communications device based upon a plurality of determined propagation delays.

2. The wireless communications system of claim 1 wherein said controller estimates the range based upon an average of the propagation delays.

3. The wireless communications system of claim 1 wherein said target wireless communications device generates unsolicited signals including the UID thereof; wherein said controller cooperates with said transceiver to receive at least one unsolicited signal from said target device; and wherein said controller determines the UID for said target wireless communications device from the at least one unsolicited signal.

4. The wireless communications system of claim 3 wherein said controller determines the device type of said target wireless communications device based upon the UID thereof.

5. The wireless communications system of claim 4 wherein the UIDs comprise media access control (MAC) addresses of respective wireless communications devices, and wherein said controller determines the device type of said target wireless communications device based upon the MAC address thereof.

6. The wireless communications system of claim 1 wherein said at least one antenna comprises a plurality of antennas; and wherein said controller cooperates with said plurality of antennas to determine a bearing to said target wireless communications device based upon at least one of the received reply signals.

7. The wireless communications system of claim 6 wherein the bearing is a three-dimensional bearing.

8. The wireless communications system of claim 1 wherein said at least one antenna comprises at least one directional antenna.

9. The wireless communications system of claim 1 wherein said wireless device locator further comprises a portable housing carrying said at least one antenna, said transceiver, and said controller.

10. The wireless communications system of claim 1 wherein said wireless communications devices comprise wireless local area network (WLAN) devices.

11. The wireless communications system of claim 1 wherein said wireless communications devices comprise mobile ad-hoc network (MANET) devices.

12. The wireless communications system of claim 1 wherein said wireless communications devices comprise cellular communications devices.

13. A wireless communications system comprising:

a plurality of wireless local area network (WLAN) devices each having a device type associated therewith from among a plurality of different device types, each WLAN device having a unique identifier (UID) associated therewith, and each device type having a known device latency associated therewith; and

12

a wireless device locator comprising at least one antenna and a transceiver connected thereto, and

a controller for cooperating with said transceiver for transmitting a plurality of location finding signals to a target WLAN device from among said plurality of WLAN devices and inserting the UID for said target wireless communications device in each of the location finding signals;

said target WLAN device transmitting a respective reply signal for each of said location finding signals based upon the UID in the location finding signals;

said controller of said wireless device locator also for cooperating with said transceiver for receiving the reply signals,

determining a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon the known device latency of said target WLAN device, and

estimating a range to said target WLAN device based upon an average of a plurality of determined propagation delays.

14. The wireless communications system of claim 13 wherein said target WLAN device generates unsolicited signals including the UID thereof; wherein said controller cooperates with said transceiver to receive at least one unsolicited signal from said target WLAN device; and wherein said controller determines the UID for said target WLAN device from the at least one unsolicited signal.

15. The wireless communications system of claim 14 wherein said controller determines the device type of said target WLAN device based upon the UID thereof.

16. The wireless communications system of claim 15 wherein the UIDs comprise media access control (MAC) addresses of respective WLAN devices, and wherein said controller determines the device type of said target WLAN device based upon the MAC address thereof.

17. The wireless communications system of claim 13 wherein said at least one antenna comprises a plurality of antennas; and wherein said controller cooperates with said plurality of antennas to determine a bearing to said target WLAN device based upon at least one of the received reply signals.

18. A wireless device locator for locating a target wireless communications device having a unique identifier (UID) associated therewith, the wireless device locator comprising:

at least one antenna and a transceiver connected thereto; and a controller for cooperating with said transceiver for transmitting a plurality of location finding signals to the target wireless communications device, inserting the UID for the target wireless communications device in each of the location finding signals, and receiving a respective reply signal for each of said location finding signals generated by the target wireless communications device based upon the UID in the location finding signals,

determining a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon a known device latency of the target wireless communications device, and

estimating a range to the target wireless communications device based upon a plurality of determined propagation delays.

13

19. The wireless device locator of claim **18** wherein said controller estimates the range based upon an average of the propagation delays.

20. The wireless device locator of claim **18** wherein the target wireless communications device generates unsolicited signals including the UID thereof; wherein said controller cooperates with said transceiver to receive at least one unsolicited signal from the target device; and wherein said controller determines the UID for the target wireless communications device from the at least one unsolicited signal. ⁵

21. The wireless device locator of claim **18** wherein said at least one antenna comprises a plurality of antennas; and wherein said controller cooperates with said plurality of antennas to determine a bearing to the target wireless communications device based upon at least one of the received reply signals. ¹⁵

22. The wireless device locator of claim **18** wherein said at least one antenna comprises at least one directional antenna.

23. The wireless device locator of claim **18** wherein said wireless device locator further comprises a portable housing carrying said at least one antenna, said transceiver, and said controller. ²⁰

24. The wireless device locator of claim **18** wherein the target wireless communications device comprises a wireless local area network (WLAN) device. ²⁵

25. The wireless device locator of claim **18** wherein the target wireless communications device comprises a mobile ad-hoc network (MANET) device.

26. The wireless device locator of claim **18** wherein the target wireless communications device comprises a cellular communications device.

27. A method for locating a target wireless communications device from among a plurality of wireless communications devices, each wireless communications device having a device type associated therewith from among a plurality of different device types, each WLAN device having a unique identifier (UID) associated therewith, and each device type having a known device latency associated therewith, the method comprising: ³⁵

transmitting a plurality of location finding signals to the target wireless communications device, inserting the

14

UID for the target wireless communications device in each of the location finding signals, and receiving a respective reply signal for each of the location finding signals generated by the target wireless communications device based upon the UID in the locations signals;

determining a propagation delay associated with the transmission of each location finding signal and the respective reply signal therefor based upon the known device latency of the target wireless communications device; and estimating a range to the target wireless communications device based upon a plurality of determined propagation delays.

28. The method of claim **27** wherein the controller estimates the range based upon an average of the propagation delays.

29. The method of claim **27** wherein the target wireless communications device generates unsolicited signals including the UID thereof; and further comprising:

receiving at least one unsolicited signal from the target device; and

determining the UID for the target wireless communications device from the at least one unsolicited signal.

30. The method of claim **29** further comprising determining the device type of the target wireless communications device based upon the UID thereof. ³⁰

31. The method of claim **27** further comprising determining a bearing to the target wireless communications device based upon at least one of the received reply signals. ³⁵

32. The method of claim **27** wherein the target wireless communications device comprises a wireless local area network (WLAN) device.

33. The method of claim **27** wherein the target wireless communications device comprises a mobile ad-hoc network (MANET) device.

34. The method of claim **27** wherein the target wireless communications device comprises a cellular communications device. ⁴⁰

* * * * *



US008792464B2

ELECTRONICALLY FILED
2014 MAR 12 PM
2014 CH 1538
CALENDAR: 11
PAGE 1 of 13
CIRCUIT COURT OF
ILLINOIS
CLERK DOROTHY BROWN

(12) **United States Patent**
Voglewede et al.

(54) **COMMUNICATION NETWORK FOR DETECTING UNCOOPERATIVE COMMUNICATIONS DEVICE AND RELATED METHODS**

(75) Inventors: **Paul E. Voglewede**, Chili, NY (US); **Nick A. Van Stralen**, Bloomfield, NY (US); **William N. Furman**, Fairport, NY (US); **Clifford Hessel**, Rochester, NY (US); **Fred C. Kellerman**, Webster, NY (US); **James J. Hood**, Victor, NY (US); **Richard J. Buckley**, Henrietta, NY (US); **Dennis Martinez**, Westford, MA (US)

(73) Assignee: **Harris Corporation**, Melbourne, FL (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 273 days.

(21) Appl. No.: **13/407,964**

(22) Filed: **Feb. 29, 2012**

(65) **Prior Publication Data**

US 2013/0223417 A1 Aug. 29, 2013

(51) **Int. Cl.**

H04W 72/04 (2009.01)
H04B 7/04 (2006.01)
H04W 4/00 (2009.01)
H04W 84/04 (2009.01)

(52) **U.S. Cl.**

CPC **H04W 72/0446** (2013.01); **H04B 7/04** (2013.01); **H04W 4/00** (2013.01); **H04W 84/045** (2013.01)
USPC **370/337**; 370/330; 370/341; 370/349; 455/456.5

(58) **Field of Classification Search**

CPC H04W 8/10; H04W 60/04; H04W 84/045;
H04W 72/04; H04B 7/04

USPC 370/328, 337

See application file for complete search history.

(10) **Patent No.:**

(45) **Date of Patent:**

US 8,792,464 B2
CHANCERY DIVISION
CLERK DOROTHY BROWN

(56)

References Cited

U.S. PATENT DOCUMENTS

5,451,956 A	9/1995	Lochhead
5,719,584 A *	2/1998	Otto
6,201,495 B1	3/2001	Lemelson et al.
6,407,703 B1 *	6/2002	Minter et al.

(Continued)

FOREIGN PATENT DOCUMENTS

WO 2010063469 6/2010

OTHER PUBLICATIONS

“3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Stage 2 functional specification of user equipment (UE) positioning in UTRAN (release 10)”, 3GPP Standard, No. V10.0.0, Oct. 2010, pp. 1-80.

(Continued)

Primary Examiner — Jeffrey M Rutkowski

Assistant Examiner — Rasha Fayed

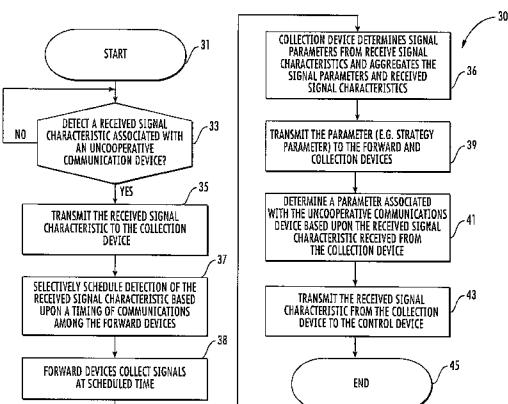
(74) *Attorney, Agent, or Firm* — Allen, Dyer, Doppelt, Milbrath & Gilchrist, P.A.

(57)

ABSTRACT

A communication network may be uncooperative with an uncooperative communications device. The communication network includes mobile wireless communications devices including a collection device and forward devices. Each forward device is configured to detect a received signal characteristic associated with the uncooperative communications device, and transmit the received signal characteristic to the collection device. The collection device is configured to selectively schedule reception of the received signal characteristic based upon a timing of communications among the forward devices, and determine a parameter associated with the uncooperative communications device based upon the received signal characteristic.

32 Claims, 5 Drawing Sheets



(56)

References Cited

U.S. PATENT DOCUMENTS

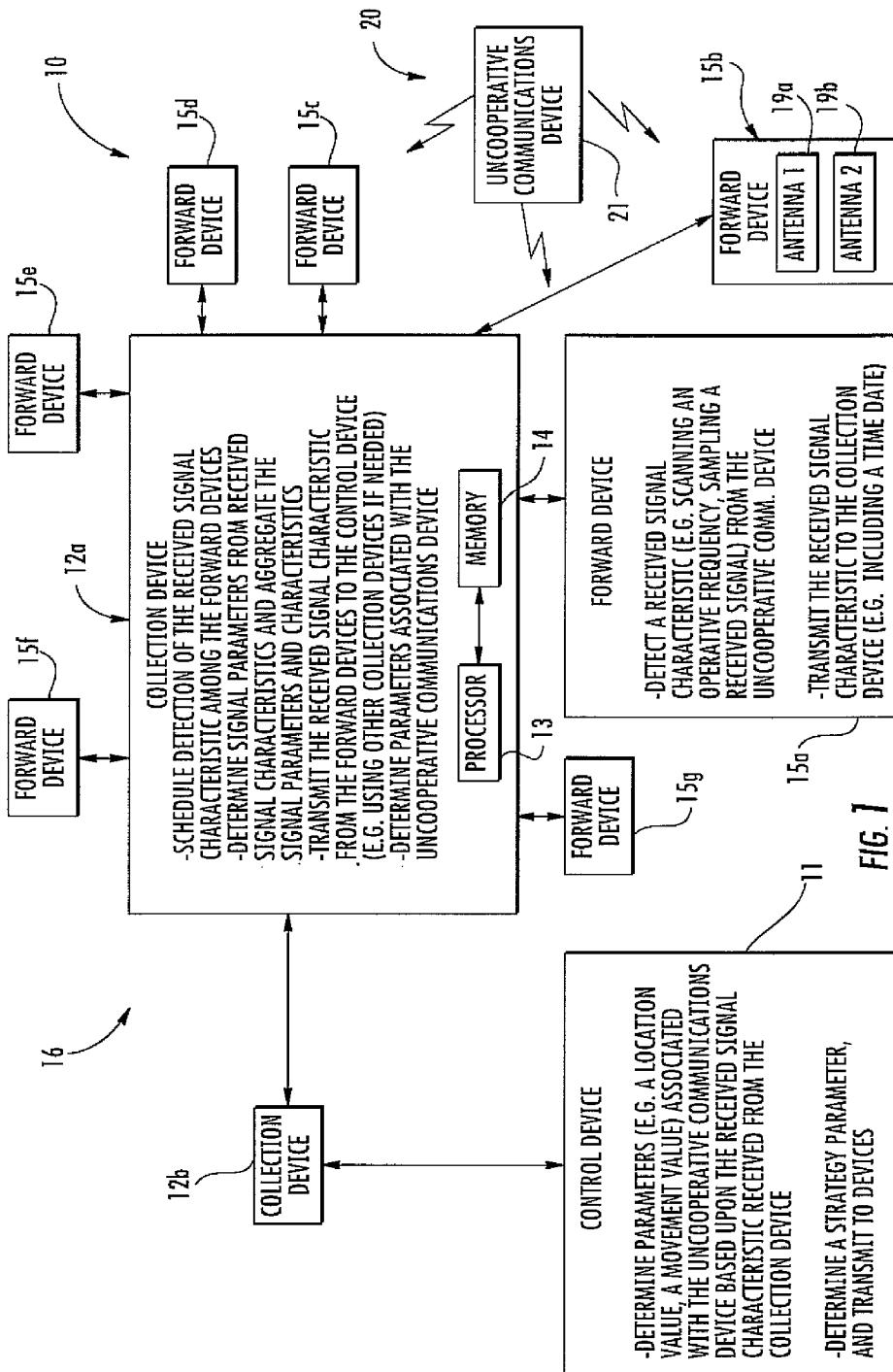
7,248,203	B2	7/2007	Gounalis	
7,358,887	B2	4/2008	Gounalis	
7,475,428	B2	1/2009	Smith et al.	
7,539,166	B2 *	5/2009	Do et al.	370/335
7,944,468	B2 *	5/2011	Hoffman et al.	348/143
8,259,652	B2 *	9/2012	Huang et al.	370/328
8,560,609	B2 *	10/2013	Nathanson	709/204
8,711,764	B2 *	4/2014	Kim et al.	370/328
2002/0181492	A1 *	12/2002	Kasami et al.	370/445
2004/0135717	A1 *	7/2004	Gounalis	342/13
2005/0105505	A1 *	5/2005	Fishler et al.	370/349

2006/0019679	A1 *	1/2006	Rappaport et al.	455/456.5
2008/0144572	A1 *	6/2008	Makhijani	370/330
2009/0074422	A1	3/2009	Stewart	
2010/0273504	A1	10/2010	Bull et al.	
2011/0148714	A1 *	6/2011	Schantz et al.	342/458
2012/0094610	A1 *	4/2012	Lunden et al.	455/67.13
2012/0195256	A1 *	8/2012	Khoury	370/328

OTHER PUBLICATIONS

"Multifunction radio system that enables spectrum superiority," Northrop Grumman, 2009, 2 pages.

* cited by examiner



ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 4 of 13

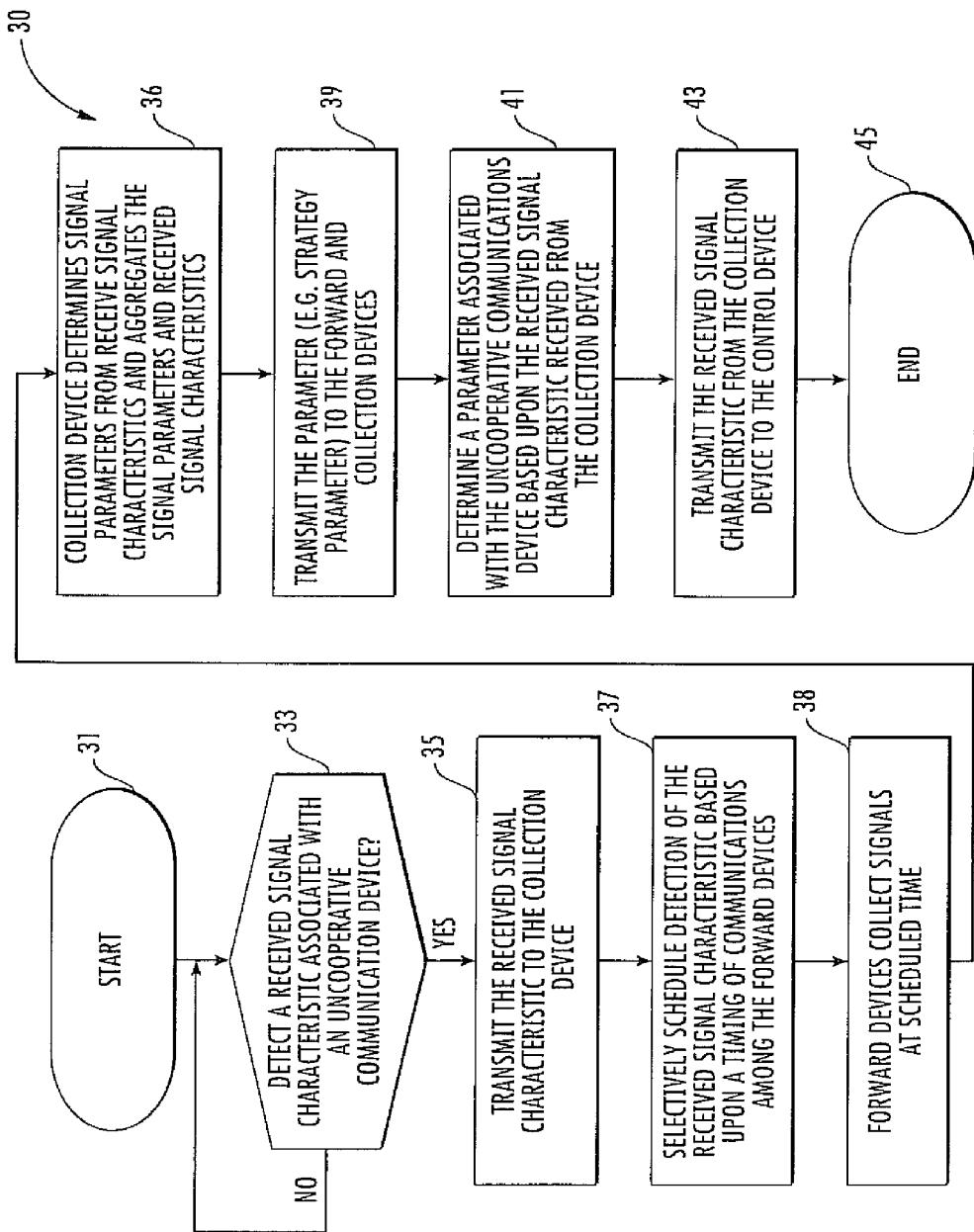


FIG. 2

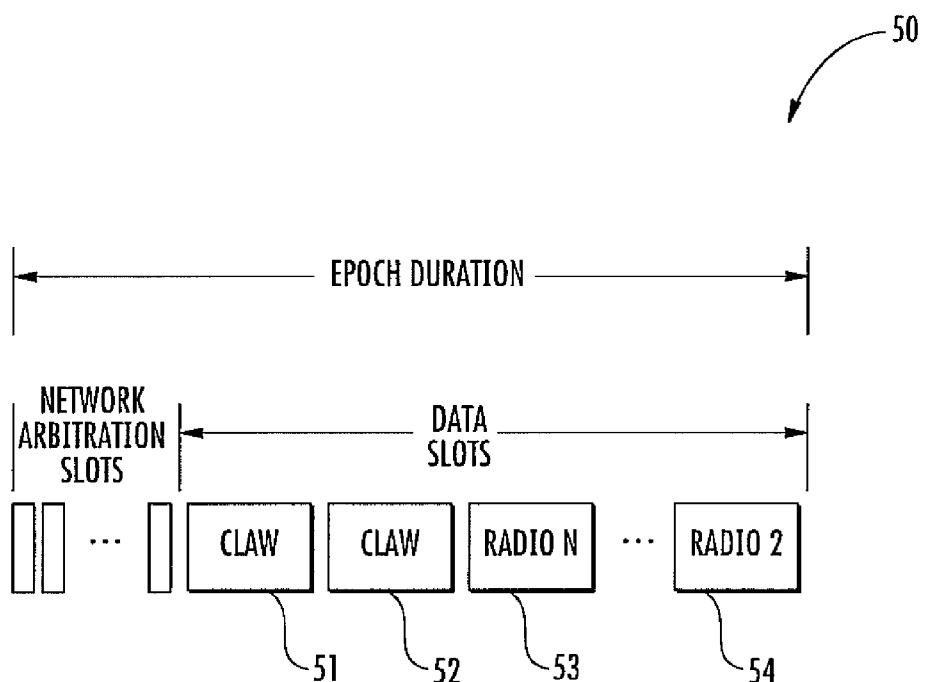


FIG. 3

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 5 of 13

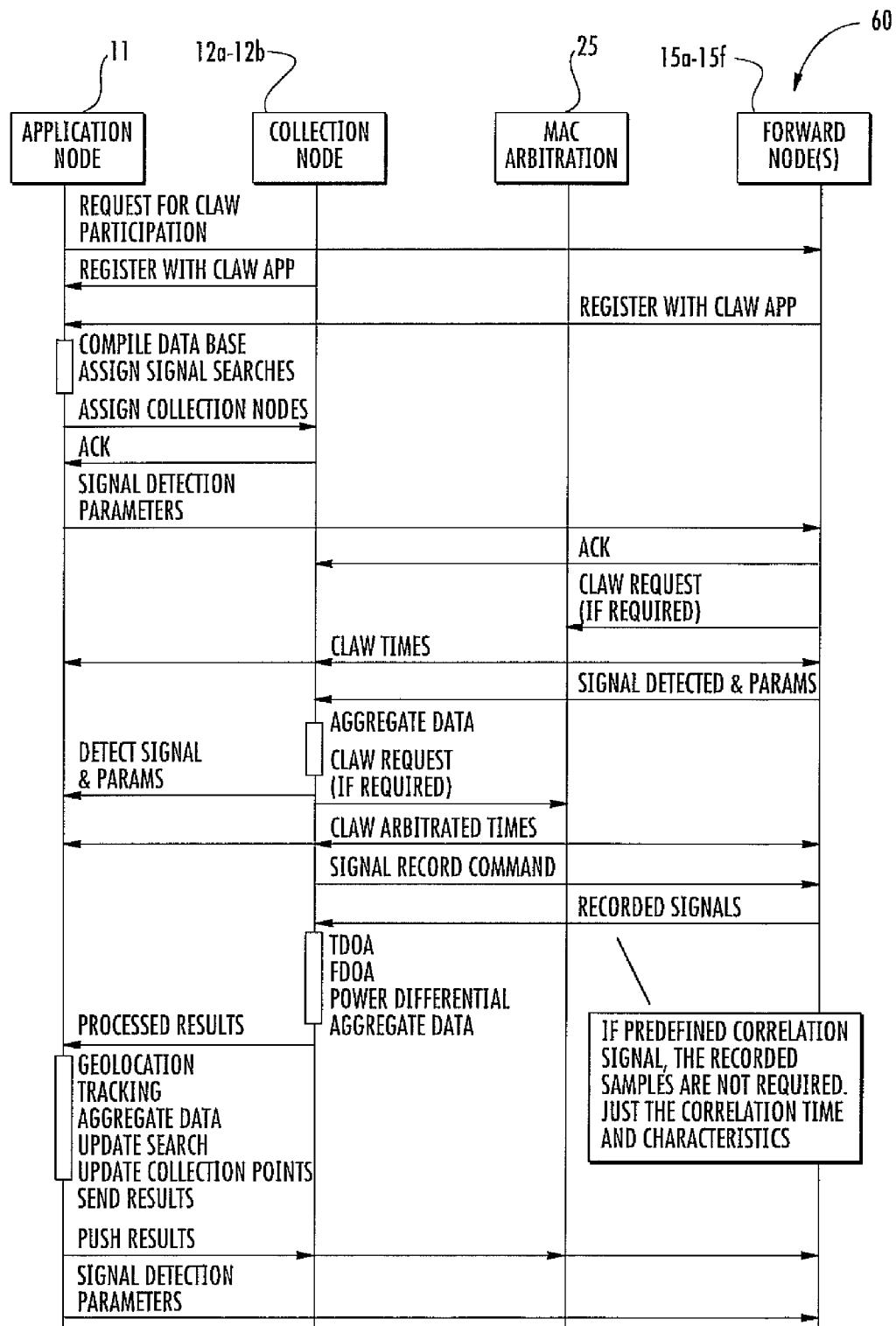


FIG. 4

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 7 of 13

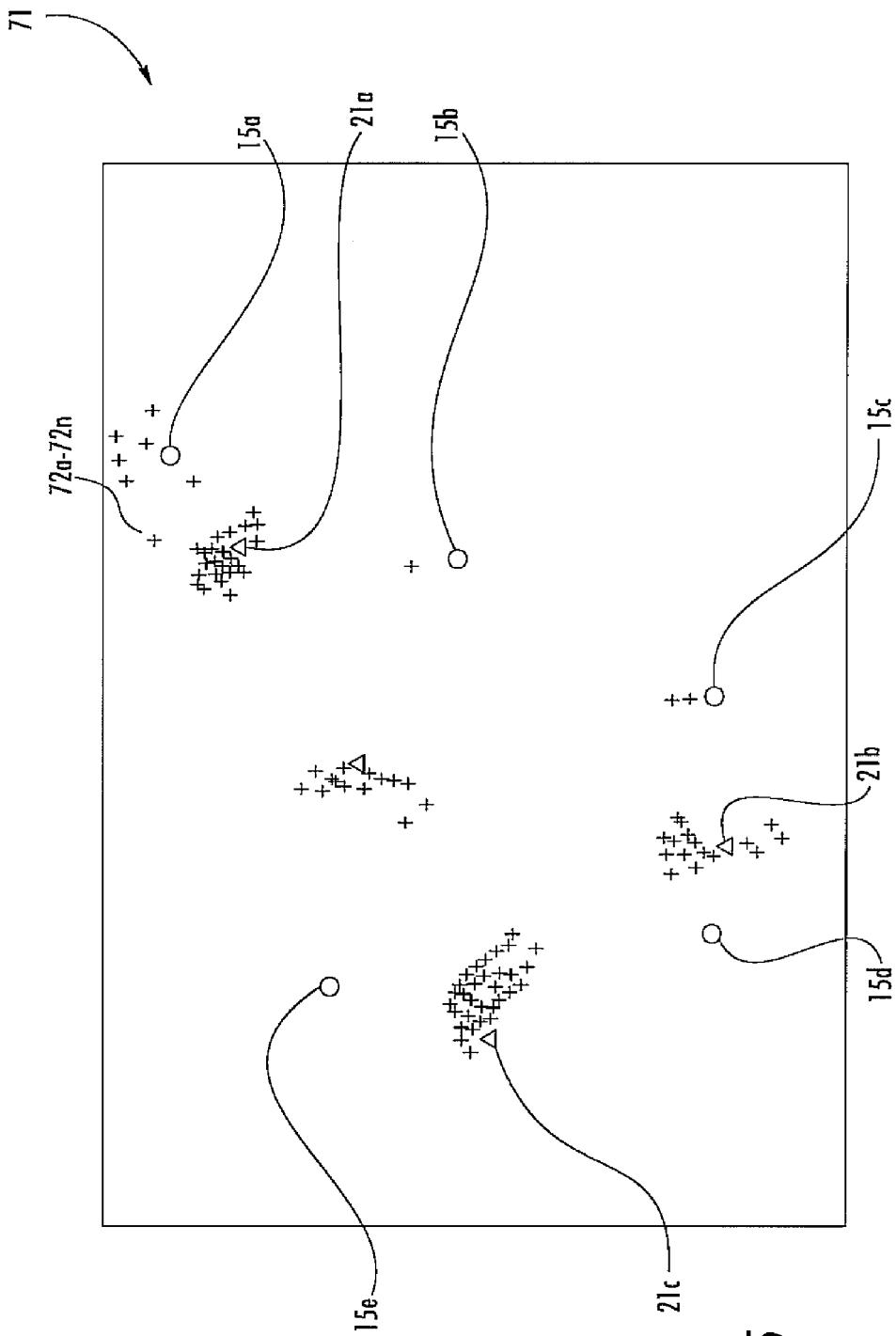


FIG. 5

**COMMUNICATION NETWORK FOR
DETECTING UNCOOPERATIVE
COMMUNICATIONS DEVICE AND RELATED
METHODS**

FIELD OF THE INVENTION

The present invention relates to the field of wireless communications, and, more particularly, to detecting wireless communications devices and related methods.

BACKGROUND OF THE INVENTION

In government, municipal, and law enforcement applications, there is sometimes a desire to track a communications device. Since it is not uncommon for a person to carry a cellular telephone device with them on a daily basis, there may be desire by local police and fire departments to use a corresponding cellular telephone device to help locate a missing person, for example, a person trapped in a collapsed building or a fugitive. Of course, in these applications, such as tracking a cellular communications device, the device and associated user are not actively attempting to mask their location, i.e. an uncooperative communications device. Conventional approaches to communications device location include systems comprising a plurality of sensors. These systems typically use a triangulation method to determine the location of the communications device.

One approach to communications device location, for example, a cellular telephone device, is disclosed by U.S. Pat. No. 6,407,703 to Minter et al. The system of Minter et al. includes a plurality of sensors situated in multiple locations/platforms. The system uses angle of arrival (AOA), time difference of arrival (TDOA), and terrain altitude information from signal intercepts from the cellular telephone device to determine the location thereof. The sensors use accurate time synchronization for determining the TDOA of the intercepted signals.

Another approach is disclosed in U.S. Pat. No. 5,719,584 to Otto, assigned to the present application's assignee, Harris Corporation of Melbourne, Fla. This system uses a plurality of ground based sensors to determine a location of the cellular telephone device by measuring TDOA and AOA values. This network of sensors is also synchronized.

Another approach is disclosed in U.S. Patent Application Publication No. 2004/0135717 to Gounalis. Gounalis discloses a system for detecting wireless transmission signals from an emitter. The system determines and implements a selective scanning strategy, for example, using a frequency domain windowing approach.

Another approach is disclosed in U.S. Pat. No. 7,944,468 to Hoffman et al. Hoffman et al. discloses a predictive threat detection system. The system includes a sensor network spread over an urban environment, and combines data for analysis from each of these sites. A potential drawback to the above systems is that no approach provides a method for distributing information to cooperative communications devices. Moreover, deploying a large network of sensors, such as in Hoffman et al., can be expensive and impractical.

SUMMARY OF THE INVENTION

In view of the foregoing background, it is therefore an object of the present invention to provide a communication network that can efficiently track uncooperative communications devices.

This and other objects, features, and advantages in accordance with the present invention are provided by a communication network uncooperative with an uncooperative communications device, the communication network comprising a plurality of mobile wireless communications devices comprising at least one collection device and a plurality of forward devices. Each forward device is configured to detect a received signal characteristic associated with the uncooperative communications device, and transmit the received signal characteristic to the at least one collection device. The at least one collection device is configured to selectively schedule reception of the received signal characteristic based upon a timing of communications among the plurality of forward devices, and to determine a parameter associated with the uncooperative communications device based upon the received signal characteristic. Advantageously, the communication network leverages the existing plurality of mobile wireless communications devices to scout the uncooperative communications device.

In some embodiments, the communication network may further comprise a control device, and the at least one collection device may be configured to transmit the received signal characteristic to the control device. The control device may be configured to cooperate with the at least one collection device to determine the parameter associated with the uncooperative communications device based upon the received signal characteristic received from the at least one collection device.

More specifically, the control device may be configured to determine a plurality of parameters associated with the uncooperative communications device based upon the received signal characteristic received from the at least one collection device, the plurality of parameters comprising a location value, a movement value, and a transmission characteristic value, for example. Each forward device may be configured to transmit a respective locational value and time value associated with the received signal characteristic to the at least one collection device. In some embodiments, each forward device may comprise a plurality of diversity antennas and may be configured to detect the received signal characteristic associated with the uncooperative communications device using the plurality of diversity antennas.

Another aspect is directed to a method of operating a communication network uncooperative with an uncooperative communications device. The communication network comprises a plurality of mobile wireless communications devices comprising at least one collection device and a plurality of forward devices. The method comprises using each forward device to detect a received signal characteristic associated with the uncooperative communications device, and transmit the received signal characteristic to the at least one collection device. The method also includes using the at least one collection device to selectively schedule reception of the received signal characteristic based upon a timing of communications among the plurality of forward devices, and to determine a parameter associated with the uncooperative communications device based upon the received signal characteristic received from the at least one collection device.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic diagram of a communication network, according to the present invention.

FIG. 2 is a flowchart illustrating operation of the communication network of FIG. 1.

FIG. 3 is a schematic diagram illustrating time slot allocation in one embodiment of the communication network, according to the present invention.

FIG. 4 is a schematic diagram illustrating a timing sequence between devices in one embodiment of the communication network, according to the present invention.

FIG. 5 is a chart illustrating a simulation for an embodiment of the communication network, according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout.

Referring initially to FIGS. 1-2, a wireless communication system 10 comprising a communication network 16 according to the present invention is now described. Also, with reference to a flowchart 30, which begins at Block 31, a method of operating the communication network 16 is also described. The wireless communication system 10 illustratively includes an other communication network 20, uncooperative to the communication network 16, comprising an uncooperative communications device 21. Of course, the other communication network 20 may comprise a plurality of uncooperative communications devices. In other words, the communication networks 20, 16 are unfriendly with each other, i.e. they do not intentionally share communication channels.

The communication network 16 includes a control device 11, and a plurality of mobile wireless communications devices comprising a plurality of collection devices 12a-12b and a plurality of forward devices 15a-15g. For ease of illustration, only one forward device 15a and one collection device 12a are shown in detail. Of course, the other companion devices may be similarly constituted. The communication network 16 can include a wide variety of differing devices, such as handheld communications devices (e.g. walkie-talkies), vehicle mounted communications devices, and a base station device. The forward devices 15a-15g, collection devices 12a-12b, and control device 11 may perform multiple roles. For example, the collection devices 12a-12b can also function as a forward device 15a-15g in the communication network 16. In some embodiments, the control device 11 may also be a collection device 12a-12b and even a forward device 15a-15g. In other words, the collection/receiver devices can perform the functionality of multiple devices, and they are not limited to a single specific role.

Each forward device 15a-15g is configured to detect a received signal characteristic associated, i.e. regarding a signal emitted therefrom, with the uncooperative communications device 21 (Block 33). For example, the received signal characteristic may comprise one or more of a bandwidth value, an assigned time value, a frequency value, and a received signal strength value.

Once a received signal characteristic is detected, the forward device 15a-15g is configured to transmit the received signal characteristic to the collection device 12a (Block 35). In some embodiments, the forward device 15a-15g may be configured to detect the received signal characteristic by scanning an operative frequency of the respective forward device. In the illustrated embodiment, each forward device

15a-15g comprises a plurality of diversity antennas 19a-19b and is configured to detect the received signal characteristic associated with the uncooperative communications device 21 using the plurality of diversity antennas. The forward device 15a-15g scans each operative frequency for all the on-board antennas 19a-19b. Multiple antennas 19a-19b at a forward device 15a-15g could provide additional capability on bearing, amplitude, and other parameters.

Typically, the forward device 15a-15g transmits the data to 10 the collection device 12a in charge of the local subnet in the communication network 16, such as a master node (mobile ad hoc network embodiments) or base station. In some embodiments, the forward device 15a-15g may be configured to transmit a respective locational value and time value associated with the received signal characteristic to the collection device 12a-12b, i.e. the forward node time/date/location stamps the data.

As such, the collection device 12a is configured to selectively schedule detection or reception of the received signal 20 characteristic based upon a timing of communications among the plurality of forward devices 15a-15g. The collection device 12a is configured to schedule detection of the received signal substantially simultaneously for each of the forward devices 15a-15g, and to transmit the received signal characteristic to the control device 11 (Blocks 37-38). In the illustrated embodiment, the collection devices 12a-12b serve as a backbone of the communication network 16 and route the information to the control device 11 (Block 39). In other embodiments, the collection devices 12a-12b may each have a direct coupling to the control device 11. The collection devices 12a-12b may be configured to coordinate with forward devices 15a-15g in a respective subnet for cooperation with nearby other forward devices to detect the received signal characteristic associated with the uncooperative communications device 21.

For example, if a particular forward device 15a-15g cannot 30 perform detection processes due to significant communication demands by the respective user (e.g. reduced receive sensitivity due to ongoing transmissions), the collection device 12a-12b may offload the detection duties to nearby forward devices 15a-15f. The communication network 16 may address this situation with the control device 11 scheduling a coordinated detection in these locations when the forward device 15a-15g is known not to have any scheduled 40 transmissions or reception. An alternate approach is to task many forward devices 15a-15g to make the detection. If a forward device 15a-15g is "busy," then it quietly disregards the command. The collection node 12a-12b can still make the measurement of location, movement, other if enough forward nodes do act on the request.

In some embodiments, the plurality of forward devices 15a-15g may be configured to operate based upon a CSMA protocol, and each forward device may be configured to detect the received signal characteristic during an absence of 50 traffic directed thereto. In different embodiments (FIG. 3), the plurality of forward devices 15a-15g may be configured to operate based upon a TDMA protocol, and the collection device 12a-12b may be configured to assign a time slot for detection of the received signal characteristic associated with the uncooperative communications device 21. In other 60 embodiments, the forward devices 15a-15g may be configured to operate with a dedicated guard receiver separate from the communications receiver. In addition to a guard receiver, other systems may use multiple antennas.

In the illustrated embodiment, the collection device 12a includes a processor 13 and a memory 14 cooperating therewith. The processor 13 may be configured to store one or 65

more uncooperative communications device type features in the memory 14 and to correlate the received signal characteristic from the plurality of forward devices 15a-15g with at least one uncooperative communications device type feature. For example, the uncooperative communications device type feature may comprise a waveform feature characteristic or a transmission signal signature of some form. Advantageously, the control device 11 may store equipment correlations with uncooperative communications device types, thereby determining uncooperative equipment location data. Also advantageously, the forward device 15a-15g may store uncooperative communications device type features in memory and correlate against them. This may reduce the transmission bandwidth required in getting data/information from the forward nodes to the collection node.

In other embodiments, the forward devices 15a-15g and/or the collections devices 12a-12b may be configured to detect the received signal characteristic by sampling a received signal from the uncooperative communications device 21, and to transmit the sampled received signal data to an upstream collection device or the control device 11. In other words, the heavy processing burdens are shifted up the communication chain to devices that likely have greater resources.

In certain embodiments, the collection device 12a-12b may be configured to determine a plurality of received signal characteristics from the data received from the forward devices 15a-15g, such as a time of arrival value, and a Doppler value. In these embodiments, some pre-processing is performed by the collection devices 12a-12b before it is routed to the control device 11. The collection device 12a-12b aggregates the data it receives, and also calculates parameters based on the signals received (Block 36). These parameters can include TDOA, FDOA, amplitude differences, etc. It may also perform location estimation; however, this would typically be done at the control device 11.

The control device 11 is configured to determine one or more parameters associated with the uncooperative communications device 21 based upon the received signal characteristic received from the collection devices 12a-12b (Block 41). For example, the plurality of parameters may comprise a location value, a movement value, a transmission characteristic value, and/or an accompanying equipment parameter.

Additionally, the control device 11 is configured to determine a strategy parameter associated with the uncooperative communications device 21 and based upon the determined parameter. For example, the control device 11 may determine that associated users of the other communication network 20, i.e. the one or more uncooperative communications devices 21, may be strategically outmaneuvering users in the communication network 16. The control device 11 is configured to transmit the parameter and the strategy parameter to the plurality of mobile wireless communications devices 15a-15g, 12a-12b (Blocks 43, 45).

In some embodiments, the control device 11 can be omitted, and its functionality can be assigned to the most capable collection device 12a-12b. In these embodiments, the collection devices 12a-12b serve not only as the backbone of the communications network 16 but also the brain.

In some embodiments, the collection devices 12a-12b may arbitrate network time for simultaneous listening, perform signal correlation determination, perform time difference of arrival estimates, perform power difference of arrival estimates, perform frequency difference of arrival estimates, and forward results to next collection point. For the forward devices 15a-15g, in some embodiments, the devices may be configured to listen at an assigned time, frequency, and bandwidth, perform signal detection, perform signal evaluation if

assigned, provide a time stamp with global positioning system (GPS), and lastly send results to assigned collection node.

In some embodiments, the control device 11 may be configured to maintain a list of radios, including capability, location, and current search list for each forward device 15a-15g. The control device 11 can also be configured to serve as the final processing stage, which includes geolocation estimation, tracking algorithms, and other processing. The control device 11 may also be configured to manage results by updating search descriptions, assigning/changing collection points, and pushing results updates back to all nodes. In some embodiments, the command/control can be an external process or internal to the radio. In versatile applications, the command/control application can exist at any node in the communication network 16.

Advantageously, the communication network 16 leverages the existing plurality of mobile wireless communications devices 12a-12b, 15a-15g to scout the uncooperative communications device 21. For example, the users of the communication network 16 can be informed of hidden uncooperative communications device 21 users via the command/control backbone. The communication network 16 may determine location, density of personnel. Also, if the control device 11 is able to determine the type of device for the uncooperative communications device 21 (particularly when the communications device type can be associated with equipment), the control device can forward this information to nearby users in the communication network 16 for strategic reasons.

Another aspect is directed to a method of operating a communication network 16 uncooperative with an other communication network 20. The other communication network 20 comprises an uncooperative communications device 21. The communication network 16 comprises a control device 11, and a plurality of mobile wireless communications devices comprising a collection device 12a-12b and a plurality of forward devices 15a-15g. The method comprises using each forward device 15a-15g to detect a received signal characteristic associated with the uncooperative communications device 21, and transmit the received signal characteristic to the collection device 12a-12b, and using the collection device to selectively schedule detection of the received signal characteristic based upon a timing of communications among the plurality of forward devices, and to transmit the received signal characteristic to the control device. The method also includes using the control device 11 to determine a parameter associated with the uncooperative communications device 21 based upon the received signal characteristic received from the collection device 12a-12b.

Referring to FIG. 3, as will be appreciated by those skilled in the art, an exemplary implementation of the wireless communication system 10 is illustrated. There are many different kinds of network protocols. A brief description of TDMA and CSMA are shown as two examples.

TDMA Media Access Control (MAC) Protocol Network

Typical ad-hoc TDMA systems include a period of network arbitration slots followed by assigned data slots 51-54. Within each data slot, a predetermined radio is allowed to transmit. The pattern of arbitration and data slots is repeated over and over. This fundamental duration is called the epoch duration 50.

Each radio in the network arbitrates an assigned time slot to transmit. During the other allocated radio transmit slots, each radio will listen to the transmission for data that is addressed to them. The assignment of a data slot is controlled by the

MAC layer for the communications waveform. Typically, a single radio in the network acts as the arbitrator master of the time slots.

When a forward node receives a request for a communication location aware waveform (CLAW) signal detection, the CLAW application can try to listen on unused slots. This can be done on slots that are assigned to be empty or on slots when a signal is not detected after a brief amount of time. If slots are not open, requests that some number of slots be allocated for it and other nodes to use for a predetermined about of time can be made to the network arbitrator. Once the time has been granted, the assigned radio will listen at the desired frequency, bandwidth, and time as illustrated in FIG. 3.

For signal detection, this time can be relatively small. For signal geolocation, the time required will increase. If the allotted CLAW time duration is not sufficient for the signals for geolocation, a large number of slots 51-54 can be allocated (up to a complete epoch 50) for a brief period of time. The additional amount of data will need to be compressed prior to collection for correlation.

CSMA MAC Protocol Network

In the CSMA architecture, each unit sends a request to send (RTS) message to the desired receiving station for point-to-point transmissions. The receiving station acknowledges the RTS message with a clear to send (CTS) message. On receipt of a CTS message, the transmitting node transmits the data package. In some instances, the receiving node responds with a “done” message. If there is traffic on the channel or if the receiving station does not respond, the requesting transmitter goes into a random back off duration before attempting to transmit again.

For the CSMA protocol, the detection durations do not necessarily have to be coordinated. If there is traffic on the channel and it is not intended for the forward node, this node is free to scan other frequencies to detect signals of interest. If a channel is heavily utilized by a particular node, then it must prioritize time for scanning along with RX or TX data. This can be accomplished by not providing a CTS message for a prescribed time or holding off lower priority data packets.

However, the time and signal for geolocation will have to be coordinated. All forward nodes may need to be receiving at exactly the same time. The collection nodes are required to communicate the time and duration to the each of the respective forward nodes under its supervision.

If another radio tries to communicate with a radio that is servicing a CLAW search, the CSMA protocols will time out. It is helpful that the collection nodes understand the CSMA protocol such as to efficiently assign time without a large penalty in system throughput due to CSMA back off durations.

Sequence Diagram

Referring now to FIG. 4, a sequence diagram 60 illustratively includes the application node (control device 11 from hereinabove), the collection node (collection device 12a-12b from hereinabove), and the forward node(s) (forward devices 15a-15g from hereinabove), each are given a separate block. There can be many forward nodes in the configuration, and some nodes can perform multiple roles. For example, a collection node may also be a forward node. The application node may be a collection node or forward node as well. These nodes may reside anywhere in a network.

Simulation

Simulations were performed for a system looking for a predefined signal pattern. This pattern was stored in the forward nodes. The MAC search window was predefined and fixed. Each radio in the network searched for the signal by correlating the received signal to the known preamble. On

detecting the preamble, the time of the correlation was determined using a GPS signal. This time was logged. Offline, the times were post processed with only TDOA techniques. The target signals were placed at different locations around Rochester, N.Y. The TDOA measurements were taken at each location. The results are shown in the image 70 of FIG. 5. The circles 15a-15g are the locations of the forward nodes. The triangles show the location of the unknown transmitter (uncooperative communications devices 21a-21c). Each x-mark 72a-72n represents a single estimate based on a single observation of the unknown transmitter location.

Many modifications and other embodiments of the invention will come to the mind of one skilled in the art having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is understood that the invention is not to be limited to the specific embodiments disclosed, and that modifications and embodiments are intended to be included within the scope of the appended claims.

That which is claimed is:

1. A communication network uncooperative with an uncooperative communications device, the communication network comprising:

a plurality of mobile wireless communications devices comprising at least one collection device and a plurality of forward devices, each forward device configured to detect a received signal characteristic associated with the uncooperative communications device, the uncooperative communications device and said plurality of mobile wireless communications devices not sharing a communication channel, transmit the received signal characteristic to said at least one collection device; said at least one collection device configured to selectively schedule listening for the received signal characteristic based upon a timing of communication transmissions among adjacent forward devices, and determine a parameter associated with the uncooperative communications device based upon the received signal characteristic received from said at least one collection device.

2. The communication network of claim 1 further comprising a control device; wherein said at least one collection device is configured to transmit the received signal characteristic to said control device; and wherein said control device is configured to cooperate with said at least one collection device to determine the parameter associated with the uncooperative communications device based upon the received signal characteristic received from said at least one collection device.

3. The communication network of claim 1 wherein the parameter comprises at least one of a location value, a movement value, and a transmission characteristic value.

4. The communication network of claim 1 wherein each forward device is configured to transmit a respective locational value and time value associated with the received signal characteristic to said at least one collection device.

5. The communication network of claim 1 wherein each forward device is configured to detect the received signal characteristic by scanning an operative frequency of the respective forward device.

6. The communication network of claim 1 wherein said at least one collection device comprises a processor and a memory cooperating therewith; and wherein said processor is configured to store an uncooperative communications device type feature in said memory and to correlate the received

signal characteristic from said plurality of forward devices with the uncooperative communications device type feature.

7. The communication network of claim **1** wherein each forward device is configured to detect the received signal characteristic by sampling a received signal from the uncooperative communications device, and to transmit the sampled received signal data to said at least one collection device.

8. The communication network of claim **2** wherein said control device is configured to:

- determine a strategy parameter associated with the uncooperative communications device and based upon the parameter; and
- transmit the parameter and the strategy parameter to said plurality of mobile wireless communications devices.

9. The communication network of claim **1** wherein said at least one collection device is configured to determine a plurality of received signal characteristics comprising a time of arrival value, and a Doppler value from the received signal characteristic from said plurality of forward devices.

10. The communication network of claim **1** wherein each forward device comprises a plurality of diversity antennas and is configured to detect the received signal characteristic associated with the uncooperative communications device using the plurality of diversity antennas.

11. The communication network of claim **1** wherein said plurality of forward devices is configured to operate based upon a time division multiple access (TDMA) protocol; and wherein said at least one collection device is configured to selectively schedule the listening for the received signal characteristic based upon the timing of communication transmissions among the adjacent forward devices using an assigned slot.

12. The communication network of claim **1** wherein said plurality of forward devices is configured to operate based upon a Carrier Sense Multiple Access (CSMA) protocol; and wherein each forward device is configured to detect the received signal characteristic during an absence of traffic directed thereto.

13. A communication network uncooperative with an uncooperative communications device, the communication network comprising:

- a control device; and
- a plurality of mobile wireless communications devices comprising at least one collection device and a plurality of forward devices, the uncooperative communications device and said plurality of mobile wireless communications devices not sharing a communication channel, each forward device configured to detect a received signal characteristic associated with the uncooperative communications device, and

- transmit the received signal characteristic, and a respective locational value and time value associated with the received signal characteristic to said at least one collection device;

- said at least one collection device configured to selectively schedule listening for the received signal characteristic based upon a timing of communication transmissions among adjacent forward devices, and to transmit the received signal characteristic to said control device;

- said control device configured to determine a plurality of parameters associated with the uncooperative communications device based upon the received signal characteristic received from said at least one collection device, the plurality of parameters comprising at least one of a location value, a movement value, and a transmission characteristic value.

14. The communication network of claim **13** wherein each forward device is configured to detect the received signal characteristic by scanning an operative frequency of the respective forward device.

15. The communication network of claim **13** wherein said at least one collection device comprises a processor and a memory cooperating therewith; and wherein said processor is configured to store an uncooperative communications device type feature in said memory and to correlate the received signal characteristic from said plurality of forward devices with the uncooperative communications device type feature.

16. The communication network of claim **13** wherein each forward device is configured to detect the received signal characteristic by sampling a received signal from the uncooperative communications device, and to transmit the sampled received signal data to said at least one at least one collection device.

17. The communication network of claim **13** wherein said control device is configured to:

- determine a strategy parameter associated with the uncooperative communications device and based upon the parameter; and
- transmit the parameter and the strategy parameter to said plurality of mobile wireless communications devices.

18. The communication network of claim **13** wherein said at least one collection device is configured to determine a plurality of received signal characteristics comprising a time of arrival value, and a Doppler value from the received signal characteristic from said plurality of forward devices.

19. A method of operating a communication network uncooperative with an uncooperative communications device, the communication network comprising a plurality of mobile wireless communications devices comprising at least one collection device, and a plurality of forward devices, the uncooperative communications device and the plurality of mobile wireless communications devices not sharing a communication channel, the method comprising:

- detecting, using each forward device, a received signal characteristic associated with the uncooperative communications device, and transmitting the received signal characteristic to the at least one collection device;
- selectively scheduling, using the at least one collection device, listening for the received signal characteristic based upon a timing of communication transmissions among adjacent forward devices; and

- determining, using the at least one collection device, a parameter associated with the uncooperative communications device based upon the received signal characteristic.

20. The method of claim **19** wherein the communication network further comprises a control device; further comprising:

- transmitting, using the at least one collection device, the received signal characteristic to the control device; and the control device and the at least one collection device cooperating with each other to determine the parameter associated with the uncooperative communications device based upon the received signal characteristic received from the at least one collection device.

21. The method of claim **19** wherein the parameter comprises at least one of a location value, a movement value, and a transmission characteristic value.

22. The method of claim **19** further comprising transmitting, using each forward device, a respective locational value and time value associated with the received signal characteristic to the at least one collection device.

11

23. The method of claim **19** further comprising detecting, using each forward device, the received signal characteristic by scanning an operative frequency of the respective forward device.

24. The method of claim **19** further comprising storing, using the at least one collection device, an uncooperative communications device type feature in a memory and correlating the received signal characteristic from the plurality of forward devices with the uncooperative communications device type feature.

25. The method of claim **19** further comprising detecting, using each forward device, the received signal characteristic by sampling a received signal from the uncooperative communications device, and transmitting the sampled received signal data to the at least one collection device.

26. The method of claim **19** further comprising:
determining a strategy parameter associated with the uncooperative communications device and based upon the parameter; and
transmitting the parameter and the strategy parameter to the plurality of mobile wireless communications devices.

27. The method of claim **19** further comprising determining a plurality of received signal characteristics comprising a time of arrival value, and a Doppler value from the received signal characteristic from the plurality of forward devices.

28. The method of claim **19** wherein each forward device comprises a plurality of diversity antennas; and further com-

12

prising detecting the received signal characteristic associated with the uncooperative communications device using the plurality of diversity antennas.

29. The method of claim **19** further comprising:
operating the plurality of forward devices based upon a time division multiple access (TDMA) protocol; and
assigning a time slot for selectively scheduling the listening for the received signal characteristic based upon the timing of communication transmissions among the adjacent forward devices using the at least one collection device.

30. The method of claim **19** further comprising:
operating the plurality of forward devices based upon a Carrier Sense Multiple Access (CSMA) protocol; and
detecting the received signal characteristic during an absence of traffic directed thereto using each forward device.

31. The communication network of claim **1** wherein said at least one collection device is configured to selectively schedule simultaneous listening using the adjacent forward devices for the received signal characteristic.

32. The communication network of claim **1** wherein said at least one collection device is configured to selectively schedule the listening based upon a transmission data load of a respective forward device.

* * * * *

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

FREDDY MARTINEZ,)
Plaintiff,)
v.) No. 2014 CH 09565
CHICAGO POLICE DEPARTMENT,)
Defendant.)

**DEFENDANT'S NOTICE OF SUPPLEMENTAL PRODUCTION
IN RESPONSE TO FOIA REQUEST**

Defendant Chicago Police Department (“CPD”), by its counsel, Drinker Biddle & Reath LLP, submits this notice of supplemental production in response to Plaintiff Freddy Martinez’s FOIA request that is the subject of the present dispute.

On March 24, 2014, CPD received a FOIA request from Mr. Martinez seeking “all records under a Freedom of Information Act Request for any information about ‘IMSI catchers.’” *See Mot. to Dismiss, Ex. 1-A.* That ambiguous and vague request was clarified by the sentence that immediately followed, which stated, “I am specifically writing for any purchase orders for any equipment that could be used to intercept GSM or CDMA (cell phone) communication.” *See id.* CPD correctly interpreted Mr. Martinez’s request for the “specific” purchase orders identified, and responded to Mr. Martinez’s specific request for purchase orders by producing two invoices and one quotation. *See id.* at Ex. 1 (Aff. of Officer Jack Enter) and Ex. 1-B.

On the basis of that request and response, Mr. Martinez filed the instant Complaint on June 6, 2014, which alleged that CPD willfully violated FOIA. CPD subsequently moved to dismiss the Complaint, as it had responded to Mr. Martinez’s FOIA request by producing the

public records reasonably identified by Mr. Martinez's request. The parties have now fully briefed CPD's pending motion to dismiss the Complaint and the Court is set to rule on that motion on December 11, 2014. *See Order entered Nov. 17, 2014.*

Subsequent to the filing of the Complaint in this action, Mr. Martinez submitted a number of other FOIA requests to CPD relating to IMSI catcher or cell phone technology, including the following requests: June 30, 2014 (Request No. 14-2787); July 25, 2014 (Request No. 14-3248); August 12, 2014 (Request No. 14-3603); September 2, 2014 (Request No. 14-3982); September 18, 2014 (Request No. 14-4288); and November 13, 2014 (Request No. 14-5298). While searching for documents responsive to Mr. Martinez's other FOIA requests, CPD discovered seven additional pages of documents that are responsive to the FOIA Request at issue in this case. CPD produced those documents to Mr. Martinez via an email to his counsel on December 8, 2014. *See Ex. A.*

The seven additional responsive pages discovered by CPD include a one-page purchase order related to the invoice for StingRay II and AmberJack equipment that CPD originally produced in response to Mr. Martinez's FOIA request. *Compare Ex. A at 1, with Mot. to Dismiss, Ex. 1-B at 3.* The remaining six pages of documents include an invoice and purchase order from a 2010 transaction, and four pages comprised of two quotes and two "request for purchase requisitions" from a 2005 transaction. *See Ex. A at 4-9.*

CPD's supplemental production of responsive documents underscores the reasonableness of its response to Plaintiff's FOIA request and its good faith. The original search for responsive records commissioned by CPD was reasonable and discovered responsive documents. *See SafeCard Servs., Inc. v. S.E.C.*, 926 F.2d 1197, 1201 (D.C. Cir. 1991); *Williams v. Fanning*, No. 13 CV 0968, 2014 WL 3900603, *5 (D.D.C. Aug. 11, 2014) ("That these searches in fact located

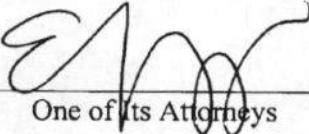
records related to [the plaintiff's] discharge underscores the adequacy and reasonableness of the searches."); Mot. to Dismiss Ex. 1 (detailing the steps taken by CPD Officer Jack Enter to respond to Mr. Martinez's FOIA request). After CPD uncovered additional responsive documents while conducting reasonable searches for records responsive to Mr. Martinez's later FOIA requests, CPD produced those responsive documents to Mr. Martinez through counsel. Thus, while CPD wanted to bring this additional production to the Court's attention in advance of the ruling date on the motion to dismiss, the additional production does not change the fact that CPD's original search for records responsive to Mr. Martinez's request was reasonable. Accordingly, the Court should dismiss Mr. Martinez's Complaint.

Dated: December 9, 2014

Respectfully submitted,

CHICAGO POLICE DEPARTMENT

By:


One of its Attorneys

Daniel J. Collins (6224698)
Jeffrey D. Perconte (6280852)
Elizabeth V. Lopez (6293255)

DRINKER BIDDLE & REATH LLP

191 N. Wacker Dr., #3700
Chicago, IL 60606
312.569.1000

Daniel.Collins@dbr.com
Jeff.Perconte@dbr.com
Elizabeth.Lopez@dbr.com
Firm ID 41748

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 4 of 13

Exhibit A

Lopez, Elizabeth V.

From: Lopez, Elizabeth V.
Sent: Monday, December 08, 2014 5:28 PM
To: Matt Topic (matt@loevy.com)
Cc: Perconte, Jeff; Collins, Daniel J.
Subject: Martinez I
Attachments: Martinez I_12_8_14 Ltr to M Topic re supplemental production.pdf; 11-1161 Responsive Documents.pdf

Dear Matt,

Please see the attached correspondence and enclosure.

Sincerely,

Elizabeth

Elizabeth V. Lopez
Drinker Biddle & Reath LLP
191 N. Wacker Dr., Ste. 3700
Chicago, IL 60606-1698
(312) 569-1439 office
(312) 569-3439 fax
Elizabeth.Lopez@dbr.com
www.drinkerbiddle.com

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-5238
PAGE 5 of 3

Elizabeth V. Lopez
312-569-1439 Direct
312-569-3439 Fax
elizabeth.lopez@dbr.com

Law Offices

191 N. Wacker Drive
Suite 3700
Chicago, IL
60606-1698

(312) 569-1000
(312) 569-3000 fax
www.drinkerbiddle.com

CALIFORNIA
DELAWARE
ILLINOIS
NEW JERSEY
NEW YORK

PENNSYLVANIA
WASHINGTON D.C.
WISCONSIN

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 6 of 13

December 8, 2014

BY E-MAIL

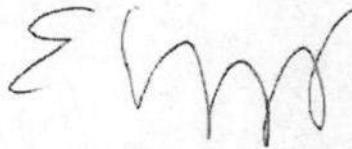
Matthew Topic
Loevy & Loevy
312 N. May Street, Ste. 100
Chicago, IL 60607

Re: *Freddy Martinez v. Chicago Police Department - Case No. 2014-CH-09565*

Dear Matt:

Enclosed please find seven pages of additional documents responsive to Mr. Martinez's FOIA Request No. 14-1161 that the Chicago Police Department recently discovered in the course of responding to Mr. Martinez's other FOIA requests.

Very truly yours,



Elizabeth V. Lopez

Enclosures

cc: Daniel J. Collins
Jeff Perconte

ACTIVE/ 78144060.1

**Chicago Police Department
Organized Crime Division**

PURCHASE ORDER

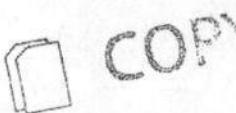
DATE: 3/9/2009
P.O. # 15457

3340 W. Fillmore Ave.
Chicago, IL 60624
Phone: 312-747-7922
james.washburn@chicagopolice.org

Delivery date = 7/9/09

VENDOR
Harris Corporation
Wireless Products Group
P.O. Box 9800
Melbourne, FL 32902-9800
800-358-5297

SHIP TO:
Sgt. James Washburn
Chicago Police Department
3340 W. Fillmore Ave.
Chicago, IL 60624
312-746-7922



SHIPPING METHOD	DELIVERY DATE	SHIPPING TERMS
	ASAP	

ITEM #	DESCRIPTION	QTY	UNIT PRICE	TOTAL
STINGRAY II-UP	StingRay II Upgrade	1	65,000.00	65,000.00
STINGRAY II-IDEN-SW	StingRay II IDEN software Package	1	22,000.00	22,000.00
PA-KIT-30W IDEN 800	PA-KIT-30W Single Band IDEN 800	1	14,000.00	14,000.00
PA-KIT-30W DUAL BAND	PA-KIT-30W Dual-Band Conus 850/900	1	17,500.00	17,500.00
PA-KIT-30W 2100	PA-KIT-30W Single Band 2100 mHz	1	16,000.00	16,000.00
AJ-W-UG	AmberJack-X or G to AmberJack-W	1	18,000.00	18,000.00
SUPERDOG	Handheld Passive DF Tool	1	12,000.00	12,000.00

Other Comments or Special Instructions:

Per our discussion with Lin Vinson, a "loaner" Sting Ray II will be supplied while our StingRay is being upgraded

SUBTOTAL \$ 164,500.00
TAX RATE NA
TAX

TOTAL \$ 164,500.00

Sergeant James Washburn #1765
Authorized by

9-Mar-09

If you have any questions about this purchase order, please contact
[Name, Phone #, E-mail, Phone, Fax]



HARRIS CORP - WIRELESS PRODUCTS GROUP
P.O. BOX 9800, M/S R5-11A
MELBOURNE, FL 32902-9800
PH: 800-358-5297, FAX: 321-309-7437, wpg@harris.com

Invoice	INV6779-02738
Date	12/14/2010
Page:	1

Invoice

Bill To:
Chicago Police Bureau of Investigative Services James Washburn 3340 W. Fillmore Ave. james.washburn@chicagopolice.org Chicago IL 60624

Ship To:
Chicago Police Department Attn: Sgt. James Washburn 3340 W. Fillmore Ave. 1-312-746-7922 Chicago IL 60624

Purchase Order No.	Customer ID	Salesperson	Shipping Method	Pmt Terms	Req Ship Date	Harris Ord No.	
10152	CPB-CHGIL-001	WPG3	BEST WAY	Net 30	2/2/2011	ORD6779-01635	
Ordered	Shipped	B/O	Item Number	Description	Discount	Unit Price	Ext. Price
1	1		KINGFISH 601	KingFish Serial Number		\$27,800.00	\$27,800.00
1	1		KF-CDMA-SW 601	KingFish CDMA Software Package Serial Number		\$18,100.00	\$18,100.00
1	1		KF-GSM-SW 601	KingFish GSM Software Package Serial Number		\$18,100.00	\$18,100.00
1	1		KF-iDEN-SW 601	KingFish iDEN Software Package Serial Number		\$18,100.00	\$18,100.00
1	1		2014069-101 601	Rugged Mini-PC Controller (GD Go Book) Serial Number		\$5,500.00	\$5,500.00
1	1		PA-KIT-25W-CONUS S/N: 1123	High Powered Filtered 25W PA Kit-800/85		\$11,500.00	\$11,500.00
1	1		CONV-2100/1700-W/BF S/N: 1027	Band IV - AWS Converter - CONUS		\$19,800.00	\$19,800.00
1	1		AJ-W 488	AmberJack Wide Band DF Antenna Serial Number		\$38,400.00	\$38,400.00

All above items received in good working order.

X

Remit Payment To:

Electronic Funds Transfer (EFT): REDACTED	GCSD Mail Deposits: REDACTED	GCSD Overnight Deliveries: REDACTED
--	---------------------------------	--

Please reference the Invoice number with your payment.

Subtotal	\$157,300.00
Deposit	\$0.00
Misc	\$0.00
Tax	\$0.00
Freight	\$0.00
Trade Discount	\$0.00
Purchase Price	\$157,300.00

**Chicago Police Department
Organized Crime Division**

PURCHASE ORDER

DATE: 11/4/2010
P.O. # 10152

3340 W. Fillmore Ave.
Chicago, IL 60624
Phone: 312-747-7922
james.washburn@chicagopolice.org

VENDOR
Harris Corp - Wireless Products Group
p.o. Box 9800 M/S R5-11A
Melbourne, FL
32902-9800
800-358-5297

SHIP TO
Sgt. James Washburn
Chicago Police Department
3340 W. Fillmore Ave.
Chicago, IL 60624
312-746-7922

SHIPPING METHOD	DELIVERY DATE	SHIPPING TERMS
	ASAP	

ITEM #	DESCRIPTION	QTY	UNIT PRICE	TOTAL
King Fish	King Fish	1	27,800.00	27,800.00
KF-CDMA-SW	King Fish CDMA Software Package	1	18,100.00	18,100.00
KF-GSM-SW	King Fish GSM Software Package	1	18,100.00	18,100.00
KF-IDEN-SW	King Fish iDEN Software Package	1	18,100.00	18,100.00
2014069-101	Rugged Mini-PC Controller (Go Book)	1	5,500.00	5,500.00
PA-KIT-25W-CONUS	High Powered 25W PA Kit	1	11,500.00	11,500.00
CONV-2100/1700-W/BP	Bond 1V-AWS Converter-CONUS	1	19,800.00	19,800.00
AJ-W	Amber Jack Wide Band DF Antenna	1	38,400.00	38,400.00
				-
				-
				-
				-

SUBTOTAL \$ 157,300.00

TAX RATE NA

Shipping

TOTAL \$157,300.00

Other Comments or Special Instructions

All Equipment per quote# QTE6779-02485
Training Included on Site at Homan Square

Sergeant James Washburn #1765

Authorized by

04 Nov. 2010

If you have any questions about this purchase order, please contact
Sgt. James Washburn, 312-746-7922, FAX 312-746-7278

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 9 of 13



3630 Commercial Ave, Northbrook, IL 60062
Phone : 847-272-6160 Fax : 847-272-8465

QUOTE: 101617-000

Date: 10/13/05

Customer No:	PO #:			
Sales person:	DH	Cust Ref:	Proj Ref:	
Name:	CITY OF CHICAGO-CPD		Ship To:	CITY OF CHICAGO-CPD
Attention:	MIKE FALATOVICS		MIKE FALATOVICS	
Address:	3510 S. MICHIGAN AVE. CHICAGO IL 60653		3510 S. MICHIGAN AVE. CHICAGO IL 60653	
Phone:	312-745-5777		312-745-5777	
Email:	michael.falatovics@chicagopolice.org			
Shipvia:	DROP SHIP Partial:			

Qty	Part No.	Vendor Part #	Description	Unit Price	Extention
1		SRAY-GSM-SW	GSM S/W FOR STINGRAY	21,000.00	21,000.00
1		TARPON	GEOLOCATION SOFTWARE	3,675.00	3,675.00
1		TRAIN-EC	TRAINING - EAST COAST	5,775.00	5,775.00

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 10 of 13

Total : 30,450.00

All prices Net Cash pre pay FOB Northbrook, Illinois, unless otherwise written agreed terms are established with us. Prices valid 21 days from date of quote and are based upon purchase of complete package quoted NOT isolated components. Please phone for alternative quotes. Failure to accept delivery of ordered items will result in a restocking fee of \$50.00 or 25% of retail price of each item whichever is greater. Above price does not include any applicable sales tax, not liable for unintentional inaccuracies and typographical or other errors.

Customer Signature : _____

Print date: 10/14/05



3630 Commercial Ave, Northbrook, IL 60062
Phone : 847-272-6160 Fax : 847-272-8465

JOTE: 101619-000

st No:	PO #:	Date:	10/13/05
les person:	DH	Cust Ref:	Proj Ref:
me:	CITY OF CHICAGO-CPD	Ship To:	CITY OF CHICAGO-CPD
ention:	MIKE FALATOVICS		MIKE FALATOVICS
dress:	3510 S. MICHIGAN AVE. CHICAGO	IL	60653
one:	312-745-5777		312-745-5777
nail:	michael.falatovics@chicagopolice.org		
ipvia:	DROP SHIP	Partial:	

Qty	Part No.	Vendor Part #	Description	Unit Price	Extention
1	DF45		DF45 DRIVE DOWN SYSTEM	19,425.00	19,425.00
1	DRT1000/DEX1		DIGITAL EXCITER MODULE	7,350.00	7,350.00
1	DRT1000/TEX1		TRANSMITTER EXCITER MODULE	12,075.00	12,075.00

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 12 of 13

Total : 38,850.00

Prices Net Cash pre pay FOB Northbrook, Illinois, unless otherwise written agreed terms are established with us. Prices valid 21 days from date shown. They are based upon purchase of complete package quoted NOT isolated components. Please phone for alternative quotes. Failure to accept all ordered items will result in a restocking fee of \$50.00 or 25% of retail price of each item whichever is greater. Above price does not include any applicable sales tax. not liable for unintentional inaccuracies and typographical or other errors.

Customer Signature : _____

Print date: 10/14/05

Request for Purchase Requisition

Information Services Division

Unit #125 - Bureau of Administrative Services

Requested by: Mike Falatovics

Date
10/15/2005

TRACKING/PR# 968

\$38,850.00 Total

158

Vendor 55

Vendor Phone

Account No. _____ Other Funding Info: _____
Charge Activity ACR Contract
Sub-Activity _____ 0

Note: Equipment for Organized Crime, Cellular Telephone Tracking
Use SOS funds - see attached

Equipment for Organized Crime, Cellular Telephone Tracking
Joe 1505 funds - See attached "To-From"

I hereby certify that the article(s) or service(s) requested herein are necessary to properly conduct the activities of this Department.

W. S. Parker

The Death of David Koschman

Report of the Special Prosecutor

Dan K. Webb

Winston & Strawn, LLP
September 18, 2013

Exhibit 1-AJ

Note To The Reader

On September 18, 2013, this Report was submitted to the Honorable Michael P. Toomin and was placed under temporary seal by the Court until the case of *People v. Vanecko* concluded.

On January 31, 2014, Mr. Vanecko waived his trial rights and pled guilty to the charge of involuntary manslaughter in connection with the death of David Koschman. Thereafter, the Special Prosecutor moved the Court to lift the temporary seal of the Report, and on February 3, 2014, the Court granted the Special Prosecutor's motion.

The Report was publicly released on February 4, 2014.

TABLE OF CONTENTS

I.	Mandate of the Special Prosecutor	1
II.	Summary of Final Conclusions of the Special Prosecutor's Investigation.....	2
A.	Issue One: Whether Criminal Charges Should be Brought Against Any Person in Connection with Koschman's Homicide	2
B.	Issue Two: Whether, From 2004 to the Present, Employees of the Chicago Police Department and the Cook County State's Attorney's Office Acted Intentionally to Suppress and Conceal Evidence, Furnish False Evidence, and Generally Impede the Investigation Into Koschman's Death	2
1.	Applicable State Law Crimes	2
2.	Burden of Proof.....	3
3.	Background on the Law of Criminal Intent (Scienter)	4
C.	The Events of 2004: Evaluating Whether Employees of CPD and SAO Violated Illinois Criminal Law	5
1.	Prosecution is Barred by the Applicable Statute of Limitations.....	5
D.	The Events of 2011-2012: Evaluating Whether Employees of CPD and SAO Violated Illinois Criminal Law	5
1.	The Events of 2011-2012: Prosecution Is Not Barred by the Applicable Statute of Limitations	5
2.	The Events of 2011-2012: Insufficient Evidence to Prove Beyond a Reasonable Doubt the Element of Criminal Intent (Scienter)	5
E.	Evidence Supporting the Decision to Appoint a Special Prosecutor.....	6
III.	Overview of the Special Prosecutor's Investigation	6
IV.	Detailed Discussion of the Evidence	9
A.	Overview of the 2004 Incident on Division Street	9
B.	The 2004 CPD Investigation of the Incident	13
1.	Early Morning Hours of April 25, 2004	13
2.	The Area 3 Investigation.....	17

a.	Assigning the Koschman Matter.....	17
b.	Investigative Steps Taken by Det. O'Leary and Det. Clemens on April 25, 2004	19
c.	Certain Issues Stemming from Area 3's Initial Work	24
i.	Assignment of Detectives on Furlough.....	24
ii.	Canvass for Additional Witnesses and Evidence.....	27
d.	Koschman's Death and Assignment of Detective Yawger.....	29
e.	Detective Yawger's Investigation.....	32
f.	Certain Issues Stemming from Area 3's Continuing Work	45
3.	May 20, 2004 (the Lineups).....	46
a.	Timing and Need for Lineups	46
b.	The Lineups	48
4.	May 20, 2004 (Felony Review Visit)	51
a.	SAO Felony Review Unit Contacted.....	53
b.	O'Brien's Interviews of Witnesses	56
c.	The Charging Decision	58
i.	O'Brien's Standard for Approving Charges	58
ii.	Issues Allegedly Preventing Charges.....	60
(A)	Supposed Lack of Witness Identification of the Offender	60
(B)	O'Brien's Evaluation of Self-Defense	61
d.	Felony Review Folder.....	66
5.	Press Inquiries	69
6.	Det. Yawger Meets with Nanci Koschman and Her Lawyer.....	71
7.	Det. Yawger Submits His Reports	72
C.	The 2011 CPD Re-investigation	74

1.	January 4, 2011, Sun-Times FOIA Request	74
2.	Reassignment to Area 5 Detectives	76
3.	Area 5's Investigation.....	80
4.	Draft Reports.....	88
5.	February 28, 2011	94
6.	Case Officially Closed.....	101
7.	The Missing CPD Koschman Homicide File.....	105
a.	Creating and Maintaining Homicide Files at Area 3	105
b.	The Various Versions of the Koschman Homicide File	107
i.	Commander Yamashiroya's Credenza File	107
ii.	Original Koschman Homicide File (Blue Three-Ring Binder)	108
iii.	Det. Yawger's "Working File"	114
iv.	Det. Clemens' Discovery	117
v.	Det. Gilger and Det. Spanos Review the Homicide Files "Discovered" by Lt. Walsh and Det. Yawger	119
D.	CPD 2011 Re-investigation and the Mayor's Office.....	120
E.	SAO's Involvement in 2011 and 2012.....	128
1.	Press Inquiries	128
2.	March 3, 2011 Meeting with CPD.....	132
3.	State's Attorney Alvarez Calls for an Independent Investigation	133
4.	State's Attorney's Office's Response to the Petition for the Appointment of a Special Prosecutor	141
V.	Legal Analysis	143
A.	Three Levels of Scienter (State of Mind): Recklessness, Knowledge, and Intent	143
1.	Recklessness	143

2.	Knowledge	144
3.	Intent	144
B.	Sciencer (State of Mind) Requirements of Relevant Criminal Statutes	144
C.	Prosecution of Conduct Committed in 2004 is Barred by the Statute of Limitations	146
1.	Public Misconduct	147
2.	Out-of-State Residency.....	147
3.	Continuous Conduct.....	147
4.	Conspiracy	148
a.	Evidence of a Conspiracy in 2004 with a Limitations Period Tolled by Subsequent Overt Acts	149
b.	Evidence of a Conspiracy Spanning Both 2004 and 2011.....	150
D.	The Events of 2011-2012: Evaluating Whether Employees of CPD and SAO Violated Illinois Criminal Law	151
1.	Prosecution is Not Barred by the Applicable Statute of Limitations.....	151
2.	Summary of the Evidence from 2011-2012 Which Was Thoroughly Reviewed for Potential Criminal Charges	151
a.	Whether CPD's 2011 Determination that Vanecko Acted In Self-Defense Was Criminal Misconduct	152
i.	Det. Gilger and Det. Spanos	152
ii.	Dept. Chief Andrews, Cmdr. Salemme and Sgt. Cirone.....	154
iii.	The Special Prosecutor's Decision Not to Seek Charges Against Det. Gilger, Det. Spanos, Dept. Chief Andrews, Cmdr. Salemme, and Sgt. Cirone	154
b.	Whether the Facts and Circumstances Surrounding Lt. Walsh's 2011 Discovery of the Missing CPD Original Koschman Homicide File Amount to Criminal Misconduct	156
i.	Lt. Walsh's Discovery of the Original Koschman Homicide File (Blue Three-Ring Binder)	157

ii.	The Special Prosecutor's Decision Not to Seek Charges Against Lt. Walsh	158
c.	The Special Prosecutor's Decision Not to Seek Charges Against Any Employee of SAO.....	160
VI.	Conclusion	160
VII.	Winston & Strawn Investigative Personnel	162

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 7 of 169

I. MANDATE OF THE SPECIAL PROSECUTOR

On April 23, 2012, Judge Michael P. Toomin appointed Dan K. Webb, Chairman of Winston & Strawn LLP, and former United States Attorney for the Northern District of Illinois, as the Special Prosecutor in the Matter of the Death of David Koschman.

In doing so, Judge Toomin ordered that the Special Prosecutor investigate two distinct issues related to the Koschman matter:

Issue One

[W]hether criminal charges should be brought against any person in connection with the homicide of David Koschman in the spring of 2004[.]¹

Issue Two

[W]hether, from 2004 to the present, employees of the Chicago Police Department and the Cook County State's Attorney's Office acted intentionally to suppress and conceal evidence, furnish false evidence, and generally impede the investigation into Mr. Koschman's death.²

Judge Toomin further ordered that "at the conclusion of his investigation, the Special Prosecutor shall submit a final report to this Court and for the benefit of the Cook County Board of Commissioners detailing the progress and ultimate results of the investigation and any criminal prosecutions commenced."³

Therefore, the Special Prosecutor, having concluded his investigation, submits this report to the Court which, in the pages that follow, describes in detail the ultimate results of the investigation undertaken pursuant to the judicial mandate set forth above.

¹ See Special Grand Jury Exhibit 5 (Order by J. Toomin (Apr. 23, 2012)).

² See Special Grand Jury Exhibit 5 (Order by J. Toomin (Apr. 23, 2012)).

³ See Special Grand Jury Exhibit 5 (Order by J. Toomin (Apr. 23, 2012)).

II. SUMMARY OF FINAL CONCLUSIONS OF THE SPECIAL PROSECUTOR'S INVESTIGATION

A. Issue One: Whether Criminal Charges Should be Brought Against Any Person in Connection with Koschman's Homicide

On December 3, 2012, the Special Prosecutor, after having thoroughly investigated whether criminal charges should be brought against any person in connection with the homicide of David Koschman in the spring of 2004, sought, and the special grand jury returned, an indictment against Richard J. (“RJ”) Vanecko charging him with involuntary manslaughter in connection with Koschman’s death. According to the trial court, the Vanecko trial is expected to commence in early 2014. With the indictment of Vanecko, the Special Prosecutor has satisfied the Court’s mandate to determine whether criminal charges should be brought in connection with Koschman’s death.

B. Issue Two: Whether, From 2004 to the Present, Employees of the Chicago Police Department and the Cook County State’s Attorney’s Office Acted Intentionally to Suppress and Conceal Evidence, Furnish False Evidence, and Generally Impede the Investigation Into Koschman’s Death

1. Applicable State Law Crimes

The Special Prosecutor, while conducting his assessment as to whether employees of the Chicago Police Department (“CPD”) and the Cook County State’s Attorney’s Office (“SAO”) acted intentionally to suppress and conceal evidence, furnish false evidence, and generally impede the investigation into Koschman’s death, first had to determine what Illinois criminal state law violations could potentially stem from such conduct, assuming the evidence could ultimately substantiate such a charge.⁴ With that in mind, the Special Prosecutor primarily evaluated the following four Illinois criminal violations: (1) official misconduct; (2) obstructing justice; (3) conspiracy; and (4) tampering with public records – each of which has a three-year statute of limitations.⁵ Under Illinois law, no prosecution can be commenced against any

⁴ The Special Prosecutor emphasizes that his evaluation was limited to Illinois state law violations only, as he lacks jurisdiction in connection with potential federal criminal law violations.

⁵ Official misconduct (720 ILCS 5/33-3) (West 2013); obstructing justice (720 ILCS 5/31-4) (West 2013); conspiracy (720 ILCS 5/8-2) (West 2013); and tampering with public records (720 ILCS 5/32-8) (West 2013). The Special Prosecutor further evaluated the potential for “organizational” criminal liability against state and municipal law enforcement agencies, such as CPD and SAO, in connection with failing to properly investigate a criminal matter, but found no applicable state law statutes.

individual under these statutes if the final act in commission of the crime occurred more than three years ago.⁶

2. Burden of Proof

Constitutional due process rights require that a person may not be convicted of a crime unless the prosecution meets its burden of proving all the elements of the charged offense beyond a reasonable doubt, including the applicable criminal intent (also known as “scienter”).⁷ In Illinois, the prosecution’s burden is explained to jurors as follows:

The defendant is presumed to be innocent of the charge against him. This presumption remains with him throughout every stage of the trial and during your deliberations on the verdict and is not overcome unless from all the evidence in this case you are convinced beyond a reasonable doubt that he is guilty.

The State has the burden of proving the guilt of the defendant beyond a reasonable doubt, and this burden remains on the State throughout the case. The defendant is not required to prove his innocence.⁸

The burden of proving all elements of a crime beyond a reasonable doubt is widely recognized as a “heavy” burden of proof.⁹ Additionally, under applicable ethical standards, a

⁶ The applicable statute of limitations, 720 ILCS 5/3-5 (West 2013), requires that prosecution for the offenses listed above “must be commenced within 3 years after the commission of the offense if it is a felony, or within one year and 6 months after its commission if it is a misdemeanor.”

However, under Illinois law, and as more fully described in Section V., in certain factual situations there can be exceptions to the statute of limitations, although, based upon the Special Prosecutor’s investigation and legal analysis, none were deemed applicable in this instance.

⁷ U.S. CONST. amend. XIV; *Christoffel v. United States*, 338 U.S. 84, 89 (1949) (“An essential part of a procedure which can be said fairly to inflict a punishment is that all the elements of the crime shall be proved beyond a reasonable doubt”); *In re Winship*, 397 U.S. 358 (1970); *Davis v. United States*, 160 U.S. 469 (1895); *People v. Hernandez*, 2012 WL 997363 (Ill. App. Ct. 1st Dist. 2012); *Speiser v. Randall*, 357 U.S. 513, 525–26 (1958); *see also In re Winship*, 397 U.S. 358, 369–72 (1970); *Morissette v. United States*, 342 U.S. 246 (1952); *People v. Anderson*, 473 N.E.2d 1345, 1351 (Ill. App. Ct. 2d Dist. 1985) (“State must prove scienter”).

⁸ Illinois Pattern Jury Instruction 2.03.

⁹ See, e.g., *People v. Antoine*, 676 N.E.2d 1374, 1378 (Ill. App. 4th Dist. 1997); *People v. Kozlowski*, 639 N.E.2d 1369, 1373 (Ill. App. Ct. 1st Dist. 1994); *People v. Sanchez*, 546 N.E.2d 268, 271 (Ill. App. Ct. 4th Dist. 1989).

prosecutor acting in good faith should not pursue a prosecution for charges that the prosecutor cannot reasonably expect to prove beyond a reasonable doubt by legally sufficient evidence at trial.¹⁰

3. Background on the Law of Criminal Intent (Scienter)

Under Illinois law, in order to convict a defendant of a criminal offense, the prosecution must prove two things beyond a reasonable doubt: first, that a crime occurred, and second, that it was committed by the person charged.¹¹ According to the Illinois Criminal Code, proof that a crime occurred requires proof of a voluntary act by the defendant¹² that is prohibited by law, and proof of criminal intent (scienter), which is a particular state of mind.¹³ In other words, under Illinois law, and as more fully described in Section V., a person can be found guilty of an offense only if, with respect to each element described by the statute defining the offense, he or she acted with the requisite criminal intent (recklessly, knowingly, or intentionally), depending upon the terms of the criminal statute.¹⁴ In proving the accused's criminal intent (scienter), the beyond a

¹⁰ See, e.g., American Bar Association, "Standards for Criminal Justice: Prosecution and Defense Function" § 3-3.9(a) (3d ed., 1993) ("A prosecutor should not institute, cause to be instituted, or permit the continued pendency of criminal charges in the absence of sufficient admissible evidence to support a conviction"); National District Attorneys Association, "National Prosecution Standards" § 4-2.2 (3d ed., 2009) ("A prosecutor should file charges that he or she believes adequately encompass the accused's criminal activity and which he or she reasonably believes can be substantiated by admissible evidence at trial.")

¹¹ *People v. Hurry*, 967 N.E.2d 817, 820 (Ill. App. Ct. 3d Dist. 2012), as modified on denial of reh'g, (Apr. 20, 2012); *People v. Bell*, 598 N.E.2d 256, 262 (Ill. App. Ct. 2d Dist. 1992); *People v. Curry*, 694 N.E.2d 630, 636 (Ill. App. Ct. 1st Dist. 1998); *People v. Groves*, 691 N.E.2d 86, 93-94 (Ill. App. Ct. 1st Dist. 1998), appeal denied, 699 N.E.2d 1034 (1998); *People v. Assenato*, 586 N.E.2d 445, 448 (Ill. App. Ct. 1st Dist. 1991), habeas corpus denied, 1998 WL 704327 (N.D. Ill. 1998); *People v. Lenius*, 688 N.E.2d 705, 718 (Ill. App. Ct. 1st Dist. 1997), appeal denied, 698 N.E.2d 546 (1998) and cert. denied, 119 S. Ct. 185 (U.S. 1998); *People v. Lloyd*, 660 N.E.2d 43, 48 (Ill. App. Ct. 1st Dist. 1995); *People v. Lesure*, 648 N.E.2d 1123, 1125 (Ill. App. Ct. 1st Dist. 1995).

¹² 720 ILCS 5/4-1 (West 2013).

¹³ 720 ILCS 5/4-3 (West 2013).

¹⁴ See *People v. Valley Steel Products Co.*, 375 N.E.2d 1297, 1305 (Ill. 1978); *People v. McMullen*, 414 N.E.2d 214, 218 (Ill. App. Ct. 4th Dist. 1980); *People v. Arron*, 305 N.E.2d 1, 3 (Ill. App. Ct. 1st Dist. 1973). The only exception, which is not relevant to the Special Prosecutor's investigation, is that "absolute liability offenses" do not require a culpable mental state as an element. *People v. Studley*, 631 N.E.2d 839, 841 (Ill. App. Ct. 4th Dist. 1994).

reasonable doubt standard is an especially high hurdle because it can rarely be proven by direct evidence; but, instead, is typically proved only by surrounding circumstances, i.e., circumstantial evidence.¹⁵

C. The Events of 2004: Evaluating Whether Employees of CPD and SAO Violated Illinois Criminal Law

1. Prosecution is Barred by the Applicable Statute of Limitations

As more fully described in Section V., any state law violations by employees of CPD and SAO relating to acts that occurred during their participation in the Koschman matter in 2004 are barred by the three-year statute of limitations.

D. The Events of 2011-2012: Evaluating Whether Employees of CPD and SAO Violated Illinois Criminal Law

1. The Events of 2011-2012: Prosecution Is Not Barred by the Applicable Statute of Limitations

Unlike the events which occurred in 2004, any state law violations by employees of CPD and SAO relating to acts that occurred during their participation in the Koschman matter in 2011 and 2012 are not barred by the applicable three-year statute of limitations as of the date of this report.

2. The Events of 2011-2012: Insufficient Evidence to Prove Beyond a Reasonable Doubt the Element of Criminal Intent (Scienter)

However, as more fully described in Section V., based upon all the evidence gathered by the Special Prosecutor and his office (the Office of the Special Prosecutor (“OSP”)) (e.g., witness interviews, sworn witness testimony before the special grand jury, documents subpoenaed and reviewed), and after having evaluated the elements of the potentially applicable state criminal laws with regard to the acts of certain individuals, the Special Prosecutor does not believe he could prove beyond a reasonable doubt by legally sufficient evidence at trial that any employee of CPD or SAO acted with the requisite criminal intent (scienter) to violate Illinois law during their participation in the Koschman matter in 2011 and 2012. Therefore, in compliance

¹⁵ See *People v. Castillo*, 974 N.E.2d 318, 326-27 (Ill. App. Ct. 1st Dist. 2012), *appeal denied*, 979 N.E.2d 881 (Sept. 26, 2012).

with his ethical obligations discussed above, the Special Prosecutor must exercise his prosecutorial discretion and not seek any additional charges in this matter.

E. Evidence Supporting the Decision to Appoint a Special Prosecutor

The sections of the report that follow summarize in great detail what the evidence actually established during the course of the Special Prosecutor's investigation. The Special Prosecutor notes that the evidence outlined below strongly supports Judge Toomin's April 6, 2012, order and decision to appoint a special prosecutor in this matter.¹⁶ Indeed, it is the Special Prosecutor's conclusion that the evidence outlined in the pages that follow does "bring transparency to the mixed signals emanating from this troubling case," as was Judge Toomin's stated objective in ordering the appointment of a special prosecutor in the Matter of the Death of David Koschman.¹⁷

III. OVERVIEW OF THE SPECIAL PROSECUTOR'S INVESTIGATION

In May 2012, the OSP engaged as its investigative partner the City of Chicago Inspector General's Office ("IGO").¹⁸ The IGO had initiated its own investigation into the Koschman matter on February 28, 2011.¹⁹ During the OSP's investigation, IGO assisted with interviewing witnesses, preparing special grand jury materials, analyzing records, and developing investigative leads.

On June 18, 2012, pursuant to Judge Toomin's Order, the Special Prosecutor empaneled a special grand jury to sit during the duration of the investigation. The special grand jury operated independently of the routine grand jury process controlled by SAO at the Leighton

¹⁶ See generally Apr. 6, 2012, Order by J. Toomin.

¹⁷ See Apr. 6, 2012, Order by J. Toomin, at 33.

¹⁸ IGO is led by Inspector General Joseph M. Ferguson, a former federal prosecutor with the United States Attorney's Office for the Northern District of Illinois.

¹⁹ The work product stemming from IGO's investigation prior to the appointment of the Special Prosecutor was shared with the OSP. This included work product related to the IGO's more than 30 interviews of witnesses in 2011 and early 2012, prior to the Special Prosecutor's appointment.

Criminal Court Building at 26th Street and S. California Avenue in Chicago.²⁰ In order to protect the independence and secrecy of the special grand jury's work, the OSP obtained court approval for the special grand jury to convene at Winston & Strawn LLP's law offices at 35 W. Wacker Drive, Chicago, Illinois.

In August 2012, the OSP also engaged the services of a well-known investigative firm, Kroll Associates, Inc. ("Kroll").²¹ Kroll's investigators assisted the OSP's investigation, including assistance in forensic and data retrieval expertise and interviewing current City of Chicago employees where the IGO's presence complicated cooperation.²²

During the course of the Special Prosecutor's investigation, 146 witnesses provided information through witness interviews and/or special grand jury testimony. The OSP interviewed 133 witnesses²³ (110 of whom agreed to sit for a voluntary interview, while 23 required the interviews be conducted pursuant to a proffer agreement).²⁴ The special grand jury was presented with the results of relevant witness interviews, and 24 witnesses personally appeared before the special grand jury and testified (14 witnesses provided live special grand jury testimony without asserting their Fifth Amendment rights, while 10 testified under court-ordered "use immunity" after they refused to testify and invoked their Fifth Amendment

²⁰ Both the office of the Clerk of the Circuit Court of Cook County and the Cook County Sheriff's Office provided the OSP valuable assistance in the coordination and administration of the special grand jury.

²¹ Kroll's Chicago office is led by Jeffrey H. Cramer, a former federal prosecutor with the United States Attorney's Office for the Northern District of Illinois.

²² In *Garrity v. New Jersey*, 385 U.S. 493, 87 S. Ct. 616 (1967), the United States Supreme Court held that police officers who were forced to speak or be terminated under their employment agreements were compelled to incriminate themselves in violation of the Fourteenth and Fifth Amendments. As such, the state was prohibited from using their compelled statements in their subsequent criminal prosecutions. In light of potential objections concerning *Garrity*, Kroll investigators assisted with conducting interviews of active City of Chicago employees rather than IGO investigators, due to IGO's authority to seek the termination of city employees.

²³ Before the Special Prosecutor was appointed, IGO interviewed 31 witnesses related to the Koschman matter, 27 of whom were re-interviewed by the OSP.

²⁴ The OSP interviewed certain witnesses pursuant to a uniform proffer agreement. As part of the proffer agreement, witnesses agreed to be interviewed and provide statements in exchange for the promise that the OSP could not use any of their actual statements against that person in any subsequent prosecution; although any leads developed from those statements could be used against that person in any subsequent prosecution.

privilege against self-incrimination).²⁵

The special grand jury issued 160 subpoenas for documentary evidence and testimony, and collected more than 22,000 documents (totaling over 300,000 pages). The records sought and collected included, among other items, telephone records, e-mails, police reports, policy manuals and procedures, attendance records, medical records, access logs, data recovered from backup tapes of shared drives, video surveillance, billing records, and receipts. In addition to the records collected by special grand jury subpoena, the OSP's investigation also procured court orders to obtain documents when necessary.

Lastly, due to the passage of eight years between the date of the incident and the appointment of a Special Prosecutor, many potentially important records from 2004 proved unavailable. For example, while phone records existed for certain individuals dating back to April 2004, other phone records, such as the personal cell phone records for the lead detective in the 2004 CPD investigation, no longer exist. Similarly, e-mail records for CPD and SAO employees from 2004 no longer exist and could not be recovered, as determined by OSP's full exploration, with the assistance of Kroll's computer forensics, of CPD and SAO's e-mail systems. These efforts uncovered that the e-mail records from 2004 no longer exist because of

²⁵ A proffer agreement is less comprehensive than court-ordered "use immunity" or "transactional immunity." The Illinois Code of Criminal Procedure authorizes a court, upon motion of the State, to order that "a witness be granted [use] immunity from prosecution in a criminal case as to any information directly or indirectly derived from the production of evidence from the witness if the witness has refused or is likely to refuse to produce the evidence on the basis of his or her privilege against self-incrimination." 725 ILCS 5/106–2.5(b) (West 1994). However, a grant of "use immunity" does not act as an absolute bar from prosecution but, rather, prohibits the State from using any evidence obtained under the grant of immunity, or leads derived from that evidence, against the immunized witness in a later criminal proceeding. *People ex rel. Cruz v. Fitzgerald*, 363 N.E.2d 835, 837, 66 Ill. 2d 546, 549 (1977); *People v. Adams*, 721 N.E.2d 1182, 1189, 308 Ill. App. 3d 995, 1004-05 (4th Dist. 1999). On the other hand, "transactional immunity" affords broader protection from future prosecution than "use immunity" and acts to completely bar the State from prosecuting an immunized witness for any offenses to which the immunity relates. 725 ILCS 5/106–1 (West 1976) and 725 ILCS 106–2 (West 1964); *see also People v. Ousley*, 919 N.E.2d 875, 885-886, 235 Ill. 2d 299, 313-314 (2009). As noted, the OSP did obtain "use immunity" orders from the Court for those witnesses who asserted their Fifth Amendment rights and refused to testify. The OSP, however, did not seek any orders for "transactional immunity." Grants of use immunity were necessary for the OSP to fulfill its court-ordered mandate.

The following witnesses were granted "use immunity": Bridget McCarthy, Kevin McCarthy, Craig Denham, Det. James Gilger, Det. Nick Spanos, Det. Edward Louis, Det. Patrick Flynn, SAO Dir. of State Program Michael Joyce, Lt. Richard Rybicki, and Det. Ronald Yawger. A request by a witness for "use immunity" should not be interpreted to mean that the person has actual criminal liability.

record retention policies and could not be recovered.

IV. DETAILED DISCUSSION OF THE EVIDENCE

A. Overview of the 2004 Incident on Division Street

On Saturday, April 24, 2004, David Koschman, then 21 years of age, and three of his friends — Scott Allen, James Copeland, and David Francis — drove together from their homes in Mount Prospect, Illinois, to Chicago's Humboldt Park neighborhood to visit their friend, Shaun Hageline, at his apartment.²⁶ Koschman and his friends, who had all gone to high school together,²⁷ had made plans to go out that night in the City and then attend the Chicago Cubs game the next day.²⁸ While at Hageline's apartment that evening, the group watched an NBA playoff basketball game,²⁹ drank beer,³⁰ and some also recounted smoking marijuana.³¹ Later that evening, the Koschman group headed to Division Street³² — a popular destination on Chicago's near-north side known for its high concentration of bars and clubs. The Koschman group visited several bars in the Division Street area that night,³³ and then, around approximately

²⁶ Hageline, Shaun, Special Grand Jury Tr. at 6:14-7:2 (Aug. 8, 2012); Allen, Scott, Special Grand Jury Tr. at 7:19-23, 8:7-24 (Aug. 8, 2012).

²⁷ Hageline, Shaun, Special Grand Jury Tr. at 6:19-24 (Aug. 8, 2012); Allen, Scott, Special Grand Jury Tr. at 7:24-8:6, 8:14-16 (Aug. 8, 2012).

²⁸ Hageline, Shaun, Special Grand Jury Tr. at 6:19-7:2 (Aug. 8, 2012); Allen, Scott, Special Grand Jury Tr. at 8:17-20 (Aug. 8, 2012) (Koschman, Francis, Copeland, and Allen planned to attend the Cubs game).

²⁹ Copeland, James, IGO Interview Rep. at 1 (May 21, 2012).

³⁰ Hageline, Shaun, Special Grand Jury Tr. at 7:3-6 (Aug. 8, 2012); Allen, Scott, Special Grand Jury Tr. at 8:21-24 (Aug. 8, 2012); Francis, David, Special Grand Jury Tr. at 12:20-23 (Aug. 8, 2012); Copeland, James, Special Grand Jury Tr. at 7:15-16 (July 11, 2012).

³¹ Hageline, Shaun, Special Grand Jury Tr. at 7:3-7:6 (Aug. 8, 2012); Allen, Scott, Special Grand Jury Tr. at 8:21-24 (Aug. 8, 2012); Francis, David, Special Grand Jury Tr. at 12:20-23 (Aug. 8, 2012).

³² Hageline, Shaun, Special Grand Jury Tr. at 7:7-9 (Aug. 8, 2012); Copeland, James, Special Grand Jury Tr. at 7:17-19 (July 11, 2012).

³³ Allen, Scott, Special Grand Jury Tr. at 9:1-6 (Aug. 8, 2012); Hageline, Shaun, Special Grand Jury Tr. at 7:9-13 (Aug. 8, 2012); Copeland, James, Special Grand Jury Tr. at 7:21-22 (July 11, 2012).

3:15 a.m.,³⁴ the group left the area and began walking westward³⁵ down Division Street to make their way back to Hageline's apartment.³⁶

That same night, Richard J. Vanecko, Craig Denham, Kevin McCarthy, Bridget McCarthy, and others attended an engagement dinner for Vanecko's cousin, Katherine Daley, at the Adobo Grill in the Old Town neighborhood of Chicago.³⁷ Vanecko is the nephew of Richard M. Daley, who in 2004, was the Mayor of the City of Chicago. Following dinner, a group of people from the engagement party — including Vanecko, the McCarthys, and Denham — went to a bar in the River North area of Chicago called the Pepper Canister.³⁸ After a few hours there,³⁹ the McCarthys, Vanecko, and Denham — planning to go to Butch McGuire's, a bar — took a cab to Division Street, where they exited just west of Dearborn Street and started walking eastward.⁴⁰

³⁴ Allen, Scott, Special Grand Jury Tr. at 9:7-13 (Aug. 8, 2012); Hageline, Shaun, Special Grand Jury Tr. at 7:16-21 (Aug. 8, 2012).

³⁵ Allen, Scott, Special Grand Jury Tr. at 9:7-13 (Aug. 8, 2012); Hageline, Shaun, Special Grand Jury Tr. at 7:16-21 (Aug. 8, 2012).

³⁶ Hageline, Shaun, IGO Interview Tr. at 10:1-6 (July 16, 2011).

³⁷ McCarthy, Bridget, Special Grand Jury Tr. at 14:21-15:15 (Aug. 15, 2012); Denham, Craig, Special Grand Jury Tr. at 14:17-15:24 (Aug. 15, 2012); Special Grand Jury Exhibit 57 at 1 (Michael Daley Special Grand Jury Declaration (Aug. 16, 2012)).

³⁸ McCarthy, Bridget, Special Grand Jury Tr. at 15:11-19 (Aug. 15, 2012); Denham, Craig, Special Grand Jury Tr. at 16:8-11 (Aug. 15, 2012).

³⁹ Both groups had been drinking much of the night. Before the special grand jury, Bridget McCarthy testified that she, her husband, Vanecko, and Denham had been drinking for approximately eight hours. *See McCarthy, Bridget, Special Grand Jury Tr. at 29:2-3, 29:17-30:4 (Aug. 15, 2012); see also McCarthy, Kevin, Special Grand Jury Tr. at 39:9-22 (Aug. 15, 2012)* (stating he had been with his wife, Vanecko, and Denham for eight hours and "had had some drinks"); Denham, Craig, Special Grand Jury Tr. at 35:11-12 (Aug. 15, 2012) (acknowledging he was "drunk"). Similarly, in addition to drinking beers at Hageline's apartment, Copeland testified before the special grand jury that Koschman's group of friends left Hageline's apartment to head to Division Street around 10 p.m. that night, where the group continued drinking and was intoxicated. Copeland, James, Special Grand Jury Tr. at 7:15-8:1 (July 11, 2012); *see also Francis, David, Special Grand Jury Tr. at 32:3-7 (Aug. 8, 2012)* (acknowledging he was "intoxicated"); Hageline, Shaun, Special Grand Jury Tr. at 21:21-22:11 (Aug. 8, 2012) (acknowledging he was "intoxicated"); Allen, Scott, Special Grand Jury Tr. at 9:10-13 (Aug. 8, 2012) ("We were all drunk, but we weren't slurring our words. We were not slurring our words or stumbling.").

⁴⁰ *See McCarthy, Bridget, Special Grand Jury Tr. at 15:20-16:9 (Aug. 15, 2012).*

While walking, the Koschman group and the Vanecko group crossed paths on the south sidewalk of Division Street,⁴¹ during which Koschman bumped into Denham.⁴² A verbal altercation ensued, and then Vanecko hit⁴³ Koschman with “a flush head-on punch that hit Koschman square in the face.”⁴⁴ Another witness at the scene described: “[Koschman] came flying back and fell straight back like a dead weight.”⁴⁵ Koschman’s head then struck the pavement.⁴⁶ At the time of the incident, Vanecko was 29 years old, 6’3” and 230 pounds, while Koschman was 21 years old, 5’5” and 125 pounds.⁴⁷

Immediately after Vanecko hit Koschman, Vanecko and Denham ran from the scene and took a taxi back to the Pepper Canister.⁴⁸ Kevin McCarthy was briefly detained by police and

⁴¹ McCarthy, Bridget, Special Grand Jury Tr. at 16:10-18 (Aug. 15, 2012); Hageline, Shaun, IGO Interview Rep. at 1-2 (May 19, 2012).

⁴² See Allen, Scott, Special Grand Jury Tr. at 9:23-24; 39:21-40:3 (Aug. 8, 2012); see Denham, Craig, Special Grand Jury Tr. at 17:8-11 (Aug. 15, 2012).

⁴³ See Allen, Scott, Special Grand Jury Tr. at 21:13-22:4 (Aug. 8, 2012); see Copeland, James, IGO Interview Tr. at 30:20-22 (June 23, 2011); see also Copeland, James, Special Grand Jury Tr. at 7:21-24 (Aug. 8, 2012).

⁴⁴ Copeland, James, Special Grand Jury Tr. at 9:16-18 (Jul. 11, 2012).

⁴⁵ Kohler, Phillip, Special Grand Jury Tr. at 9:7-11 (July 11, 2012).

⁴⁶ Dr. Stephen F. Futterer, a neuroradiologist at Northwestern Memorial Hospital who reviewed Koschman’s initial CT brain scans on April 26, 2004, determined that Koschman suffered: (1) a fracture in the right back of the head (or the right occipital bone); (2) a separate fracture in the left back of the head (or left occipital bone); (3) a fracture on the left, inner side of the skull (extending across the left petrous apex, which is part of the temporal bone); (4) elevated intracranial pressure (based upon a paucity of sulci and crowding of the basilar cisterns); and (5) bruises of the brain tissue (or hemorrhagic contusions in the bilateral inferior/anterior frontal lobes, left greater than right). See Special Grand Jury Exhibit 24 at 3 (Statement of Dr. Stephen F. Futterer (Aug. 8, 2012)).

Dr. Gordon Sze, Professor of Radiology and Chief of Neuroradiology at Yale University School of Medicine, who serves as a consulting medical expert to the OSP, stated in his expert report, among other things: “It should be noted that the occipital bone constitutes one of the thicker portions of the skull. It should also be noted that the petrous apex lies more than half way across the skull and is in the interior of the skull. Therefore, the amount of force necessary to cause a fracture of the occipital bone, with propagation to the petrous apex, is very significant.” Gordon Sze, MD, Expert Report at 3 (Apr. 3, 2013).

⁴⁷ See Special Grand Jury Exhibit 10 (CPD001115-CPD001118) (Case Supplementary Report 3193543 (approved Nov. 10, 2004)).

⁴⁸ See Denham, Craig, Special Grand Jury Tr. at 21:9-15 (Aug. 15, 2012).

released at the scene of the crime.⁴⁹ When Kevin McCarthy was questioned at the scene, he lied to police, claiming he did not know the identities of the other men who had run (Vanecko and Denham).⁵⁰ When released, Kevin McCarthy and his wife, Bridget McCarthy, entered a taxi on Division Street, conferred with Vanecko by cell phone, and traveled to the Pepper Canister to meet Vanecko and Denham.⁵¹ While the Pepper Canister had been officially closed, someone at the bar allowed the four to enter and meet.⁵²

Koschman was taken unconscious by ambulance from Division Street to Northwestern Memorial Hospital.⁵³ Despite numerous surgeries over the next eleven days, on May 6, 2004,

⁴⁹ See McCarthy, Kevin, Special Grand Jury Tr. at 21:12-16, 22:8-15 (Aug. 15, 2012).

⁵⁰ See Special Grand Jury Exhibit 6 at CPD001050 (CPD001049-CPD001050) (General Offense Case Report (approved Apr. 25, 2004)) (“McCarthy states he doesn’t know who other offenders are.”) Kevin McCarthy testified before the special grand jury that he did not recall being asked by Ofc. Tremore whether he knew the other individuals at the scene. See McCarthy, Kevin, Special Grand Jury Tr. at 52:6-11 (Aug. 15, 2012). But, Kevin McCarthy did admit during his testimony before the special grand jury that he lied to detectives later that same morning when he told them his wife and he exited the taxi alone and came upon two groups of people arguing. See McCarthy, Kevin, Special Grand Jury Tr. at 53:5-6 (Aug. 15, 2012).

⁵¹ See McCarthy, Kevin, Special Grand Jury Tr. at 22:14-19, 86:14-17, 87:6-9 (Aug. 15, 2012); McCarthy, Bridget, Special Grand Jury Tr. at 19:2-8 (Aug. 15, 2012); Sprint Account Statement for Richard Vanecko at SPR000547 (May 22, 2004) (SPR000545-SPR000548).

⁵² Before the special grand jury, Bridget McCarthy was the only member of the Vanecko group who would agree that the Pepper Canister was closed when the group was there after the incident (the altercation on Division Street occurred at approximately 3:15 a.m.), while Denham and Kevin McCarthy could not recall. See McCarthy, Bridget, Special Grand Jury Tr. at 54:7-15 (Aug. 15, 2012); Denham, Craig, Special Grand Jury Tr. at 40:3-9 (Aug. 15, 2012); McCarthy, Kevin, Special Grand Jury Tr. at 75:17-19 (Aug. 15, 2012). No one in the Vanecko group could explain how the group was let into the bar when it was closed. See McCarthy, Bridget, Special Grand Jury Tr. at 54:7-24 (Aug. 15, 2012); Denham, Craig, Special Grand Jury Tr. at 40:3-8 (Aug. 15, 2012). The OSP interviewed Ivan McCullagh, who was the manager of the Pepper Canister in 2004, and he explained that in 2004, the Pepper Canister closed at 3:00 a.m. on Saturdays and did not have a late-night liquor license. See McCullagh, Ivan, IGO Interview Rep. at 1 (Aug. 22, 2012). The OSP also interviewed Steve Bringas and Dominic O’Mahony, two bartenders at the Pepper Canister in 2004. See Special Grand Jury Exhibit 63 (Bringas, Steve, IGO Interview (Sept. 13, 2012)) and O’Mahony, Dominic, IGO Interview Rep. (Nov. 21, 2012). No one (McCullagh, Bringas, or O’Mahony) recalled ever letting the McCarthys, Denham, and Vanecko into the Pepper Canister after the bar had closed.

⁵³ See Special Grand Jury Exhibit 23 (Statement of Dr. Matthew R. Levine (May 8, 2004)); Special Grand Jury Exhibit 24 at 2-4 (Statement of Dr. Steven F. Futterer (Aug. 8, 2012)); Patient Progress Notes (May 2, 2004) (IG_002067).

Koschman died from injuries resulting from Vanecko's physical assault.⁵⁴

B. The 2004 CPD Investigation of the Incident

1. Early Morning Hours of April 25, 2004

On April 25, 2004, at approximately 3:15 a.m.,⁵⁵ after Koschman was hit⁵⁶ by Vanecko, on Division Street, Vanecko and Denham ran away⁵⁷ and the McCarthys also walked away from the immediate scene.⁵⁸ Koschman's friends flagged down 18th District Patrol Ofc. Edwin Tremore, directed him to where the altercation had occurred, and pointed out the McCarthys, who were still in the vicinity.⁵⁹ Before attending to Koschman, Tremore placed Kevin McCarthy in handcuffs and seated him in the back of his squad car.⁶⁰ Tremore then continued on foot

⁵⁴ See Special Grand Jury Exhibit 25 (Statement of Dr. Tae Lyong An (Aug. 13, 2012)). Koschman's Blue Cross Blue Shield insurance policy covered his medical expenses, totaling approximately \$250,000 incurred during his hospitalization. Northwestern Memorial Hospital patient billing records (NMH004303-NMH004307).

⁵⁵ See Special Grand Jury Exhibit 6 at CPD001049 (CPD001049-CPD001050) (General Offense Case Report (approved Apr. 25, 2004)).

⁵⁶ See Allen, Scott, Special Grand Jury Tr. at 11:7-9, 11:13-14 (Aug. 8, 2012) ("Right at this time, I saw Koschman get punched in the face."); (the punch "was definitely a sucker punch"); see Copeland, James, Special Grand Jury Tr. at 9:7-9 (Aug. 8, 2012) ("[The punch] was flush. It was closed fists. It wasn't like a smack."); and Copeland, James, Special Grand Jury Tr. at 9:16-18 (Jul. 11, 2012) ("The punch was a flush head-on punch that hit Koschman square in the face."); Hageline, Shaun, Special Grand Jury Tr. at 10:22-11:2 (Aug. 8, 2012) ("I don't remember Koschman trying to break his fall, which leads me to believe that he was knocked out before he hit the ground."); Kohler, Phillip, Special Grand Jury Tr. at 9:8-12 (Jul. 11, 2012) ("Almost immediately after Koschman moved between the two groups, he came flying back and fell straight back like a dead weight. It was like an explosion."). Furthermore, according to their testimony before the special grand jury in 2012, neither Kevin McCarthy, Bridget McCarthy, nor Craig Denham saw the physical contact between Vanecko and Koschman because they had each turned their backs and were walking away at the time Koschman was struck. See McCarthy, Kevin, Special Grand Jury Tr. at 18:9-14, 20:8-22, 49:14-18 (Aug. 15, 2012); McCarthy, Bridget, Special Grand Jury Tr. at 17:23-18:14, 39:5-14 (Aug. 15, 2012); Denham, Craig, Special Grand Jury Tr. at 20:4-10, 47:7-14, 48:7-10 (Aug. 15, 2012); see also General Progress Report at CPD001542 (CPD001541-CPD001543) (May 13, 2004).

⁵⁷ See Denham, Craig, Special Grand Jury Tr. at 20:4-24 (Aug. 15, 2012).

⁵⁸ See McCarthy, Bridget, Special Grand Jury Tr. at 17:23-18:2 (Aug. 15, 2012).

⁵⁹ See Tremore, Edwin, Kroll Interview Rep. at 2-3 (Sept. 18, 2012).

⁶⁰ See Tremore, Edwin, Kroll Interview Rep. at 3 (Sept. 18, 2012).

down Division Street, where he found Koschman lying in the street unconscious.⁶¹ Tremore immediately called for an ambulance.⁶²

In response to Tremore's request, the Office of Emergency Management and Communications ("OEMC") dispatched the Chicago Fire Department's ("CFD") Engine 4 and Ambulance 11.⁶³ By approximately 3:21 a.m.,⁶⁴ the dispatched CFD personnel began attending to Koschman. Koschman, having been attended to primarily by CFD Paramedic-in-Charge Patrick Jessee, was then transferred from the street into Ambulance 11 via a scene-stretcher, and at approximately 3:30 a.m., the ambulance departed to take Koschman to Northwestern Memorial Hospital, which was about a mile away.⁶⁵ Koschman arrived at Northwestern Memorial Hospital at approximately 3:35 a.m. and was immediately taken from Ambulance 11 into the emergency room via a hospital stretcher.⁶⁶

Meanwhile, back on Division Street, Tremore questioned Kevin McCarthy.⁶⁷ During the questioning, Kevin McCarthy lied to Tremore by claiming he did not know the identities of the other men who had run from the scene (Vanecko and Denham).⁶⁸ After interviewing Kevin McCarthy, Tremore ultimately released him on-site, after Koschman's friends told Tremore that

⁶¹ See Tremore, Edwin, Kroll Interview Rep. at 3 (Sept. 18, 2012).

⁶² See Tremore, Edwin, Kroll Interview Rep. at 3 (Sept. 18, 2012).

⁶³ See CFD Pre-Hospital Care Report at CLD000001 (Apr. 25, 2004) (CLD000001-CLD000003); see CFD Pre-Hospital Care Report at CFD000012 (Apr. 25, 2004) (CFD000011-CFD000014).

⁶⁴ See CFD Pre-Hospital Care Report at CFD000012 (Apr. 25, 2004) (CFD000011-CFD000014); see CFD Pre-Hospital Care Report at CLD000001 (Apr. 25, 2004) (CLD000001-CLD000003).

⁶⁵ See CFD Pre-Hospital Care Report at CFD000012-CFD000013 (Apr. 25, 2004) (CFD000011-CFD000014).

⁶⁶ See CFD Pre-Hospital Care Report at CFD000012-CFD000013 (Apr. 25, 2004) (CFD000011-CFD000014).

⁶⁷ See Special Grand Jury Exhibit 6 (CPD001049-CPD001050) (General Offense Case Report (approved Apr. 25, 2004)).

⁶⁸ Tremore's General Offense Case Report identifies four "offenders" (which includes Kevin McCarthy); three of them were listed as "unknown." See Special Grand Jury Exhibit 6 at CPD001049 (CPD001049-CPD001050) (General Offense Case Report (approved Apr. 25, 2004)). It is now known the three "unknown offenders" were Vanecko, Denham, and Bridget McCarthy.

it was not Kevin McCarthy who assaulted Koschman.⁶⁹ Bridget McCarthy remained nearby⁷⁰ while her husband was in temporary custody and left by taxi with her husband when he was released. The OSP has found no indication that Bridget McCarthy spoke with anyone from CPD that night.⁷¹

Tremore also took statements from Michael Connolly, a bystander witness, and Koschman's friend, Shaun Hageline.⁷² According to Tremore's General Offense Case Report, Hageline told him that Koschman was punched in the face.⁷³ According to the same report, Connolly told Tremore that Koschman was pushed in the chest;⁷⁴ however Connolly explained to the special grand jury in August 2012 that he did not actually see the physical contact between Vanecko and Koschman, because his view was obstructed,⁷⁵ although he did see Koschman fall like a "dead weight" after the physical contact occurred.⁷⁶

According to Tremore, because the unidentified men who fled the scene had simply been described by the witnesses as "white males," he did not put out a bulletin for other officers to be on the lookout for them, due to the amount of white males that were in the area at that time of the

⁶⁹ See McCarthy, Kevin, Special Grand Jury Tr. at 22:8-15 (Aug. 15, 2012).

⁷⁰ See McCarthy, Bridget, Special Grand Jury Tr. at 45:8-16 (Aug. 15, 2012).

⁷¹ See, e.g., McCarthy, Bridget, Special Grand Jury Tr. at 100:15-101:7 (Aug. 15, 2012).

⁷² See Special Grand Jury Exhibit 6 (CPD001049-CPD001050) (General Offense Case Report (approved Apr. 25, 2004)).

⁷³ See Special Grand Jury Exhibit 6 at CPD001050 (CPD001049-CPD001050) (General Offense Case Report (approved Apr. 25, 2004)) ("Witness #2 [Hageline] stated the same except he says victim was punched in the face not pushed.") In his 2012 special grand jury testimony, Hageline stated, "I did not actually see the punch thrown, but I heard a noise that could have been the sound of a punch or the sound of Koschman's head hitting the pavement." See Hageline, Shaun, Special Grand Jury Tr. at 10:10-15 (Aug. 8, 2012). Other than Vanecko and Koschman, the only other people at the scene of the incident who saw the physical contact between Vanecko and Koschman were Allen and Copeland, and both have consistently stated since 2004 that Vanecko punched Koschman in the face.

⁷⁴ See Special Grand Jury Exhibit 6 at CPD001049 (CPD001049-CPD001050) (General Offense Case Report (approved Apr. 25, 2004)) ("Witness #1 (Connelly) [sic] stated . . . one of the unknown offenders pushed victim in the chest....")

⁷⁵ See Connolly, Michael, Special Grand Jury Tr. at 9:9-13 (July 11, 2012).

⁷⁶ See Connolly, Michael, Special Grand Jury Tr. at 9:14-16 (July 11, 2012); see also Kohler, Phillip, Special Grand Jury Tr. at 9:8-12 (July 7, 2012).

morning (closing time for many of the bars).⁷⁷ Additionally, Tremore did not enter any of the businesses near the altercation in an attempt to identify any additional witnesses, citing that the incident took place just west of Dearborn Street, at a section of the block with no bars.⁷⁸ After departing the scene, Tremore drove to Northwestern Memorial Hospital to check on the condition of Koschman.⁷⁹ There he spoke with the emergency room attending physician, Dr. Matthew Levine, who related that Koschman was being treated for a head injury and was in serious condition.⁸⁰

In order for Tremore to complete the required CPD paperwork (the General Offense Case Report), he needed OEMC to assign a “records division number,” also known as a RD #. Tremore was provided RD # HK323454 for his report.⁸¹ Based on the facts known at that time, Tremore categorized the offense as a simple battery, a designation that his Sergeant, Patrick Moyer, approved.⁸² Tremore simultaneously notified detectives in the Violent Crimes section of Area 3 about the incident.⁸³ Around 5:15 a.m., approximately two hours after Koschman had been struck, Tremore officially completed his work on the matter.⁸⁴ He was never contacted by any detectives during their subsequent 2004 and 2011 investigations into the Koschman case.⁸⁵

⁷⁷ See Tremore, Edwin, Kroll Interview Rep. at 4 (Sept. 18, 2012).

⁷⁸ See Tremore, Edwin, Kroll Interview Rep. at 5 (Sept. 18, 2012).

⁷⁹ See Tremore, Edwin, Kroll Interview Rep. at 5 (Sept. 18, 2012).

⁸⁰ See Tremore, Edwin, Kroll Interview Rep. at 5 (Sept. 18, 2012); see Special Grand Jury Exhibit 6 at CPD001050 (CPD001049-CPD001050) (General Offense Case Report (approved Apr. 25, 2004)).

⁸¹ See Tremore, Edwin, Kroll Interview Rep. at 5 (Sept. 18, 2012); see Special Grand Jury Exhibit 6 at CPD001050 (CPD001049-CPD001050) (General Offense Case Report (approved Apr. 25, 2004)).

⁸² See Special Grand Jury Exhibit 6 at CPD001049 (CPD001049-CPD001050) (General Offense Case Report (approved Apr. 25, 2004)).

⁸³ See Special Grand Jury Exhibit 6 at CPD001049 (CPD001049-CPD001050) (General Offense Case Report (approved Apr. 25, 2004)).

⁸⁴ See Tremore, Edwin, Kroll Interview Rep. at 3 (Sept. 18, 2012); It is unknown how many CPD officers were actually at the scene of the altercation that morning and may have interacted with witnesses or bystanders. Only Tremore has been identified.

⁸⁵ See Tremore, Edwin, Kroll Interview Rep. at 6 (Sept. 18, 2012).

2. The Area 3 Investigation

a. Assigning the Koschman Matter

Upon notification of Area 3 detectives, responsibility for investigating the matter moved from CPD's Patrol Division to the Detective Division. Typically, detectives receive new assignments from their sergeant (and sometimes through a sergeant within the Area's Case Management Office) after their "watch" roll call.⁸⁶ In any given 24-hour period, CPD personnel typically work one of three possible "watches" (or shifts). Although the specific start and end times vary, generally speaking, the "first watch" is from approximately midnight until 9 a.m.; the "second watch" is from approximately 8 a.m. until 5 p.m.; and the "third watch" is from approximately 4 p.m. until 1 a.m. Sergeants are generally responsible for overseeing the assignments given to detectives during their watch,⁸⁷ although detectives are given wide latitude as to how best to handle the details of a particular investigation they are assigned.⁸⁸

Area 3 Violent Crimes Sgt. Robert O'Leary primarily worked the second watch in 2004, and was working on the morning of April 25, 2004.⁸⁹ According to Robert O'Leary, he assigned Det. Rita O'Leary (no relation) and Det. Robert Clemens, both of whom primarily worked second watch in 2004, to follow up on the Koschman case when they arrived to begin their watch the morning of April 25.⁹⁰ Robert O'Leary cannot recall why he assigned Rita O'Leary and

⁸⁶ See Special Grand Jury Exhibit 123 at 2-3 (O'Leary, Robert, Kroll Interview Rep. (Oct. 8, 2012)).

⁸⁷ See Special Grand Jury Exhibit 123 at 2-3 (O'Leary, Robert, Kroll Interview Rep. (Oct. 8, 2012)).

⁸⁸ See Special Grand Jury Exhibit 122 at 3 (O'Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012)); see Clemens, Robert, Kroll Interview Rep. (Proffer) at 7 (Oct. 25, 2012).

⁸⁹ See Special Grand Jury Exhibit 123 at 2, 5 (O'Leary, Robert, Kroll Interview Rep. (Oct. 8, 2012)).

⁹⁰ See Special Grand Jury Exhibit 123 at 5 (O'Leary, Robert, Kroll Interview Rep. (Oct. 8, 2012)). Det. Andrew Sobolewski is listed on police reports from 2004 as the "Primary Detective Assigned" to the matter, even though he never worked on the case. See, e.g., Special Grand Jury Exhibit 10 at CPD001115 (CPD001115-CPD001128) (Case Supplementary Report 3193543 (approved Nov. 10, 2004)); see Special Grand Jury Exhibit 15 at CPD001218 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 858620 (approved Feb. 28, 2011)). Sobolewski passed away on July 22, 2012, and did not testify before the special grand jury; however, the IGO interviewed him about the Koschman matter in August 2011. Det. Edward Day, who worked in Area 3's Case Management Office, believes he assigned Sobolewski to the Koschman matter in the Criminal History Records Information System (CHRIS), CPD's system for electronically storing police reports, a couple of days after the April 25 incident. See

Clemens to the Koschman matter, but he noted that it could “have been as simple as they were the first two detectives in that day.”⁹¹ Both Rita O’Leary and Clemens had pre-planned furloughs, with both working their final days before vacation or furlough on April 27,⁹² with Rita O’Leary set to return May 20,⁹³ and Clemens on May 19.⁹⁴

Neither Rita O’Leary nor Clemens are absolutely certain which sergeant assigned the case to them.⁹⁵ Rita O’Leary asserts she was never truly “assigned” the Koschman case, but rather was only asked to conduct a very narrow initial portion of the work (a few witness interviews and to follow up on Koschman’s medical condition).⁹⁶

Similarly, Clemens believes he was either “assigned to assist” Rita O’Leary’s investigation⁹⁷ — as opposed to being formally assigned the investigation himself — or that he may have simply “volunteered” to help Rita O’Leary interview Kevin McCarthy without ever being assigned anything by a sergeant.⁹⁸ Nevertheless, Clemens is confident that Rita O’Leary

Day, Edward, IGO Interview Rep. at 4-5 (Nov. 29, 2012). Once a name is entered in CHRIS as a matter’s “Primary Detective Assigned,” that name carries forward regardless of a detective’s actual involvement. *See* Sobolewski, Andrew, IGO Interview Tr. at 8:7-9:3, 23:6-12 (Aug. 5, 2011). Sobolewski stated that although he was listed as “Primary Detective Assigned,” he was not responsible for investigating the matter. *See* Sobolewski, Andrew, IGO Interview Tr. at 23:6-12 (Aug. 5, 2011). Sobolewski did not recall ever working on the Koschman matter, including aiding or being asked to aid Rita O’Leary on the case. *See* Sobolewski, Andrew, IGO Interview Tr. at 2:24-8:6, 36:9-11 (Aug. 5, 2011).

⁹¹ *See* Special Grand Jury Exhibit 123 at 5 (O’Leary, Robert, Kroll Interview Rep. (Oct. 8, 2012)).

⁹² *See* CPD Attendance & Assignment Record, Det. Div. Area 3 at IG_004044-IG_004045 (Apr. 27, 2004) (IG_004041-IG_004051); CPD Attendance & Assignment Record, Det. Div. Area 3 at IG_004054-IG_004056 (Apr. 28, 2004) (IG_004052-IG_004061).

⁹³ *See* CPD Attendance & Assignment Record, Det. Div. Area 3 at IG_004279 (IG_004276-IG_004285) (May 20, 2004).

⁹⁴ *See* CPD Attendance & Assignment Record, Det. Div. Area 3 at IG_004268 (IG_004266-IG_004275) (May 19, 2004).

⁹⁵ *See* Special Grand Jury Exhibit 122 at 3 (O’Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012)); Clemens, Robert, Kroll Interview Rep. (Proffer) at 5 (Oct. 25, 2012).

⁹⁶ *See* Special Grand Jury Exhibit 122 at 3, 9 (O’Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012)).

⁹⁷ *See* Clemens, Robert, Special Grand Jury Tr. at 17:1-14 (Apr. 24, 2013).

⁹⁸ *See* Clemens, Robert, Special Grand Jury Tr. at 69:10-70:19 (Apr. 24, 2013).

was officially assigned the investigation⁹⁹ — likely by Robert O’Leary¹⁰⁰ — even though he believes that the scope of what Rita O’Leary (and potentially he himself) was asked to do was not the “investigation in total.”¹⁰¹

b. Investigative Steps Taken by Det. O’Leary and Det. Clemens on April 25, 2004

The first investigative work done on the Koschman matter by Area 3 detectives occurred at approximately 9:30 a.m. on the morning of April 25, 2004, when Rita O’Leary called Northwestern Memorial Hospital to check on Koschman’s condition.¹⁰² Rita O’Leary spoke with a nurse over the phone and learned that Koschman was unconscious, unable to be interviewed, and was in critical but stable condition.¹⁰³

At approximately 11:00 a.m.,¹⁰⁴ Rita O’Leary was joined by Clemens,¹⁰⁵ and they drove¹⁰⁶ to Kevin McCarthy’s residence to interview him (Kevin McCarthy had been identified in Tremore’s report from earlier that morning).¹⁰⁷ Once inside Kevin McCarthy’s residence, Rita O’Leary took the lead in questioning him,¹⁰⁸ while Clemens listened and asked follow-up

⁹⁹ See Clemens, Robert, Special Grand Jury Tr. at 69:10-19, 75:4-6 (Apr. 24, 2013); see Clemens, Robert, Kroll Interview Rep. (Proffer) at 3 (Oct. 25, 2012).

¹⁰⁰ See Clemens, Robert, Kroll Interview Rep. (Proffer) at 5 (Oct. 25, 2012).

¹⁰¹ See Clemens, Robert, Special Grand Jury Tr. at 75:18-76:4 (Apr. 24, 2013).

¹⁰² See Special Grand Jury Exhibit 7 at CPD001058 (CPD001054-CPD001060) (Case Supplementary Report 3215651 (approved Nov. 10, 2004)).

¹⁰³ See Special Grand Jury Exhibit 7 at CPD001058 (CPD001054-CPD001060) (Case Supplementary Report 3215651 (approved Nov. 10, 2004)).

¹⁰⁴ See Clemens, Robert, Special Grand Jury Tr. at 86:13-19 (Apr. 24, 2013); see Special Grand Jury Exhibit 122 at 6 (O’Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012)).

¹⁰⁵ See Clemens, Robert, Special Grand Jury Tr. at 69:10-24 (Apr. 24, 2013).

¹⁰⁶ See Clemens, Robert, Kroll Interview Rep. (Proffer) at 9 (Oct. 25, 2012).

¹⁰⁷ See Special Grand Jury Exhibit 6 (CPD001049-CPD001050) (General Offense Case Report (approved Apr. 25, 2004)).

¹⁰⁸ See Clemens, Robert, Kroll Interview Rep. (Proffer) at 9 (Oct. 25, 2012).

questions.¹⁰⁹ Rita O’Leary described Kevin McCarthy as appearing to be hungover and groggy.¹¹⁰ Clemens thought Kevin McCarthy smelled of alcohol and was still intoxicated from the night before.¹¹¹

During the questioning, Kevin McCarthy once again denied knowing anyone involved in the altercation, which was false.¹¹² While questioning Kevin McCarthy in his home, detectives asked him if they could speak to his wife, Bridget McCarthy.¹¹³ Kevin insisted Bridget was not available at that time.¹¹⁴ The detectives asked Kevin McCarthy where Bridget and he went after he was released by Tremore. Kevin McCarthy told the detectives that they went home,¹¹⁵ which was also false. In fact, after Kevin McCarthy was released by Tremore, the McCarthys got into a cab on Division Street.¹¹⁶ Then, Bridget McCarthy called Vanecko on her cellphone from the

¹⁰⁹ See Clemens, Robert, Kroll Interview Rep. (Proffer) at 4 (Oct. 25, 2012).

¹¹⁰ See Special Grand Jury Exhibit 122 at 6 (O’Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012)).

¹¹¹ See Clemens, Robert, Special Grand Jury Tr. at 89:6-14 (Apr. 24, 2013). Both groups had been drinking for a number of hours that night and were intoxicated to some degree. See McCarthy, Bridget, Special Grand Jury Tr. at 29:2-3 (Aug. 15, 2012) (“I had definitely been drinking and was drunk”); McCarthy, Kevin, Special Grand Jury Tr. at 39:9-22 (Aug. 15, 2012) (stating he had been with his wife, Vanecko, and Denham for eight hours and “had had some drinks”); Denham, Craig, Special Grand Jury Tr. at 35:11-12 (Aug. 15, 2012) (acknowledging he was “drunk”); Francis, David, Special Grand Jury Tr. at 32:3-7 (Aug. 8, 2012) (acknowledging he was “intoxicated”); Hageline, Shaun, Special Grand Jury Tr. at 21:21-22:11 (Aug. 8, 2012) (acknowledging he was “intoxicated”); Allen, Scott, Special Grand Jury Tr. at 9:10-13 (Aug. 8, 2012) (“We were all drunk, but we weren’t slurring our words. We were not slurring our words or stumbling”); Copeland, James, Special Grand Jury Tr. at 7:21-8:1 (July 11, 2012) (acknowledging he was “intoxicated”). According to toxicology reports, Koschman’s blood alcohol level was 0.193. See Toxicology Report (Apr. 25, 2004) (IG_000610-IG_000611).

¹¹² See Special Grand Jury Exhibit 122 at 6 (O’Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012)).

¹¹³ See Clemens, Robert, Kroll Interview Rep. (Proffer) at 4 (Oct. 25, 2012); see Special Grand Jury Exhibit 122 at 6 (O’Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012)).

¹¹⁴ See Special Grand Jury Exhibit 122 at 6 (O’Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012)).

¹¹⁵ See Special Grand Jury Exhibit 7 at CPD001059 (CPD001054-CPD001060) (Case Supplementary Report 3215651 (approved Nov. 10, 2004)).

¹¹⁶ See McCarthy, Bridget, Special Grand Jury Tr. at 19:2-8 (Aug. 15, 2012).

cab.¹¹⁷ Vanecko advised Bridget McCarthy that he and Denham were at the Pepper Canister, and the McCarthys went there to meet them.¹¹⁸ Denham and Kevin McCarthy testified before the special grand jury that they could not recall anything that happened at that meeting.¹¹⁹ Bridget McCarthy testified before the special grand jury that she only recalled telling the group at the Pepper Canister that Kevin had been handcuffed.¹²⁰

Both Rita O'Leary and Clemens thought Kevin McCarthy was lying to them throughout the interview.¹²¹ Rita O'Leary stated that both she and Clemens "probably" took notes during their interview of Kevin McCarthy,¹²² while Clemens, on the other hand, testified that he did not take any notes.¹²³

Detectives typically record their interview notes on General Progress Report ("GPR") forms.¹²⁴ GPRs are thereafter used to prepare detectives' Case Supplementary Reports, or "case supps," as they are often referred to. Both the GPRs and the case supps are, according to CPD protocol,¹²⁵ supposed to be preserved in case files¹²⁶ and tendered to defense counsel under

¹¹⁷ See Special Grand Jury Exhibit 32 at SP000024 (SPR000023-SPR000027) (cell phone bill for cell phone number associated with Bridget McCarthy reflecting calls on April 25, 2004); *see also* McCarthy, Bridget, Special Grand Jury Tr. at 50:11-54:6 (Aug. 15, 2012).

¹¹⁸ See McCarthy, Bridget, Special Grand Jury Tr. at 19:3-8, 54:1-6 (Aug. 15, 2012).

¹¹⁹ See McCarthy, Kevin, Special Grand Jury Tr. at 23:2-8 (Aug. 15, 2012); Denham, Craig, Special Grand Jury Tr. at 21:15-17 (Aug. 15, 2012).

¹²⁰ See McCarthy, Bridget, Special Grand Jury Tr. at 57:2-23 (Aug. 15, 2012).

¹²¹ See Special Grand Jury Exhibit 122 at 6 (O'Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012)); *see also* Clemens, Robert, Special Grand Jury Tr. at 89:6-18 (Apr. 24, 2013).

¹²² See Special Grand Jury Exhibit 122 at 6 (O'Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012)).

¹²³ See Clemens, Robert, Special Grand Jury Tr. at 78:18-79:1, 87:24-88:4 (Apr. 24, 2013). But note, at one point during Clemens' proffer interview with the OSP, he stated he could not recall whether he took notes during the interview of Kevin McCarthy. See Clemens, Robert, Kroll Interview Rep. (Proffer) at 4 (Oct. 25, 2012).

¹²⁴ Villardita, Anthony, IGO Interview Rep. at 3 (Feb. 13, 2013); *see also* Chasen, Michael, IGO Interview Tr. at 51:4-20 (Aug. 23, 2011); Giralamo, Anthony, IGO Interview Rep. at 2 (Dec. 21, 2012).

¹²⁵ See CPD's Detective Division Standard Operating Procedures, Ch. 8, Sec. 8.3, Conducting a Field Investigation, Sub. Sec. (L)(4) at IG_005310-IG_005311 (1988) (IG_005234-IG_005450) (stating

prevailing discovery rules.

Rita O’Leary believes the GPRs she took throughout the day on April 25, 2004, formed the basis of the Case Supplementary Reports (one draft and one final report) she created for the Koschman case.¹²⁷ However, Rita O’Leary’s GPRs of her interview of Kevin McCarthy, as well as her GPRs from her other interviews taken that day, are missing.¹²⁸ In former CPD Superintendent Jody Weis’s opinion, missing GPRs raise red flags about an investigation.¹²⁹

At approximately 3:00 p.m. on April 25, 2004,¹³⁰ Rita O’Leary called Connolly, one of the two bystander witnesses (but the only one of whom Tremore had taken a statement from at the scene earlier that morning), and conducted a brief interview.¹³¹ Connolly told Rita O’Leary that he and his friend, Phillip Kohler (who was the other bystander witness), witnessed the altercation on Division Street that morning.¹³²

that “[i]n every case received for field investigation the assigned detective will . . . submit to the watch supervisor . . . all general progress reports and investigative notes prepared during the investigation.”)

¹²⁶ In normal practice, detectives are required to attach corresponding GPRs to their draft reports submitted to sergeants for review. *See* Special Grand Jury Exhibit 123 at 10 (O’Leary, Robert, Kroll Interview Rep. (Oct. 8, 2012)); *see* Special Grand Jury Exhibit 122 at 5 (O’Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012)) (stating that she typically submitted GPRs with her reports); *see* Louis, Edward, Special Grand Jury Tr. at 34:24-36:7 (Feb. 20, 2013) (stating that as a matter of practice the GPRs go with the Case Supplementary Reports). Specifically, Robert O’Leary stated that Area 3 detectives were required to put their GPRs in a bin for a sergeant to review and sign, and then those GPRs were to be placed in the case file. *See* Special Grand Jury Exhibit 123 at 10 (O’Leary, Robert, Kroll Interview Rep. (Oct. 8, 2012)).

¹²⁷ *See* Special Grand Jury Exhibit 122 at 6 (O’Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012)).

¹²⁸ While Robert O’Leary stated there have been instances when GPRs are not turned in with reports, he believes Rita O’Leary’s April 25, 2004 GPRs should have been turned in and ultimately placed in the Koschman case file. *See* Special Grand Jury Exhibit 123 at 10 (O’Leary, Robert, Kroll Interview Rep. (Oct. 8, 2012)). Additionally, even though it would have been Rita O’Leary’s typical practice to turn in her GPRs, she cannot recall whether she specifically did in this instance. *See* Special Grand Jury Exhibit 122 at 5 (O’Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012)).

¹²⁹ *See* Weis, Jody, IGO Interview Rep. at 2 (May 28, 2013).

¹³⁰ *See* Michael Connolly Phone Records at IG_002403 (IG_002399-IG_002413).

¹³¹ *See* Special Grand Jury Exhibit 7 at CPD001059-CPD001060 (CPD001054-CPD001060) (Case Supplementary Report 3215651 (approved Nov. 10, 2004)).

¹³² *See* Special Grand Jury Exhibit 7 at CPD001059-CPD001060 (CPD001054-CPD0001060) (Case Supplementary Report 3215651 (approved Nov. 10, 2004)).

The final Case Supplementary Report recording this interview was altered from what was recorded in the draft. Rita O'Leary's April 25, 2004, draft Case Supplementary Report contained a short write-up on her phone interview of Connolly. A portion of the draft report reads as follows:

CONNOLLY does see the victim get into the center of the altercation, he does not know if the victim was a [sic] aggressor or peacemaker, then he saw the victim get 'pushed or shoved' from the group and fall to the ground.¹³³

The same paragraph in Rita O'Leary's May 20, 2004 final Case Supplementary Report reads as follows:

CONNOLLY saw the victim get into the center of the altercation, and then he saw the victim get 'pushed or shoved' from the group and fall to the ground.

The final case supp removes the phrase "he [Connolly] does not know if the victim was a [sic] aggressor or peacemaker."¹³⁴ Rita O'Leary's April 25, 2004 handwritten GPR of this telephone interview of Connolly is missing.¹³⁵

At approximately 3:20 p.m., Rita O'Leary called Northwestern Memorial Hospital again

¹³³ See Special Grand Jury Exhibit 14 at CPD001619 (CPD001616-CPD001619) (Draft CPD Case Progress Report 323454 (drafted Apr. 25, 2004)).

¹³⁴ See Special Grand Jury Exhibit 7 at CPD001059 (CPD001054-CPD001060) (Case Supplementary Report 3215651 (approved Nov. 10, 2004)). Rita O'Leary testified that she did not know whether she removed the phrase on her own or upon someone else's instruction, but either way she believed the phrase was "redundant." See Special Grand Jury Exhibit 122 at 7-8 (O'Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012)). Connolly testified before the special grand jury that this statement was not an accurate reflection of what he told CPD in 2004 and that he "would not have said the term 'peacemaker' at all." Connolly, Michael, Special Grand Jury Tr. at 7:10-14 (Aug. 8, 2012). He further testified that he has "always said that the victim was the verbal aggressor in the incident. And definitely no peacemaking action on his part at all." Connolly, Michael, Special Grand Jury Tr. at 7:10-14 (Aug. 8, 2012). Connolly explained to the special grand jury that he did not actually see the physical contact between Vanecko and Koschman, because his view was obstructed, although he did see Koschman fall like a "dead weight" after being struck. See Connolly, Michael, Special Grand Jury Tr. at 9:9-16 (July 11, 2012).

¹³⁵ The Court noted this discrepancy between the draft narrative and the final case supplementary report in its April 6, 2012 Order granting the petition to appoint a special prosecutor. See Order by J. Toomin at 12, Apr. 6, 2012.

to check on Koschman's medical condition.¹³⁶ Rita O'Leary spoke with the same nurse she had spoken with earlier in the day, and the report was the same — Koschman remained in critical but stable condition.¹³⁷ At that time, the nurse handed the telephone to Nanci Koschman, David's mother, who, according to the case supp, explained her son's injuries in more detail and related that David would be sedated for at least the next five days.¹³⁸

With that, Rita O'Leary and Clemens's investigative work ended. However, based on their April 25, 2004 work alone, they were provided with the names of at least six additional individuals (Bridget McCarthy, Scott Allen, James Copeland, David Francis, Phillip Kohler, and Vrej Sazian) who could provide further information. All six were listed as "TO BE INTERVIEWED" in Rita O'Leary's draft case supp.¹³⁹ Rita O'Leary and Clemens never contacted these witnesses. In fact, none of these witnesses were contacted by any CPD personnel until May 9, 2004 — three days after Koschman had died. To be clear, no Area 3 detective work occurred on the Koschman matter from the end of Rita O'Leary and Clemens's April 25 shift until May 9, 2004 (13 days).

c. Certain Issues Stemming from Area 3's Initial Work

i. Assignment of Detectives on Furlough

Both detectives assigned on April 25, 2004, to investigate the Koschman matter were scheduled to take an extended period of time off (through the use of vacation days and official furlough) beginning April 28 — meaning that on the day they were assigned the case, at a maximum, they were available to work three shifts before stopping. Detectives knew, from information gathered from Tremore's conversation with the emergency room doctor, and from

¹³⁶ See Special Grand Jury Exhibit 7 at CPD001059 (CPD001054-CPD001060) (Case Supplementary Report 3215651 (approved Nov. 10, 2004)).

¹³⁷ See Special Grand Jury Exhibit 7 at CPD001059 (CPD001054-CPD001060) (Case Supplementary Report 3215651 (approved Nov. 10, 2004)).

¹³⁸ See Special Grand Jury Exhibit 7 at CPD001059 (CPD001054-CPD001060) (Case Supplementary Report 3215651 (approved Nov. 10, 2004)). Nanci Koschman also told Rita O'Leary that earlier that day she had received a phone call from Sazian, a friend of David's, who was the first person to inform her that David had been injured in an altercation while out with his friends Scott Allen, James Copeland, and David Francis.

¹³⁹ See Special Grand Jury Exhibit 14 at CPD001617-CPD001618 (CPD001616-CPD001619) (Draft Case Supplementary Report (drafted Apr. 25, 2004)).

Rita O'Leary's calls to the hospital, that Koschman would be unable to provide an immediate statement because he had suffered a severe head injury, was in critical condition, and would be sedated for at least five additional days.

According to CPD witnesses, given Koschman's condition, Rita O'Leary and Clemens (or certainly at least other Area 3 detectives) should have continued to investigate the matter through April 27, and upon leaving for their extended periods of time off, the case should have been immediately reassigned to other Area 3 detectives.¹⁴⁰ Neither occurred.

Rita O'Leary explained she did not work on the matter on April 26 or 27 because her assignment was narrow in scope and was limited to conducting a few witness interviews and following up on Koschman's medical condition.¹⁴¹ According to Rita O'Leary, the work she did on April 25 was the totality of the work she was assigned to handle, and she "got the ball rolling" by identifying additional witnesses to be interviewed.¹⁴² However, she did not attempt to contact those additional witnesses herself before leaving for furlough. Clemens explained he did not work on the matter on April 26 or 27 because he was simply "assigned to assist"¹⁴³ the investigation or may have simply "volunteered"¹⁴⁴ for the matter. According to Clemens, responsibility for the investigation should have rotated to third watch detectives.¹⁴⁵

According to Clemens, it was "common knowledge" that Rita O'Leary and he were scheduled for furlough in late April,¹⁴⁶ a sentiment that Rita O'Leary echoed.¹⁴⁷ In fact, Rita

¹⁴⁰ See Rybicki, Richard, Special Grand Jury Tr. at 65:19-67:1 (Mar. 27, 2013); see McLaughlin, Gillian, IGO Interview Rep. at 5 (Jan. 25, 2013); see also Chasen, Michael, IGO Interview Tr. at 100:19-101:6 (Aug. 23, 2011).

¹⁴¹ See Special Grand Jury Exhibit 122 at 3 (O'Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012)).

¹⁴² See Special Grand Jury Exhibit 122 at 3-4 (O'Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012)).

¹⁴³ See Clemens, Robert, Special Grand Jury Tr. at 17:9-14 (Apr. 24, 2013).

¹⁴⁴ See Clemens, Robert, Special Grand Jury Tr. at 69:10-70:19 (Apr. 24, 2013).

¹⁴⁵ See Clemens, Robert, Kroll Interview Rep. (Proffer) at 6 (Oct. 25, 2012). Commander James Gibson also believes this procedure should have occurred. See Gibson, James, Kroll Interview Rep. at 4 (Dec. 13, 2012). In the spring of 2004, Gibson was an Area 3 sergeant who typically worked the "third shift." See Sobolewski, Andrew, IGO Interview Tr. at 19:10-20:8 (Aug. 5, 2011) (explaining that cases often get passed from shift to shift).

¹⁴⁶ See Clemens, Robert, Special Grand Jury Tr. at 71:23-72:5 (Apr. 24, 2013).

O'Leary explained that she reminded her sergeant when she was given the case that she was going on furlough.¹⁴⁸ Also, Clemens explained that furlough schedules are widely known, with the Area Commander and Case Management Office both having knowledge of the applicable dates for all detectives.¹⁴⁹ Both Clemens and Rita O'Leary have explained that they bid on the April/May 2004 furlough dates in 2003.¹⁵⁰

The initial days of an investigation are critical, since a case can become a "cold case" relatively quickly and it is atypical for both detectives working a matter to be gone at the same time.¹⁵¹ Former Area 3 Sgt. James Gibson explained that the fact that both detectives would soon be on furlough "would not preclude them from beginning the investigation," but ideally, the same detectives work an investigation day after day.¹⁵² Another Area 3 sergeant, Gillian McLaughlin (who in 2004 typically worked second watch), noted that the Koschman case should not have been assigned to Rita O'Leary and Clemens if they were leaving on furlough; that is, unless the unit was short-handed.¹⁵³ Philip Cline, then CPD Superintendent, stated it was not

¹⁴⁷ See Special Grand Jury Exhibit 122 at 3 (O'Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012)).

¹⁴⁸ See Special Grand Jury Exhibit 122 at 3 (O'Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012)).

¹⁴⁹ See Clemens, Robert, Special Grand Jury Tr. at 72:6-23 (Apr. 24, 2013).

¹⁵⁰ See Clemens, Robert, Special Grand Jury Tr. at 72:6-13 (Apr. 24, 2013); see Special Grand Jury Exhibit 122 at 3 (O'Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012)). In response to a special grand jury subpoena, CPD produced a Records Disposal Certificate indicating that the applicable furlough request forms had been destroyed, pursuant to CPD policy, in approximately March 2004. See CPD Records Disposal Certificate for Area 3 Detective Division at CPD003148 (CPD003144-CPD003148). During its investigation, the OSP has found no evidence that undermines Clemens' and Rita O'Leary's assertion that their April 2004 furloughs were scheduled well in advance, pursuant to the normal CPD furlough selection procedures. In fact, the applicable CPD directive on furlough selections supports their statements. See CPD Department Notice No. 03-53 regarding Annual Watch, Furlough Selections, and Vacation Schedules 2004 (Issued Oct. 16, 2003) (CPD001937-CPD001940).

¹⁵¹ As stated by Sgt. Thomas Mills, who worked as a sergeant in the Violent Crimes office in Detective Division Area 5 in 2011, "lots of information comes in within 48 hours" and "[a] case can become a cold case relatively quickly." See Special Grand Jury Exhibit 108 at 3 (Mills, Thomas, Kroll Interview Rep. (Aug. 20, 2012)).

¹⁵² See Gibson, James, Kroll Interview Rep. at 4 (Dec. 13, 2012).

¹⁵³ See McLaughlin, Gillian, IGO Interview Rep. at 5 (Jan. 25, 2013); see Clemens, Robert, Kroll Interview Rep. (Proffer) at 5 (Oct. 25, 2012) (stating that sometimes a sergeant just has to "pick who's available"); see Special Grand Jury Exhibit 122 at 3 (O'Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012))

ideal for detectives leaving for vacation to be assigned aggravated battery cases.¹⁵⁴ Similarly, then Detective Division Chief James Molloy said that “common sense says you shouldn’t” assign a new investigation to detectives about to begin furlough.¹⁵⁵

The OSP was told that it was “odd” the case was not reassigned.¹⁵⁶ Det. Anthony Villardita simply noted: “someone dropped the ball.”¹⁵⁷ According to police, the failure to reassign the case and the resulting halt in the investigation is “surpris[ing],”¹⁵⁸ “uncommon,”¹⁵⁹ has “no explanation,”¹⁶⁰ does not “look good,”¹⁶¹ and is “embarrass[ing]” for CPD.¹⁶²

When asked whose responsibility it is to make sure cases do not “fall through the cracks,” McLaughlin did not attempt to skirt the obligation, answering: it is the sergeants’ responsibility.¹⁶³ Area 3 Lt. Richard Rybicki, who supervised the Violent Crimes sergeants and detectives, testified that, ultimately, it was his responsibility “to make sure that a case [didn’t] fall through the cracks like this.”¹⁶⁴

ii. Canvass for Additional Witnesses and Evidence

Immediately after the April 25, 2004 incident, detectives were aware that Koschman

(stating that she likely was given the assignment because no other detectives were available); *see* Gibson, James, Kroll Interview Rep. at 4 (Dec. 13, 2012) (stating that detective assignments are largely determined based upon who is available on any given day).

¹⁵⁴ *See* Cline, Phillip, IGO Interview Rep. at 6 (Dec. 28, 2012).

¹⁵⁵ *See* Molloy, James, Kroll Interview Rep. at 4 (Dec. 7, 2012).

¹⁵⁶ *See* McLaughlin, Gillian, IGO Interview Rep. at 5 (Jan. 25, 2013) (McLaughlin also stated that things like this happen at CPD when things “fall through the cracks”).

¹⁵⁷ *See* Villardita, Anthony, IGO Interview Rep. (Proffer) at 7 (Feb. 13, 2013).

¹⁵⁸ *See* Gibson, James, Kroll Interview Rep. at 5 (Dec. 13, 2012).

¹⁵⁹ *See* Clemens, Robert, Kroll Interview Rep. (Proffer) at 6 (Oct. 25, 2012).

¹⁶⁰ *See* Special Grand Jury Exhibit 123 at 7 (O’Leary, Robert, Kroll Interview Rep. (Oct. 8, 2012)).

¹⁶¹ *See* Kobel, Richard, IGO Interview Rep. at 5 (Jan. 17, 2013).

¹⁶² *See* Clemens, Robert, Kroll Interview Rep. (Proffer) at 6 (Oct. 25, 2012).

¹⁶³ *See* McLaughlin, Gillian, IGO Interview Rep. at 5 (Jan. 25, 2013).

¹⁶⁴ *See* Rybicki, Richard, Special Grand Jury Tr. at 60:16-21 (Mar. 27, 2013).

suffered serious head injuries,¹⁶⁵ was in critical condition,¹⁶⁶ and would be sedated for at least the next five days.¹⁶⁷ Nevertheless, according to CPD personnel, the inability to interview a victim should not delay the progress of an investigation.¹⁶⁸ In addition, according to CPD's Detective Division Standard Operating Procedures:

[C]ertain investigative procedures must be accomplished in each follow-up investigation. In every case received for field investigation the assigned detective will: ... (B) seek witnesses by a canvass of the area in the immediate vicinity of the location of occurrence [and] (C) view the crime scene and locate, secure and evaluate any evidence found.¹⁶⁹

Area 3 detectives did not canvass for additional witnesses or evidence (including video surveillance).¹⁷⁰ Numerous current and former detectives and police officers, including

¹⁶⁵ See Tremore, Edwin, Kroll Interview Rep. at 5 (Sept. 18, 2012); See Special Grand Jury Exhibit 6 at CPD001050 (CPD001049-CPD001050) (General Offense Case Report (approved Apr. 25, 2004)).

¹⁶⁶ See Special Grand Jury Exhibit 7 at CPD001058 (CPD001054-CPD001060) (Case Supplementary Report 3215651 (approved Nov. 10, 2004)).

¹⁶⁷ See Special Grand Jury Exhibit 7 at CPD001059 (CPD001054-CPD001060) (Case Supplementary Report 3215651 (approved Nov. 10, 2004)).

¹⁶⁸ See, e.g., Gilger, James, Special Grand Jury Tr. at 121:3-8 (Jan. 23, 2013) (agreeing that “the fact you cannot interview the victim is not supposed to stop you from continuing your investigation”).

¹⁶⁹ See CPD's Detective Division Standard Operating Procedures, Ch. 8, Sec. 8.3 Conducting a Field Investigation, Sub. Sec. (B) and (C) at IG_005309-IG_005310 (1988) (IG_005234-IG_005450).

¹⁷⁰ Detectives never canvassed for video surveillance, either in 2004 or as part of the 2011 re-investigation. In 2012, in an effort to obtain any surveillance videos that may have recorded the incident, the special grand jury issued subpoenas to those businesses, or entities that owned the businesses, located on Division Street on April 25, 2004, including: Bar Chicago, Butch McGuire's Tavern, Empire Restaurant, FedEx Store, Fifth Third Bank, Jewel Food Store, The Lodge, Original Mother's, Starbucks, T-Mobile store, UPS Store, and Walgreens.

Only Original Mother's had retained any surveillance videos from April 25, 2004 — taken from a video camera mounted inside the bar monitoring the entrance/exit — and provided a copy of the video to the OSP. The video contained footage of Koschman and his friends entering and exiting the Original Mother's bar on that same date (approximately three hours before the incident), but did not capture anything else of any relevance. The following businesses responded that they had no external surveillance video recording devices in 2004: Butch McGuire's, Empire Restaurant, The Lodge, and Original Mother's.

Superintendent Cline, explained that detectives should have canvassed the scene for witnesses and video surveillance shortly after the incident occurred.¹⁷¹ When Rita O’Leary was asked why she did not conduct a canvass of the area or seek video surveillance, she did not have an answer, other than to say she was assigned only to conduct some interviews.¹⁷² Clemens believes the third watch (the shift that started directly after Rita O’Leary’s and his shift ended), should have taken over the investigation on April 25, and immediately canvassed the scene for witnesses and video.¹⁷³ As previously noted, the investigation did not transition to third watch detectives on April 25, 2004.

d. Koschman’s Death and Assignment of Detective Yawger

Koschman died on May 6, 2004, from injuries sustained as a result of the April 25 attack. After Koschman died, hospital staff notified CPD and the Cook County Medical Examiner’s Office.¹⁷⁴ In response, 18th District Patrol Ofc. Tracie Sheehan was dispatched to the hospital to document Koschman’s transfer to the Medical Examiner’s Office.¹⁷⁵ That same day, Sheehan

The following businesses may have had external surveillance video recording devices in 2004, but some did not know for certain, and regardless, any video from those devices no longer exists: FedEx, Fifth Third Bank, Jewel Food Store, Starbucks Coffee Company, T-Mobile store, UPS Store and Walgreens.

¹⁷¹ See Cline, Phillip, IGO Interview Rep. at 2-3, 6 (Dec. 28, 2012); see Kobel, Richard, IGO Interview Rep. at 3-4 (Jan. 17, 2013) (stating that he would have done those things as a detective); McLaughlin, Gillian, IGO Interview Rep. at 5 (Jan. 25, 2013); Jacobs, Jesse, IGO Interview Rep. at 4 (Oct. 16, 2012); Special Grand Jury Exhibit 108 at 3 (Mills, Thomas, Kroll Interview Rep. (Aug. 20, 2012)); Louis, Edward, Special Grand Jury Tr. at 52:1-53:4 (Feb. 20, 2013) (stating that there was no reason not to take investigative steps such as gathering physical evidence, interviewing doormen, checking for videotapes, and trying to locate witnesses, while Koschman was unconscious in the hospital); Special Grand Jury Exhibit 123 at 11 (O’Leary, Robert, Kroll Interview Rep. (Oct. 8, 2012)); Gibson, James, Kroll Interview Rep. at 5 (Dec. 13, 2012); Molloy, James, Kroll Interview Rep. at 5, 8 (Dec. 7, 2012); Chasen, Michael, IGO Interview Rep. at 4 (Nov. 27, 2012); Rybicki, Richard, Special Grand Jury Tr. at 64:11-16 (Mar. 27, 2013).

¹⁷² See Special Grand Jury Exhibit 122 at 8 (O’Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012)).

¹⁷³ See Clemens, Robert, Kroll Interview Rep. (Proffer) at 6 (Oct. 25, 2012).

¹⁷⁴ See CPD Hospitalization Case Report (May 7, 2004) (CPD001061); Special Grand Jury Exhibit 26 (CCME000015) (Office of the Medical Examiner Case Report (May 8, 2004)).

¹⁷⁵ See Sheehan, Tracie, Kroll Interview Rep. at 2 (Oct. 17, 2012); see CPD Hospitalization Case Report (May 7, 2004) (CPD001061). All cases handled by CPD are given a unique identifier, called an RD # (Records Division), which is used to organize and track that case. On April 25, the Koschman

notified McLaughlin of Koschman's death.¹⁷⁶ On May 7, Koschman's body was transferred to the Medical Examiner's Office,¹⁷⁷ and an autopsy was conducted on May 8.¹⁷⁸ The Deputy Medical Examiner, Tae Lyong An, M.D., concluded the postmortem examination report by providing the following opinion regarding Koschman's cause of death: "This 21 year old white male, DAVID KOSCHMAN, died from craniocerebral injuries due to a blunt trauma. The manner of death is classified as homicide."¹⁷⁹ On May 10, Area 3 detectives reclassified the case from a simple battery to a homicide based upon the Medical Examiner's report.¹⁸⁰

matter was assigned RD # HK323454. *See* Special Grand Jury Exhibit 6 (CPD001049-CPD001050) (General Offense Case Report (approved Apr. 25, 2004)). That RD # should have carried forward for all of CPD's work on the Koschman case. However, on May 6, 2004, the Koschman investigation was given a second RD #. The second RD # was created when Sheehan was dispatched to the hospital on May 6, to handle the arrangements for Koschman's body to be transferred to the Medical Examiner's Office. *See* Sheehan, Tracie, Kroll Interview Rep. at 2-3 (Oct. 17, 2012). The second RD # provided by the dispatcher to Sheehan was HK348411. As Det. Patrick Flynn, who was the liaison between Area 3 and the Medical Examiner's Office, explained, it is not uncommon for a dispatcher to supply another RD # under the same victim's name when an officer is sent to the hospital to coordinate the delivery of a body to the morgue. *See* CPD Hospitalization Case Report (May 7, 2004) (CPD001061); Flynn, Patrick, Special Grand Jury Tr. at 66:2-17 (Mar. 13, 2013); *see also* Skelly, Thomas, Kroll Interview Rep. at 2 (Nov. 5, 2012) (stating the issuance of multiple RD #'s happens frequently); *see also* Webb, Kenneth, IGO Interview Rep. at 3 (Feb. 11, 2013) (stating it happens once or twice a week). Flynn discovered the dual RD #'s on July 19, 2004, and submitted a Case Supplementary Report which not only "unfounded" the second RD # but also included a notation that all investigative reports should be entered under the original RD #. *See* Special Grand Jury Exhibit 114 (IG_007578-IG_007579) (Case Supplementary Report 3364006 (approved July 20, 2004)). According to Flynn, unfounding a case under these circumstances simply means the underlying matter has already been given a RD #, and that the second RD # should not be used any longer. *See* Flynn, Patrick, Special Grand Jury Tr. at 63:6-66:17 (Mar. 13, 2013). Therefore, for a period of time, certain CPD paperwork on the Koschman matter was filed under the original RD #, while a small number of records were filed under the second RD #.

¹⁷⁶ *See* CPD Hospitalization Case Report (May 7, 2004) (CPD001061).

¹⁷⁷ *See* Office of the Medical Examiner, First Call Sheet (May 7, 2004) (CCME000016).

¹⁷⁸ *See* Office of the Medical Examiner, Report of Postmortem Examination at CCME000008 (May 8, 2004) (CCME000008-CCME000013).

¹⁷⁹ *See* Office of the Medical Examiner, Report of Postmortem Examination at CCME000013 (May 8, 2004) (CCME000008-CCME000013). *See also* Special Grand Jury Exhibit 54 at 5 (Statement of Dr. Joshua M. Rosenow (Aug. 8, 2012)) (the Northwestern Memorial Hospital physician who admitted Koschman) (stating "I would classify Koschman's cause of death as complications stemming from a traumatic brain injury.")

¹⁸⁰ *See* Special Grand Jury Exhibit 9 at CPD001067-CPD001068 (CPD001066-CPD001068) (Case Supplementary Report 3192832 (approved May 10, 2004)).

Det. Ronald Yawger was officially assigned on May 9, 2004, to continue the Koschman investigation, which had remained dormant since April 25, 2004.¹⁸¹ However, the OSP uncovered some evidence indicating Yawger was involved in the investigation prior to May 9, 2004. Specifically, on April 25, 2011, at 11:43 a.m., approximately eight hours after the incident, Yawger (who is identified by his PC Login ID number “PC0N556”), accessed criminal arrest records for Kevin McCarthy.¹⁸² The timing of the inquiry indicates the search may have been run in conjunction with Rita O’Leary’s and Clemens’ interview of Kevin McCarthy on April 25, 2004.¹⁸³ Yawger testified before the special grand jury in July 2013, and after being shown the access evidence, he acknowledged having accessed Kevin McCarthy’s criminal arrest records on April 25, 2004; however, he stated he “knew nothing about this case [the Koschman case] until . . . it was assigned to [him]” on May 9, 2004.¹⁸⁴ Furthermore, Yawger testified that he did not know who asked him to access Kevin McCarthy’s criminal arrest records on April 25, 2004.¹⁸⁵

When Yawger testified before the special grand jury in July 2013, he also stated that he may have been assigned the matter on May 9, 2004, by Robert O’Leary.¹⁸⁶ According to Yawger, Robert O’Leary was his immediate supervisor on the Koschman investigation,¹⁸⁷ although Robert O’Leary did not recall assigning the case.¹⁸⁸ According to Yawger’s special grand jury testimony, he personally did the majority of the detective work on the 2004

¹⁸¹ See General Progress Report (May 9, 2004) (CPD001065).

¹⁸² McCarthy, Kevin CLEAR Rep. (Apr. 25, 2004) (CPD001679); *see also* CLEAR Rep. Personnel Who Accessed Case Rep. HK323454 (Sept. 19, 2011) (CPD004075) (identifying PC0N556 as Yawger’s User ID).

¹⁸³ See McCarthy, Kevin CLEAR Rep. (Apr. 25, 2004) (CPD001679).

¹⁸⁴ See Yawger, Ronald, Special Grand Jury Tr. at 39:16-40:6, 44:10-18, 45:10-12 (July 15, 2013).

¹⁸⁵ See Yawger, Ronald, Special Grand Jury Tr. at 46:9-12, 46:16-21 (July 15, 2013).

¹⁸⁶ See Yawger, Ronald, Special Grand Jury Tr. at 111:23-112:2 (July 15, 2013).

¹⁸⁷ See Yawger, Ronald, IGO Interview Tr. at 92:7-15 (July 1, 2011).

¹⁸⁸ O’Leary, Robert, Kroll Interview Rep. at 5 (Oct. 8, 2012).

Koschman case.¹⁸⁹

Yawger also previously told IGO investigators that he did not know why he was assigned the case,¹⁹⁰ and that he was “[j]ust assigned.”¹⁹¹ But, according to other detectives working in Area 3 in 2004, Yawger was likely chosen because of his reputation.¹⁹² Area 3 Commander Michael Chasen stated he was not involved in the decision to add Yawger to the Koschman investigation, but speculated that Yawger was probably chosen because he was a good detective with an excellent reputation for handling homicide and death investigations.¹⁹³ Likewise, even though McLaughlin was not sure why Yawger was assigned to the matter, she reiterated that if the Koschman case had in fact fallen through the cracks, Yawger was the kind of detective who could get the case “back to where it needed to be” because he had a reputation of being a thorough detective.¹⁹⁴ She believes that if the proverbial “ball was dropped” by CPD during the initial days, then the case would have been reassigned to its “best guy” – someone like Yawger.¹⁹⁵

e. Detective Yawger’s Investigation

On May 9, 2004, Yawger called Koschman’s three friends who were with Koschman on Division Street the night of the altercation —Allen, Copeland, and Francis — each of whom said they could be interviewed in person on May 12.¹⁹⁶ Yawger also left voicemails for Bridget

¹⁸⁹ See Yawger, Ronald, Special Grand Jury Tr. at 34:22-24 (July 15, 2013).

¹⁹⁰ See Yawger, Ronald, IGO Interview Tr. at 75:23-76:2 (July 1, 2011).

¹⁹¹ See Yawger, Ronald, Special Grand Jury Tr. at 111:17-19 (July 15, 2013).

¹⁹² Yawger retired from CPD on August 15, 2007, and currently works as an investigator for the Illinois Attorney General’s Office. See Yawger, Ronald, IGO Interview Tr. at 98:12-18 (July 1, 2011).

¹⁹³ See Chasen, Michael, IGO Interview Rep. at 4 (Nov. 27, 2012).

¹⁹⁴ See McLaughlin, Gillian, IGO Interview Rep. at 6 (Jan. 25, 2013).

¹⁹⁵ See McLaughlin, Gillian, IGO Interview Rep. at 6 (Jan. 25, 2013). Yawger stated during his testimony before the special grand jury in July 2013, that even after the Koschman case became a homicide, he never canvassed the scene for additional witnesses, such as Division Street bar bouncers, who may have viewed the April 25, 2004 altercation. See Yawger, Ronald, Special Grand Jury Tr. at 35:15-20 (July 15, 2013).

¹⁹⁶ See General Progress Report (May 9, 2004) (CPD001065); see Giralamo, Anthony, IGO Interview Rep. at 4 (Dec. 21, 2012) (stating Yawger drafted this report and noting that he (Det. Giralamo)

McCarthy, Sazian, and Kohler, asking them to contact detectives.¹⁹⁷ Finally, he left a note for third watch detectives asking them to locate and interview Bridget McCarthy, Sazian, and Kohler.¹⁹⁸

On May 10, Det. Giralamo interviewed Kohler at the Third Municipal District Courthouse in Rolling Meadows.¹⁹⁹ Giralamo's GPR states that Kohler was walking east on Division Street when he saw two groups of people arguing and pushing, with Koschman standing "curbside" and towards "the back of the group."²⁰⁰ It further states that Kohler saw

did not participate in any of the phone calls mentioned in Yawger's GPR). The OSP made extensive efforts to acquire Yawger's cell phone records from 2004, and of particular interest were his records from April 25, 2004 (the date of the incident) through May 20, 2004 (the date of the lineups). While the issuance of multiple subpoenas yielded phone records from September 2004 through December 2004, the OSP could not obtain the aforementioned and potentially critical April 2004 through May 2004 records, even after working diligently with the applicable carrier's subpoena compliance center. Ultimately, the OSP received confirmation in writing indicating that the remaining requested 2004 phone records no longer existed. *See* correspondence from AT&T (April 15, 2013) (ATT005988-ATT005996).

¹⁹⁷ *See* General Progress Report (May 9, 2004) (CPD001065).

¹⁹⁸ *See* General Progress Report (May 9, 2004) (CPD001065).

¹⁹⁹ Kohler was at the courthouse for jury duty. *See* Kohler, Phillip, IGO Interview Rep. at 3 (May 16, 2012). In 2012, Kohler told the OSP it was during this interview that he was first shown two or three grainy black-and-white street camera photographs of a white male wearing a hat. *See* Kohler, Phillip, IGO Interview Rep. at 3 (May 16, 2012). Kohler also recalled that when he was at Area 3 on May 20, 2004, to view lineups, detectives again showed him what might have been the same photographs he was shown previously. *See* Kohler, Phillip, IGO Interview Rep. at 3-4 (May 16, 2012). Kohler noted he did not recognize the person in the photographs. Giralamo did not recall showing Kohler any photographs during the May 10, 2004 interview. *See* Giralamo, Anthony, IGO Interview Rep. at 5 (Dec. 21, 2012). However, Giralamo did state that generally speaking, if Yawger or one of his sergeants directed him to show a witness some photographs, he would have. *See* Giralamo, Anthony, IGO Interview Rep. at 5 (Dec. 21, 2012). According to Yawger's special grand jury testimony, he does not think Kohler was ever shown photographs. *See* Yawger, Ronald, Special Grand Jury Tr. at 116:1-24 (July 15, 2013). But, Yawger also testified that he was not present for Kohler's May 10, 2004 interview. *See* Yawger, Ronald, Special Grand Jury Tr. at 114:18-115:7 (July 15, 2013). Besides Kohler, no other witnesses or CPD personnel have mentioned the black-and-white street camera photographs. The special grand jury sought these photographs from CPD via subpoena and no responsive materials were produced. *See* Special Grand Jury Subpoena Duces Tecum to CPD at 2, June 27, 2012.

²⁰⁰ *See* General Progress Report (approved May 13, 2004) (CPD001588). On July 11, 2012, as part of his testimony, Kohler read a statement which, in part, stated that he was walking with Connolly east on Division Street when they encountered the two groups and, "As we got closer, we stopped to take a look. The group that I know — that I now know included David Koschman, had their backs to us and were facing east. The other group was facing west. Koschman was standing about three feet in front of us and behind the other members of his group. I remember Koschman being a small kid." Kohler, Phillip, Special Grand Jury Tr. at 7:22-8:10 (July 11, 2012).

Koschman “rush[ing] forward into [the] center of [the] group (aggressive).”²⁰¹ Giralamo’s GPR notes that Koschman was observed almost immediately being pushed out of the center of the group, where he fell backwards and hit his head.²⁰² During his testimony before the special grand jury in July 2012, Kohler stated that he “lost sight of Koschman after he moved in between the two groups,” but that “[a]lmost immediately after Koschman moved between the two groups, he came flying back and fell straight back like a dead weight. It was like an explosion.”²⁰³ Kohler further stated: “Koschman hit his head pretty hard on the curb, and I believe his head actually bounced off the curb.”²⁰⁴ According to Giralamo’s GPR, Kohler also told detectives that he had never seen anyone in Vanecko’s group before that night and was unable to identify any of the participants in the altercation.²⁰⁵

On May 12, Yawger interviewed Francis,²⁰⁶ Copeland,²⁰⁷ and Allen.²⁰⁸ Giralamo may have also participated in these interviews.²⁰⁹ That same day, Sazian²¹⁰ was also interviewed by

²⁰¹ See General Progress Report (approved May 13, 2004) (CPD001588). Kohler clarified before the special grand jury that Koschman was being “verbally aggressive,” but did not recall any physical contact. Kohler, Phillip, Special Grand Jury Tr. at 8:18-9:4 (July 11, 2012) (Koschman “jumped through a small space between his friends and into the middle of the two groups. I don’t recall Koschman clenching his fists or actually touching anyone in the other group, but he was being verbally aggressive toward the people who said something to him. To the best of my memory, Koschman’s friends were not restraining him.”)

²⁰² See General Progress Report (approved May 13, 2004) (CPD001588).

²⁰³ See Kohler, Phillip, Special Grand Jury Tr. at 9:5-12 (July 11, 2012).

²⁰⁴ See Kohler, Phillip, Special Grand Jury Tr. 9:11-16 (July 11, 2012).

²⁰⁵ See General Progress Report (approved May 13, 2004) (CPD001588). Kohler would later tell detectives and *Sun-Times* reporters in 2011 that he in fact attended high school with Vanecko at Loyola Academy. Kohler, Phillip, Special Grand Jury Tr. 10:23-11:15 (July 11, 2012).

²⁰⁶ See General Progress Report (approved May 13, 2004) (CPD001586-CPD001587).

²⁰⁷ See General Progress Report (approved May 13, 2004) (CPD001584-CPD001585).

²⁰⁸ See General Progress Report (approved May 13, 2004) (CPD001581-CPD001583).

²⁰⁹ See Giralamo, Anthony, IGO Interview Rep. at 5 (Dec. 21, 2012).

²¹⁰ See Special Grand Jury Exhibit 106 (CPD001577) (General Progress Report (May 12, 2004)).

Yawger or Giralamo over the phone.²¹¹ While GPRs have been located for the interviews of Francis, Copeland, and Allen, the existence and location of a GPR for the Sazian interview is unknown, even though Yawger testified he would have created a GPR (if he interviewed him).²¹² During Yawger's interviews, Francis, Allen, and Copeland provided statements bearing on the identity of the offender, as well as whether Koschman was punched or pushed. According to Yawger's GPR of his interview with Francis, Francis did not know whether Koschman was "hit or pushed."²¹³ According to Yawger's GPR of the interview with Copeland, Copeland stated that, "the larger of the three guys punched [Koschman] in the face."²¹⁴ Additionally, according to Yawger's GPR of his interview with Allen, Allen stated that "the larger of the 3 guys punched [Koschman] in the face."²¹⁵

Yawger's GPR of the Allen interview also contained several sentences that were scratched out by Yawger.²¹⁶ In 2011, the IGO, in an attempt to decipher what had been crossed out, sent the original GPR to the FBI for analysis by the FBI's Questioned Documents Unit.²¹⁷ Even with the use of sophisticated technology, the FBI was unable to read the entire obliterated portion.²¹⁸ However, based on the FBI's analysis, and the context of Allen's statement, a portion of Yawger's GPR which was crossed out states, "After a few minutes, arguing became 'more

²¹¹ See Yawger, Ronald, Special Grand Jury Tr. at 33:14-34:1 (July 15, 2013).

²¹² See Yawger, Ronald, Special Grand Jury Tr. at 34:8-14, 28:6-10 (July 15, 2013).

²¹³ See General Progress Report at CPD001587 (approved May 13, 2004) (CPD001586-CPD001587).

²¹⁴ See General Progress Report at CPD001584 (approved May 13, 2004) (CPD001584-CPD001585).

²¹⁵ See General Progress Report at CPD001582 (approved May 13, 2004) (CPD001581-CPD001583).

²¹⁶ See General Progress Report at CPD001581 (approved May 13, 2004) (CPD001581-CPD001583). See Yawger, Ronald, Special Grand Jury Tr. at 60:19-21 (July 15, 2013).

²¹⁷ See FBI Laboratory Report of Examination (Dec. 19, 2011) (IG_005735-IG_005736).

²¹⁸ See FBI Laboratory Report of Examination (Dec. 19, 2011) (IG_005735-IG_005736).

heated, the larger of the three guys, now becomes very aggressive, starts saying alright come on lets go.”²¹⁹

Later that day, Yawger spoke over the phone with Bridget and Kevin McCarthy’s attorney, Bill Dwyer.²²⁰ Dwyer informed Yawger that his clients knew the other two people involved in the incident (something Kevin McCarthy had twice previously denied).²²¹ Dwyer told Yawger he would bring his clients in for an interview on May 13.²²² As noted below, Bridget was interviewed on May 13 as planned, while Kevin was not interviewed until May 19. Before leaving for the day, Yawger left another note for third watch detectives asking them to interview Hageline in person.²²³

²¹⁹ See General Progress Report at CPD001581 (approved May 13, 2004) (CPD001581-CPD001583); see FBI Laboratory Report of Examination at IG_005736 (Dec. 19, 2011) (IG_005735-IG_005736). According to Yawger’s grand jury testimony, GPRs are “extremely important” because they record what a witness says to the interviewing officer. See Yawger, Ronald, Special Grand Jury Tr. at 63:22-64:1, 31:11-14 (July 15, 2013).

²²⁰ See Special Grand Jury Exhibit 106 (CPD001577) (General Progress Report (May 12, 2004)).

²²¹ See Special Grand Jury Exhibit 106 (CPD001577) (General Progress Report (May 12, 2004)). As would ultimately be disclosed, the other two people involved were Vanecko and Denham.

²²² See Special Grand Jury Exhibit 106 (CPD001577) (General Progress Report (May 12, 2004)).

²²³ See Special Grand Jury Exhibit 106 (CPD001577) (General Progress Report (May 12, 2004)). Yawger’s note also instructed third watch detectives to “PLEASE CALL ME AT HOME OR ON MY CELL PHONE BEFORE YOU GO TO INTERVIEW HIM” and left his cell phone number. Louis testified that he did not call Yawger as instructed, while his partner, Villardita, could not recall if he called Yawger, although he believes he would have followed the instructions. Louis, Edward, Special Grand Jury Tr. at 38:22-39:6, 72:6-15 (Feb. 20, 2013); Villardita, Anthony, IGO Interview Rep. (Proffer) at 4-5 (Feb. 13, 2013). Both said it was not unusual to leave requests such as the one left by Yawger. See Louis, Edward, Special Grand Jury Tr. at 40:1-6 (Feb. 20, 2013); Villardita, Anthony, IGO Interview Rep. (Proffer) at 5 (Feb. 13, 2013); see also Giralamo, Anthony, IGO Interview Rep. at 5 (Dec. 21, 2012) (stating it was typical for Yawger to leave notes). While Villardita could not recall precisely, he presumed Yawger wanted to be called before the witness was interviewed so that Yawger could provide background or ensure that a specific topic was covered during the interview. See Villardita, Anthony, IGO Interview Rep. (Proffer) at 5 (Feb. 13, 2013). During his July 2013 special grand jury testimony, Yawger confirmed Villardita’s presumption as to the purpose of his note, see Yawger, Ronald, Special Grand Jury Tr. at 121:23-123:19 (July 15, 2013), although Yawger could not recall whether Detectives Louis or Villardita actually called him in response to his note, see Yawger, Ronald, Special Grand Jury Tr. at 121:17-19 (July 15, 2013).

On May 13, Detectives Villardita and Louis interviewed Hageline, though the existence and location of any GPR is unknown.²²⁴ Louis testified that there would have been a GPR generated in connection with the Hageline interview, and that it was his practice and procedure to submit GPRs with his case supps.²²⁵ Villardita similarly stated that he recalls GPRs for the Hageline interview, and that the notes should have accompanied the case supp into the Koschman homicide file.²²⁶ Following Hageline's interview, Louis submitted his case supp report that evening (which was approved by Gibson on May 17, 2004).²²⁷

According to Louis's case supp, Hageline described the individuals in Vanecko's group.²²⁸ Hageline described: subject #1 as a 6'-6'2" white male weighing 190-230 pounds, wearing a black hat and gray shirt; subject #2 as a 5'9"-6' white male weighing 185 pounds, with black hair and glasses; subject #3 as a 5'8" white male with no further description; and subject #4 as a white female with blond hair.²²⁹ According to Louis's case supp, Hageline described how Koschman and subjects #1-2 were "calling names" back and forth.²³⁰ When Hageline turned his head to find a taxi, he heard a noise "like a snap sound" and saw Koschman on the ground.²³¹ Hageline reported that when he attended to Koschman, Koschman's lip was

²²⁴ See Special Grand Jury Exhibit 11 (CPD001698-CPD001701) (Case Supplementary Report 3201023 (approved May 17, 2004)).

²²⁵ See Louis, Edward, Special Grand Jury Tr. at 35:2-36:10 (Feb. 20, 2013).

²²⁶ See Villardita, Anthony, IGO Interview Rep. (Proffer) at 4-5 (Feb. 13, 2013).

²²⁷ See Special Grand Jury Exhibit 11 at CPD001698 (CPD001698-CPD001701) (Case Supplementary Report 3201023 (approved May 17, 2004)).

²²⁸ See Special Grand Jury Exhibit 11 at CPD001700 (CPD001698-CPD001701) (Case Supplementary Report 3201023 (approved May 17, 2004)).

²²⁹ See Special Grand Jury Exhibit 11 at CPD001700-CPD001701 (CPD001698-CPD001701) (Case Supplementary Report 3201023 (approved May 17, 2004)).

²³⁰ See Special Grand Jury Exhibit 11 at CPD001701 (CPD001698-CPD001701) (Case Supplementary Report 3201023 (approved May 17, 2004)).

²³¹ See Special Grand Jury Exhibit 11 at CPD001701 (CPD001698-CPD001701) (Case Supplementary Report 3201023 (approved May 17, 2004)). On August 8, 2012, as part of his testimony, Hageline read in a statement which, in part, stated, "[a]s the argument continued to go on, I walked a couple of steps away from the group to grab a cab. My back was to the groups at that time. Out of the corner of my eye, I saw a movement, and then Koschman stumbled back and fell into Division Street. I

swollen.²³² According to Louis's case supp, Hageline reported he did not see who actually struck Koschman, "but believed it was subject #1."²³³

Meanwhile, that same day, Yawger interviewed Bridget McCarthy.²³⁴ Bridget McCarthy informed Yawger that the two previously unidentified men who were with Kevin and her on Division Street the morning of the altercation were Vanecko and someone she knew only as "Craig."²³⁵ Bridget McCarthy described walking with Denham when someone in a group of "kids" walking the other direction "flicked" Denham's glasses off — starting an argument between this "kid" and Denham.²³⁶ According to Yawger's GPR, Vanecko and Kevin McCarthy then arrived after paying for the taxi, grabbed Denham, and said "let's go."²³⁷ Bridget McCarthy further described to Yawger that Koschman's friends were trying to "drag" Koschman away.²³⁸ According to Yawger's GPR, the McCarthys, Denham, and Vanecko all turned their backs and started to walk away.²³⁹ Bridget then stated that she was talking to the others while walking

did not actually see the punch thrown, but I heard a noise that could have been the sound of a punch or the sound of Koschman's head hitting the pavement. Koschman fell back — Koschman fell on his back, and he was facing up. Koschman's nose and mouth were bleeding, and there was blood bubbles in his spit. I don't remember Koschman trying to break his fall, which leads me to believe that he was knocked out before he hit the ground." Hageline, Shaun, Special Grand Jury Tr. at 10:1-11:2 (Aug. 8, 2012).

²³² See Special Grand Jury Exhibit 11 at CPD001701 (CPD001698-CPD001701) (Case Supplementary Report 3201023 (approved May 17, 2004)).

²³³ See Special Grand Jury Exhibit 11 at CPD001701 (CPD001698-CPD001701) (Case Supplementary Report 3201023 (approved May 17, 2004)). On August 8, 2012, as part of his testimony, Hageline read in a statement which, in part, stated, "I remember saying to one of the guys in the group, What the fuck did you do that for? This guy was built like a linebacker and it seemed like he could have beaten us all up. I think this was the guy who struck Koschman. He was the most threatening guy and was the biggest of all of them." Hageline, Shaun, Special Grand Jury Tr. at 11:3-13 (Aug. 8, 2012).

²³⁴ See General Progress Report (May 13, 2004) (CPD001541-CPD001543).

²³⁵ See General Progress Report at CPD001541 (May 13, 2004) (CPD001541-CPD001543). We know now that Bridget was referring to Denham. During Yawger's July 2013 special grand jury testimony, he stated he "was the very first person [at CPD] to become aware of [Vanecko's involvement]" in the April 25, 2004 incident. See Yawger, Ronald, Special Grand Jury Tr. at 48:6-11 (July 15, 2013).

²³⁶ See General Progress Report at CPD001541 (May 13, 2004) (CPD001541-CPD001543).

²³⁷ See General Progress Report at CPD001542 (May 13, 2004) (CPD001541-CPD001543).

²³⁸ See General Progress Report at CPD001542 (May 13, 2004) (CPD001541-CPD001543).

²³⁹ See General Progress Report at CPD001542 (May 13, 2004) (CPD001541-CPD001543).

away until she realized her husband, Denham, and Vanecko were not following her — at which point she turned around and saw Koschman on the ground.²⁴⁰ Bridget McCarthy stated she did not see whether Koschman was “hit or pushed.”²⁴¹ Yawger’s GPR reflects that Bridget McCarthy stated she then saw Denham and Vanecko run from the scene.²⁴² According to Yawger’s GPR, Bridget McCarthy then stated that police eventually released Kevin McCarthy and placed them in a taxi, whereupon the couple “went home,” which was false.²⁴³ As previously noted, Bridget McCarthy testified before the special grand jury in 2012 that her husband and she in fact met up with Vanecko and Denham at the Pepper Canister, after the bar had already closed.²⁴⁴

Dwyer, the McCarthys’ lawyer, informed Yawger that Vanecko was Mayor Daley’s nephew.²⁴⁵ According to Yawger, he was the first person at CPD to learn of Vanecko’s involvement in the Koschman matter²⁴⁶ – something he first was told by Bridget McCarthy during her May 13, 2004 interview.²⁴⁷ Yawger, upon learning that a relative of Mayor Daley was involved in the altercation, immediately notified Robert O’Leary and Chasen.²⁴⁸

However, Rybicki testified that CPD knew of the Mayor’s nephew’s (Vanecko) involvement only a “couple of days” after April 25, 2004, when the case arrived at Area 3. According to Rybicki, he was not present when the case first arrived at Area 3 but became aware of it hours later, or possibly the next day.²⁴⁹ Rybicki first learned of Vanecko’s involvement in

²⁴⁰ See General Progress Report at CPD001542 (May 13, 2004) (CPD001541-CPD001543).

²⁴¹ See General Progress Report at CPD001542 (May 13, 2004) (CPD001541-CPD001543).

²⁴² See General Progress Report at CPD001542 (May 13, 2004) (CPD001541-CPD001543).

²⁴³ See General Progress Report at CPD001543 (May 13, 2004) (CPD001541-CPD001543).

²⁴⁴ See McCarthy, Bridget, Special Grand Jury Tr. at 19:2-16 (Aug. 15, 2012).

²⁴⁵ See Yawger, Ronald, IGO Interview Tr. at 78:1-16 (July 1, 2011).

²⁴⁶ See Yawger, Ronald, Special Grand Jury Tr. at 48:6-11 (July 15, 2013).

²⁴⁷ See Yawger, Ronald, IGO Interview Tr. at 78:1-16 (July 1, 2011).

²⁴⁸ Yawger, Ronald, IGO Interview Rep. at 2 (July 1, 2011).

²⁴⁹ See Rybicki, Richard, Special Grand Jury Tr. at 33:18-24 (Mar. 27, 2013).

the incident “pretty shortly thereafter,” or within a “a couple of days” of learning about the case.²⁵⁰ According to Rybicki, he first learned of Vanecko’s involvement when the investigation was still in its early stages and Rita O’Leary and Clemens were working the case.²⁵¹ Although Rybicki could not recall the specific details of any conversations with Chasen about the case, he recalled having one conversation with Chasen where it came up that “holy crap, maybe the mayor’s nephew is involved.”²⁵² Likewise, Mayor Daley’s Deputy Chief of Staff for Public Safety, Matthew Crowl, was uncertain of the exact date, but believed he became aware of the Koschman matter shortly after the incident, when someone at CPD informed him that a nephew of Mayor Daley had been involved in a bar fight on the North Side, possibly in the Rush/Division Street area.²⁵³

Rybicki further testified that the assignment of the case to Yawger may have been influenced in part by Vanecko’s involvement.²⁵⁴ Rybicki testified that it was important to assign the case to someone competent “because of the fact of who was involved.”²⁵⁵ Rybicki also testified that Yawger “was a highly-experienced homicide detective, and [he thought] it was more a matter of, let’s be real careful here.”²⁵⁶

Following Bridget’s interview, Dwyer told Yawger that Vanecko would be represented

²⁵⁰ See Rybicki, Richard, Special Grand Jury Tr. at 34:16-35:18 (Mar. 27, 2013).

²⁵¹ See Rybicki, Richard, Special Grand Jury Tr. at 33:18-35:18, 67:6-10 (Mar. 27, 2013).

²⁵² See Rybicki, Richard, Special Grand Jury Tr. at 37:16-38:22 (Mar. 27, 2013). According to Area 3 attendance records, Rybicki was on furlough (or was otherwise not working) starting May 12, 2004 and ending May 27, 2004. See Area 3 Detective Division Attendance & Assignment Sheets (Apr. 24, 2004-May 28, 2004) (IG_004011-IG_004354). Thus, when Bridget McCarthy informed Yawger of Vanecko’s involvement, Rybicki had already begun his time away. The OSP has not been able to identify who it was that informed CPD of Vanecko’s involvement prior to Rybicki’s departure on May 12, 2004.

²⁵³ Crowl, Matthew, IGO Interview Rep. at 2 (Apr. 25, 2013).

²⁵⁴ See Rybicki, Richard, Special Grand Jury Tr. at 68:7-69:22 (Mar. 27, 2013).

²⁵⁵ See Rybicki, Richard, Special Grand Jury Tr. at 69:6-22 (Mar. 27, 2013).

²⁵⁶ See Rybicki, Richard, Special Grand Jury Tr. at 68:7-14 (Mar. 27, 2013).

by attorney Terence Gillespie.²⁵⁷ Yawger then called Gillespie and it was agreed that Gillespie would meet with Yawger on May 17 to schedule a time to bring in Vanecko for an interview (an interview which never occurred).²⁵⁸ On May 17, Gillespie met with Yawger at Area 3 headquarters.²⁵⁹ Yawger informed Gillespie of the circumstances surrounding the incident, and it was agreed that Vanecko would stand in a lineup on May 20.²⁶⁰ Thus, Yawger determined he would place Vanecko in a physical lineup (and communicated this to Vanecko's attorney) prior to speaking with Vanecko or the two other males with Bridget McCarthy at the scene of the incident.²⁶¹

On May 19, Dwyer arrived at Area 3 headquarters with his clients Kevin McCarthy and Denham.²⁶² Yawger interviewed Kevin McCarthy and Denham, and both admitted Vanecko was

²⁵⁷ See Special Grand Jury Exhibit 10 at CPD001124 (CPD001115-CPD001128) (Case Supplementary Report 3193543 (approved Nov. 10, 2004)). It appears from Yawger's notes that he was advised that both Terrence Gillespie and attorney Marc Martin represented Vanecko. See Special Grand Jury Exhibit 170 (IG_001525) (Handwritten Notes). This representation resulted from a referral made to Vanecko by Michael Daley, a Chicago attorney who is Vanecko's uncle and the brother of former Mayor Richard M. Daley. See Special Grand Jury Exhibit 57 at 2 (Michael Daley Special Grand Jury Declaration (Aug. 16, 2012)).

²⁵⁸ See Special Grand Jury Exhibit 10 at CPD001124 (CPD001115-CPD001128) (Case Supplementary Report 3193543 (approved Nov. 10, 2004)).

²⁵⁹ See Special Grand Jury Exhibit 10 at CPD001124 (CPD001115-CPD001128) (Case Supplementary Report 3193543 (approved Nov. 10, 2004)).

²⁶⁰ See Special Grand Jury Exhibit 10 at CPD001124 (CPD001115-CPD001128) (Case Supplementary Report 3193543 (approved Nov. 10, 2004)). According to GPRs authored by Yawger, on May 18, Yawger called Kohler, Allen, Copeland, Francis, and Connolly, and they all agreed to come to Area 3 headquarters on May 20 to view lineups and be interviewed by Assistant Cook County State's Attorneys. See General Progress Report (May 18, 2004) (CPD001091). Yawger also left voicemail messages for Hageline. See General Progress Report (May 18, 2004) (CPD001091). Lastly, Yawger left a note asking third watch detectives to contact Hageline to try and get him to view the lineups at the same time as his friends. See General Progress Report (May 18, 2004) (CPD001091).

²⁶¹ As of May 17, 2004, Yawger had not spoken with either Vanecko or Denham. While detectives had previously spoken with Kevin McCarthy on April 25, 2004, the version of events he relayed to detectives on that date was contradicted by his wife's statements to Yawger on May 13, 2004.

²⁶² See Special Grand Jury Exhibit 10 at CPD001124 (CPD001115-CPD001128) (Case Supplementary Report 3193543 (approved Nov. 10, 2004)).

the fourth member of their group during the altercation on Division Street on April 25.²⁶³ According to Yawger's GPRs, both Kevin McCarthy and Denham indicated they attended an engagement party the night of the incident and that after that party, they took a taxi, along with Bridget McCarthy and Vanecko, to Division Street.²⁶⁴ Denham told police that once on Division Street, he and Bridget McCarthy exited the cab while Kevin McCarthy and Vanecko stayed behind to pay the fare.²⁶⁵ According to Yawger's GPR, a "bunch of guys" bumped into Denham and knocked his glasses off.²⁶⁶ Yawger's notes indicate that Denham then began arguing with the other group — which involved "pushing and shoving," as well as "a lot of swearing and name calling."²⁶⁷ By this time, Kevin McCarthy and Vanecko had caught up to Denham and Bridget McCarthy.²⁶⁸

According to the GPR of Kevin McCarthy's interview, he and Vanecko stepped in

²⁶³ See Special Grand Jury Exhibit 10 at CPD001124, CPD001126 (CPD001115-CPD001128) (Case Supplementary Report 3193543 (approved Nov. 10, 2004)).

²⁶⁴ See General Progress Report at CPD001100 (May 19, 2004) (CPD001100-CPD001103); General Progress Report at CPD001097 (May 19, 2004) (CPD001097-CPD001099). According to her case supp, Bridget McCarthy also informed Yawger that the four of them "were at an engagement party for mutual friends." See Special Grand Jury Exhibit 10 at CPD001123 (CPD001115-CPD001128) (Case Supplementary Report 3193543 (approved Nov. 10, 2004)). There is no indication that Yawger ever inquired who else was at the engagement party or whose engagement party they attended. In 2012, the OSP learned through witness interviews that the engagement party on April 24, 2004 was for Katherine Daley, Vanecko's cousin and the daughter of attorney Michael Daley. See Daley, Katherine, IGO Interview Rep. (Proffer) at 1-2 (July 27, 2012); Special Grand Jury Exhibit 56 at 2 (Jill Denham Special Grand Jury Declaration (Aug. 28, 2012)).

On May 25, 2004, Bridget McCarthy sent Katherine Daley, her close friend, an e-mail referencing the Koschman incident. In the e-mail, Bridget McCarthy explains that she cannot discuss the night of the incident because "it is best for myself and RJ [Vanecko] that it not be discussed and anyone know what happened." Bridget McCarthy-Katherine Daley e-mail at ACE031977 (May 10-25, 2004) (ACE031977-ACE031989). Bridget McCarthy adds, "The evening should be kept between the four of us present" Bridget McCarthy-Katherine Daley e-mail at ACE031977 (May 10-25, 2004) (ACE031977-ACE031989).

²⁶⁵ See General Progress Report at CPD001097 (May 19, 2004) (CPD001097-CPD001099).

²⁶⁶ See General Progress Report at CPD001097 (May 19, 2004) (CPD001097-CPD001099).

²⁶⁷ See General Progress Report at CPD001097 (May 19, 2004) (CPD001097-CPD001099).

²⁶⁸ See General Progress Report at CPD001098 (May 19, 2004) (CPD001097-CPD001099).

between the two groups and tried to separate them by pushing Craig along.²⁶⁹ According to Kevin McCarthy, as he and Vanecko attempted to remove Denham from the scene, Koschman broke free from his friends, pushed his way past Vanecko and Kevin McCarthy, and attempted to “get at” Denham.²⁷⁰ The GPR further states that Kevin McCarthy stepped in the way, while Koschman’s friends grabbed Koschman and restrained him again.²⁷¹ According to Yawger’s GPR, Kevin McCarthy told Yawger that Koschman attempted to attack Denham “physically and verbally” but was restrained by his friends.²⁷²

Kevin McCarthy also told Yawger that, at that point, all four turned their backs and began walking eastbound on Division Street away from “the group of kids.”²⁷³ The incident “was over” as far as Kevin McCarthy was concerned.²⁷⁴ Yawger’s GPR of his interview with Denham similarly relayed that Denham “thought everything was over” at that point.²⁷⁵ Denham further described that as he was walking away, Vanecko was behind him (while the McCarthys were ahead), he felt a “hard jolt from behind,” and next thing he knew, he and Vanecko were running down the street.²⁷⁶

According to Yawger’s GPRs for both interviews, both Denham and Kevin McCarthy

²⁶⁹ See General Progress Report at CPD001101 (May 19, 2004) (CPD001100-CPD001103).

²⁷⁰ See General Progress Report at CPD001101 (May 19, 2004) (CPD001100-CPD001103).

²⁷¹ See General Progress Report at CPD001101 (May 19, 2004) (CPD001100-CPD001103).

²⁷² See General Progress Report at CPD001102 (May 19, 2004) (CPD001100-CPD001103).

²⁷³ See General Progress Report at CPD001102 (May 19, 2004) (CPD001100-CPD001103).

²⁷⁴ See General Progress Report at CPD001102 (May 19, 2004) (CPD001100-CPD001103).

²⁷⁵ See General Progress Report at CPD001098 (May 19, 2004) (CPD001097-CPD001099).

²⁷⁶ See General Progress Report at CPD001098 (May 19, 2004) (CPD001097-CPD001099). On August 15, 2012, as part of his testimony, Denham read in a statement which, in part, stated, “[a]t some point I turned and began walking away. After walking away, I felt a jolt or some force in my back, and I started running. I do not know what jolted me in the back. I did not know if the jolt was a push encouraging me to run or if it was an aggressive act, but I recall reflectively [sic] reacting to the jolt and beginning to run. I know at some point R. J. Vanecko was running with me.” Denham, Craig, Special Grand Jury Tr. at 20:4-20 (Aug. 15, 2012).

turned their backs to walk away and did not see who struck Koschman.²⁷⁷ Denham told Yawger he did not see Koschman on the ground, did not see anyone get hit or pushed, and did not know why he was running — speculating it could have been because he did not want to be “jumped” or it may have been fear of getting into trouble for public intoxication.²⁷⁸ At the conclusion of the interviews, Yawger made arrangements with Kevin McCarthy and Denham’s attorney Dwyer to have both his clients stand in lineups the following day, May 20.²⁷⁹ While Kevin McCarthy had lied to police on two separate occasions about the identities of the other members of his group, police did not seek charges against him for obstructing justice.²⁸⁰

²⁷⁷ See General Progress Report at CPD001098 (May 19, 2004) (CPD001097-CPD001099); General Progress Report at CPD001102-CPD001103 (May 19, 2004) (CPD001100-CPD001103).

²⁷⁸ See General Progress Report at CPD001098 (May 19, 2004) (CPD001097-CPD001099).

²⁷⁹ See Yawger, Ronald, Special Grand Jury Tr. 35:5-6 (July 15, 2013).

²⁸⁰ According to detectives, obstruction of justice or similar charges were not considered against Kevin McCarthy because, in essence, there is no statute prohibiting lying to the police. For example, Molloy noted that even though Kevin McCarthy lied to police during its investigation, CPD did not seek charges because “there’s no law in Chicago against lying to the police.” See Molloy, James, Kroll Interview Rep. at 7 (Dec. 7, 2012). Chasen explained further that CPD detectives are lied to by witnesses on a daily basis, something that he too believes is not against the law. See Chasen, Michael, IGO Interview Rep. at 10 (Nov. 27, 2012). While it is true there is no state law that directly criminalizes lying to a police officer under all circumstances, there is a state obstruction of justice statute which could cover such behavior if the requisite elements are met. See 720 ILCS 5/31-4 (West 2013) (“(a) A person obstructs justice when, with intent to prevent the apprehension or obstruct the prosecution or defense of any person, he or she knowingly commits any of the following acts: (1) Destroys, alters, conceals or disguises physical evidence, plants false evidence, furnishes false information; or (2) Induces a witness having knowledge material to the subject at issue to leave the State or conceal himself or herself; or (3) Possessing knowledge material to the subject at issue, he or she leaves the State or conceals himself. . .”). The statute of limitations for this offense is three years. 720 ILCS 5/3-5(b) (West 2011).

Former Superintendent Cline noted that lying to police is so common that Kevin McCarthy’s actions did not rise to asking for charges. See Cline, Phillip, IGO Interview Rep. at 6 (Dec. 28, 2012). And according to Robert O’Leary, even though police are lied to very often, charges for obstruction of justice are never filed. See Special Grand Jury Exhibit 123 at 11 (O’Leary, Robert, Kroll Interview Rep. (Oct. 8, 2012)). Lastly, while Rita O’Leary firmly believes that “Kevin’s lies hurt [CPD’s] investigation,” she cannot remember a single instance of a witness being charged with obstruction of justice. See Special Grand Jury Exhibit 122 at 6 (O’Leary, Rita, Kroll Interview (Oct. 5, 2012)). 2004 Deputy Chief of Detectives Richard Kobel stated obstruction charges can happen, while not typical, if the lies told in any instance are particularly harmful to a case. See Kobel, Richard, IGO Interview Rep. at 5-6 (Jan. 17, 2013).

f. Certain Issues Stemming from Area 3's Continuing Work

Although according to Yawger's GPRs, Kevin McCarthy stated he later left the scene in a taxi and Denham stated he accompanied Vanecko to another bar after the incident, there is no indication in any of the GPRs or case supps that Yawger asked either Denham or Kevin McCarthy where they went after the incident and whether they spoke with Vanecko about the matter. In fact, during his July 2013 testimony before the special grand jury, Yawger stated he never asked them those questions, though he did acknowledge he "should have asked them that."²⁸¹ In 2012, the McCarthys testified before the special grand jury that they met Denham and Vanecko at the Pepper Canister immediately after the incident.²⁸² Denham also testified that although he could not recall going to the Pepper Canister after the incident, he was told by Vanecko's attorney, Terence Gillespie, that both he and Vanecko in fact took a taxi there afterwards.²⁸³ As stated previously, the Pepper Canister was closed by the time the altercation happened.²⁸⁴ Kevin McCarthy and Denham testified that they did not speak about the incident, while Bridget McCarthy testified they may have spoken about the fact that her husband was detained, but nothing else.²⁸⁵

Area 3 detectives also did not seek phone records; therefore, could not discover that Vanecko and Bridget McCarthy called each other several times between 3:30 a.m. and 4 a.m.

²⁸¹ See Yawger, Ronald, Special Grand Jury Tr. at 57:4-11 (July 15, 2013).

²⁸² See McCarthy, Kevin, Special Grand Jury Tr. at 22:8-19 (Aug. 15, 2012); McCarthy, Bridget, Special Grand Jury Tr. at 19:2-8 (Aug. 15, 2012).

²⁸³ See Denham, Craig, Special Grand Jury Tr. at 21:9-17 (Aug. 15, 2012).

²⁸⁴ See McCarthy, Bridget, Special Grand Jury Tr. at 53:24-54:24 (Aug. 15, 2012); Farley, Pam, Special Grand Jury Tr. at 22:16-23:6 (Jan. 23, 2013). The special grand jury issued subpoenas to the Pepper Canister seeking records identifying employees working the night of the incident, receipts and credit card records, and the bar's liquor license for 2004, but was unable to obtain any employment or payment records from 2004. Pam Farley, co-owner of the Pepper Canister in 2004, testified before the special grand jury that employment and payment records could not be located due to their age and because the records had been stored in a basement that had flooded. See Farley, Pam, Special Grand Jury Tr. at 15:22-20:11 (Jan. 23, 2013). The OSP also interviewed Ivan McCullagh, who received ownership of the Pepper Canister from Farley in 2012, and who was the manager of the bar in 2004 — as well as Steve Bringas and Dominic O'Mahony, two bartenders at the Pepper Canister in 2004. No one recalled letting the McCarthys, Denham, and Vanecko into the Pepper Canister after the bar had closed.

²⁸⁵ See McCarthy, Kevin, Special Grand Jury Tr. at 23:2-8 (Aug. 15, 2012); McCarthy, Bridget, Special Grand Jury Tr. at 57:2-5 (Aug. 15, 2012); see also Denham, Craig, Special Grand Jury Tr. at 21:15-17, 40:3-18 (Aug. 15, 2012) (Denham testified that he has no memory of any conversations there).

leading up to their meeting at the Pepper Canister.²⁸⁶

3. May 20, 2004 (the Lineups)

Beginning May 17, 2004, Yawger started making arrangements, through their counsel, to have Vanecko, Kevin McCarthy, and Denham stand in lineups at Area 3 headquarters on May 20.²⁸⁷ Some CPD officers interviewed by the OSP described a “buzz” at Area 3 headquarters on the day of the lineups because it had become known that the Mayor’s nephew (Vanecko) was going to be a lineup participant.²⁸⁸ Yawger and Det. Patrick Flynn conducted the lineups, with Yawger standing outside the lineup room with witnesses and Flynn standing inside the lineup room with those individuals being viewed.²⁸⁹

a. Timing and Need for Lineups

In this case, however, Assistant State’s Attorney (“ASA”) Darren O’Brien, head of SAO’s Felony Review unit in 2004, testified before the special grand jury in 2013 that he is not sure whether he requested the lineups held on May 20, 2004.²⁹⁰ According to his 2013 testimony before the special grand jury, Yawger arranged the lineups.²⁹¹

Before the lineups were even conducted, detectives already believed Vanecko was the

²⁸⁶ See Special Grand Jury Exhibit 32 at SPR000024 (SPR000023-SPR000027) (Sprint phone charges for phone number associated with Bridget McCarthy reflecting calls between Bridget McCarthy and Vanecko’s cellular phones).

²⁸⁷ See Yawger, Ronald, Special Grand Jury Tr. at 35:5-6 (July 15, 2013) (stating that he arranged the May 20, 2004 lineups) (May 1, 2004).

²⁸⁸ See, e.g., Special Grand Jury Exhibit 122 at 9 (O’Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012)).

²⁸⁹ See Special Grand Jury Exhibit 12 at CPD001107 (CPD001105-CPD1108) (Case Supplementary Report 3222163 (approved Nov. 8, 2004)). Det. John Griffin took the photos of the first lineup. See Special Grand Jury Exhibit 12 at CPD001107 (CPD001105-CPD001108) (Case Supplementary Report 3222163 (approved Nov. 8, 2004)). Evidence Technician Willard Streff took the photos of the second lineup. See Special Grand Jury Exhibit 13 at CPD001113 (CPD001111-CPD001114) (Case Supplementary Report 3222388 (approved Nov. 10, 2004)).

²⁹⁰ See O’Brien, Darren, Special Grand Jury Tr. at 33:16-34:1 (May 8, 2013). Although in O’Brien’s opinion, “In this case lineups were absolutely necessary to establish the identity of any prospective offender” See O’Brien, Darren, Special Grand Jury Tr. at 34:23-35:1 (May 8, 2013).

²⁹¹ Yawger, Ronald, Special Grand Jury Tr. at 35:5-6 (July 15, 2013).

person who had struck Koschman. For instance, Yawger has stated that he knew Vanecko was the person who struck Koschman based on the witnesses' statements and through the process of elimination.²⁹² For example, Koschman's friends (Allen and Copeland — the only two eyewitnesses to the actual physical contact between Vanecko and Koschman) had provided definitive statements that, in sum and substance, the largest of the males in the other group had punched Koschman. Furthermore, Kevin McCarthy and Denham told Yawger they did not hit Koschman, and it was known the female (Bridget McCarthy) also did not strike Koschman.²⁹³ Based on appearance, Yawger could tell Vanecko was the "biggest guy" in the group.²⁹⁴ In other words, according to Yawger, Vanecko was "the guy" (meaning the offender).²⁹⁵ Additionally, Flynn testified that Area 3 detectives did not consider Kevin McCarthy or Denham to be suspects at the time they stood in the lineups.²⁹⁶ Despite the detectives' beliefs, based on the evidence, that Vanecko was the offender, the lineups were still held.

With regard to timing, the lineups were held nearly a month after the altercation, and were conducted without first attempting to speak with Vanecko. Superintendent Cline stated that lineups should be held as soon as possible after an incident.²⁹⁷ Indeed, it is especially important to hold lineups as soon after an incident as possible where, as here, the incident occurred late at night between strangers²⁹⁸ and lasted but a few minutes.²⁹⁹

In 2012, Chasen explained to the OSP that conducting a lineup was the right thing to do.

²⁹² See Yawger, Ronald, IGO Interview Tr. at 94:16-96:4 (July 1, 2011); see also Yawger, Ronald, Special Grand Jury Tr. at 50:5-17 (July 15, 2013).

²⁹³ See Yawger, Ronald, IGO Interview Tr. at 94:16-96:4 (July 1, 2011).

²⁹⁴ See Yawger, Ronald, IGO Interview Tr. at 94:16-96:4 (July 1, 2011).

²⁹⁵ See Yawger, Ronald, IGO Interview Tr. at 94:16-96:4 (July 1, 2011).

²⁹⁶ See Flynn, Patrick, Special Grand Jury Tr. at 45:3-46:14 (Mar. 13, 2013).

²⁹⁷ See Cline, Philip, IGO Interview Rep. at 3 (Dec. 28, 2012); Yawger, Ronald, Special Grand Jury Tr. at 50:24-51:5 (July 15, 2013).

²⁹⁸ See O'Brien, Darren, Special Grand Jury Tr. at 34:6-8 (May 8, 2013) (stating "when parties are complete strangers, conducting a lineup sooner is better than later.").

²⁹⁹ See Flynn, Patrick Special Grand Jury Tr. at 29:18-30:15 (Mar. 13, 2013); O'Brien, Darren, Special Grand Jury Tr. at 34:2-8 (May 8, 2013); Yawger, Ronald, Special Grand Jury Tr. at 51:13-15 (July 15, 2013).

He noted that detectives could not only presume Vanecko was the offender, but rather an identification had to be made by a witness.³⁰⁰ Similarly, Flynn believes that even if CPD can identify a witness through process of elimination, a lineup is still necessary so witnesses can identify the person they saw commit the offense³⁰¹ — a sentiment echoed in 2013 by 2004 Deputy Superintendent Steven Peterson.³⁰² Likewise, Superintendent Cline noted that even if a suspect can be identified through process of elimination, holding a lineup helps ensure that CPD has the correct offender.³⁰³ Indeed, despite the length of time between the April 25, 2004 incident and the May 20, 2004 lineups, according to Yawger, there still was no doubt in his mind that the witnesses would pick Vanecko out of the lineup.³⁰⁴ Furthermore, Giralamo noted that SAO requests lineups for all homicide cases when feasible.³⁰⁵ Chasen also noted that lineups are conducted in the “majority” of homicide cases.³⁰⁶

b. The Lineups

The first lineup consisted of six lineup participants: Vanecko along with five CPD officers who acted as “fillers.”³⁰⁷ Once Area 3 has a description of the suspect who will stand in the lineup, detectives try to find “fillers” matching the suspect’s description somewhere in the vicinity, including individuals in lockup or volunteers in and around the building.³⁰⁸ In this case, according to detectives, finding “fillers” on the day of the lineup who matched Vanecko’s description proved somewhat difficult. For example, Yawger recalls delays in finding “big,”

³⁰⁰ See Chasen, Michael, IGO Interview Rep. at 6 (Nov. 27, 2012).

³⁰¹ See Flynn, Patrick, Special Grand Jury Tr. at 74:3-17, 78:15-20 (Mar. 13, 2013).

³⁰² See Peterson, Steve, IGO Interview Tr. at 99:8-100:18 (Jan. 10, 2012).

³⁰³ See Cline, Philip, IGO Interview Rep. at 3 (Dec. 28, 2012).

³⁰⁴ See Yawger, Ronald, IGO Interview Tr. at 4:10-17, 26:17-24 (July 1, 2011).

³⁰⁵ See Giralamo, Anthony, IGO Interview Rep. at 7 (Dec. 21, 2012).

³⁰⁶ See Chasen, Michael, IGO Interview Rep. at 6 (Nov. 27, 2012).

³⁰⁷ See Special Grand Jury Exhibit 12 at CPD001107 (CPD001105-CPD001108) (Case Supplementary Report 3222163 (approved Nov. 8, 2004)).

³⁰⁸ See Flynn, Patrick, Special Grand Jury Tr. at 17:1-14 (Mar. 13, 2013).

white male “fillers.”³⁰⁹ In fact, Flynn asked Area 3 lockup to identify anyone matching Vanecko’s description, and he personally checked the courtroom areas and other floors of headquarters to see if he could find “fillers.”³¹⁰ Flynn ultimately selected “fillers” from available police officers.³¹¹

All six of the participants in the first lineup were white males of similar height, weight, and age.³¹² Vanecko chose to stand in position number two.³¹³ Vanecko’s lawyer, Terence

³⁰⁹ See Yawger, Ronald, IGO Interview Tr. at 1:16-18 (July 1, 2011).

³¹⁰ See Flynn, Patrick, Special Grand Jury Tr. at 23:14-23 (Mar. 13, 2013).

³¹¹ See Flynn, Patrick, Special Grand Jury Tr. at 23:24-24:11, 43:3-9 (Mar. 13, 2013). See also General Order 88-18 at CPD095827 (effective Sept. 24, 1988) (CPD095827-CPD095828) (stating “Police officers should not be used [as ‘fillers’] unless other alternatives have been exhausted.”).

³¹² See Special Grand Jury Exhibit 12 at CPD001108 (CPD001105-CPD001108) (Case Supplementary Report 3222163 (approved Nov. 8, 2004)).

On May 13, 2004, Hageline told detectives the largest male in the other group (Vanecko) was wearing a black hat the night of the altercation on Division Street. Special Grand Jury Exhibit 11 at CPD001700-CPD001701 (CPD001698-CPD001701) (Case Supplementary Report 3201023 (approved May 17, 2004)). Hageline also told detectives that one of the other males in the group (Denham) was wearing glasses – something Bridget McCarthy, Kevin McCarthy, and Denham himself have also stated. See Special Grand Jury Exhibit 11 at CPD001700-CPD001701 (CPD001698-CPD001701) (Case Supplementary Report 3201023 (approved May 17, 2004)); see Special Grand Jury Exhibit 10 at CPD001123, CPD001126 (CPD001115-CPD001128) (Case Supplementary Report 3193543 (approved Nov. 10, 2004)); see McCarthy, Kevin, Special Grand Jury Tr. at 16:9-14, 41:16-19 (Aug. 15, 2012). Even so, the Vanecko lineup participants did not wear hats, nor did the Denham/Kevin McCarthy lineup participants wear glasses. According to Flynn, typically speaking, if a witness identified something distinctive about a potential suspect, such as a hat, he would try to mimic that characteristic in the lineup. See Flynn, Patrick, Special Grand Jury Tr. at 26:24-27:17 (Mar. 13, 2013). Griffin stated that depending on the circumstances of the case, if a witness identifies a potential suspect as having worn a hat or glasses, he would have the lineup participants put such items on and take them off while witnesses viewed the lineup. See Griffin, John, IGO Interview Rep. at 3, 5-6 (Dec. 12, 2012). The decision as to whether the lineup participants would temporarily wear either was Yawger’s to make. See Flynn, Patrick, Special Grand Jury Tr. at 38:5-9 (Mar. 13, 2013). Yawger stated that, despite Hageline’s statement that the offender was wearing a hat, he did not think it was an important factual issue in the case, and he did not think a hat would make any difference, as he was sure Vanecko would be identified by the witnesses. See Yawger, Ronald, IGO Interview Tr. at 42:17-43:9 (July 1, 2011).

³¹³ See Special Grand Jury Exhibit 12 at CPD001108 (CPD001105-CPD001108) (Case Supplementary Report 3222163 (approved Nov. 8, 2004)).

Gillespie, was also present.³¹⁴ Detectives were unable to interview Vanecko prior to his participation in the lineup, which is not uncommon, especially for suspects represented by counsel.³¹⁵

The first lineup was viewed separately by six witnesses: Connolly, Kohler, Hageline, Allen, Copeland, and Francis.³¹⁶ Connolly, Kohler, Copeland and Francis were unable to positively identify anyone.³¹⁷ Hageline identified the officer in the fourth position as the offender (but added he was not positive).³¹⁸ And Allen identified the officer in the first position as the offender (but added he was not positive).³¹⁹ It has been suggested by the press that Vanecko, in preparation for the lineup, attempted to change his appearance from how he looked the night of the incident (including potentially shaving his head). However, the OSP did not uncover evidence that substantiated this notion.

The second lineup on May 20, 2004, also consisted of six lineup participants: Kevin McCarthy, Denham, and four “fillers” (one of whom was a CPD officer and another an ASA).³²⁰ All six lineup participants were white males of similar height, weight, and appearance.³²¹ Kevin

³¹⁴ See Special Grand Jury Exhibit 12 at CPD001107 (CPD001105-CPD001108) (Case Supplementary Report 3222163 (approved Nov. 8, 2004)).

³¹⁵ See Molloy, James, Kroll Interview Rep. at 6 (Dec. 7, 2012); see Chasen, Michael, IGO Interview Rep. at 6 (Nov. 27, 2012).

³¹⁶ See Special Grand Jury Exhibit 12 at CPD001107 (CPD001105-CPD001108) (Case Supplementary Report 3222163 (approved Nov. 8, 2004)).

³¹⁷ See Special Grand Jury Exhibit 12 at CPD001108 (CPD001105-CPD001108) (Case Supplementary Report 3222163 (approved Nov. 8, 2004)).

³¹⁸ See Special Grand Jury Exhibit 12 at CPD001108 (CPD001105-CPD001108) (Case Supplementary Report 3222163 (approved Nov. 8, 2004)).

³¹⁹ See Special Grand Jury Exhibit 12 at CPD001108 (CPD001105-CPD001108) (Case Supplementary Report 3222163 (approved Nov. 8, 2004)).

³²⁰ See Special Grand Jury Exhibit 13 at CPD001113-CPD001114 (CPD001111-CPD001114) (Case Supplementary Report 3222388 (approved Nov. 10, 2004)).

³²¹ See Special Grand Jury Exhibit 13 at CPD001114 (CPD001111-CPD001114) (Case Supplementary Report 3222388 (approved Nov. 10, 2004)).

McCarthy chose to stand in position number one, while Denham selected position five.³²² Their lawyer, Dwyer, was also present.³²³

The lineup was viewed separately by the same six witnesses: Connolly, Kohler, Hageline, Allen, Copeland, and Francis. Connolly, Kohler, and Copeland were unable to positively identify anyone.³²⁴ Hageline identified Denham as the person who was not only initially placed in handcuffs by the police the night of the incident,³²⁵ but also as one of the guys who tried breaking up the altercation.³²⁶ Allen identified Kevin McCarthy as not only the guy who was with the girl (Bridget McCarthy) and placed in handcuffs, but also as someone who tried breaking up the altercation.³²⁷ Lastly, Francis identified Kevin McCarthy as the person who was with the female (Bridget McCarthy) and who was stopped by the police after the incident, but Francis did not remember what role Kevin McCarthy played during the altercation.³²⁸

In summary, according to CPD reports on the lineup, on May 20, 2004, neither Koschman's friends nor the bystanders were able to positively identify Vanecko in a lineup as the person who struck Koschman.

4. May 20, 2004 (Felony Review Visit)

According to O'Brien, the role of SAO's Felony Review unit is to "review the

³²² See Special Grand Jury Exhibit 13 at CPD001114 (CPD001111-CPD001114) (Case Supplementary Report 3222388 (approved Nov. 10, 2004)).

³²³ See Special Grand Jury Exhibit 13 at CPD001113 (CPD001111-CPD001114) (Case Supplementary Report 3222388 (approved Nov. 10, 2004)).

³²⁴ See Special Grand Jury Exhibit 13 at CPD001113-CPD001114 (Case Supplementary Report 3222388 (approved Nov. 10, 2004)).

³²⁵ Kevin McCarthy was the person in the Vanecko group who was placed in handcuffs the night of the altercation, not Denham. Tremore, Edwin, Kroll Interview Rep. at 3 (Sept. 18, 2012).

³²⁶ See Special Grand Jury Exhibit 13 at CPD001114 (CPD001111-CPD001114) (Case Supplementary Report 3222388 (approved Nov. 10, 2004)).

³²⁷ See Special Grand Jury Exhibit 13 at CPD001114 (CPD001111-CPD001114) (Case Supplementary Report 3222388 (approved Nov. 10, 2004)).

³²⁸ See Special Grand Jury Exhibit 13 at CPD001114 (CPD001111-CPD001114) (Case Supplementary Report 3222388 (approved Nov. 10, 2004)).

sufficiency of the evidence gathered by the police.”³²⁹ For homicides, such as the Koschman case, when contacted by CPD, the assigned Felony Review ASA reports to the CPD detective, meets with the investigating detective, speaks with all available parties, including the suspect if possible, reads available reports, and examines all available evidence to decide what charges to approve, if any.³³⁰ When called by detectives to review a case, a Felony Review ASA can approve charges, reject charges, or classify the case as a continuing investigation (“CI”).³³¹

³²⁹ See O’Brien, Darren, Special Grand Jury Tr. at 16:22-24 (May 8, 2013).

³³⁰ SAO approval is typically required in order for police to charge any person with a felony. See Boliker, Shauna, IGO Interview Rep. at 1-2 (Mar. 25, 2013); see O’Brien, Darren, Special Grand Jury Tr. at 17:8-12 (May 8, 2013); see Milan, Bob, Special Grand Jury Tr. at 6:17-19 (Apr. 24, 2013). In 2004, SAO’s Felony Review unit consisted of one Felony Review supervisor, three Felony Review deputy supervisors, and four Felony Review teams of approximately 10 ASAs each. See Milan, Bob, Special Grand Jury Tr. at 5:22-6:7 (Apr. 24, 2013); see O’Brien, Darren, Special Grand Jury Tr. at 15:19-22 (May 8, 2013). Each of the four teams worked three consecutive days in a row in 12-hour shifts, so that the Felony Review unit operated 24 hours a day, 365 days a year. See Milan, Bob, Special Grand Jury Tr. at 6:6-15 (Apr. 24, 2013).

CPD officers are to call Felony Review dispatchers, who are on duty 24 hours a day and were charged with paging the on-duty Felony Review ASAs when a CPD officer called requesting Felony Review assistance. See O’Brien, Darren, Special Grand Jury Tr. at 16:1-12 (May 8, 2013); see Milan, Bob, Special Grand Jury Tr. at 8:17-18 (Apr. 24, 2013); see Kirk, Daniel, IGO Interview Rep. at 2 (Mar. 26, 2013). The dispatchers provided the assigned ASA with a contact, such as the detective, to facilitate the review of the case. See Kirk, Daniel, IGO Interview Rep. at 2 (Mar. 26, 2013).

According to O’Brien, detectives would occasionally contact him directly with regard to a request for Felony Review. See O’Brien, Darren, Special Grand Jury Tr. at 16:1-12 (May 8, 2013). The Felony Review unit dispatchers maintained a log of both the time that CPD called Felony Review and the time that the assigned ASA finished his or her review of the case. See O’Brien, Darren, Special Grand Jury Tr. at 16:15-22 (May 8, 2013). The time that the ASA left the Felony Review office to meet with the calling CPD officer was not recorded in the log. See O’Brien, Darren, Special Grand Jury Tr. at 16:20-22 (May 8, 2013). This log could also record whether the ASA was reviewing the case solely as an “advice.” See O’Brien, Darren, IGO Interview Rep. (Proffer) at 4 (Feb. 5, 2013). According to current SAO Chief Deputy Walt Hehner, Felony Review ASAs contacted the Felony Review dispatcher after reviewing a case to inform them of whether charges were approved or rejected. See Special Grand Jury Exhibit 151 at 3 (Hehner, Walt, IGO Interview Rep. (Mar. 11, 2013)).

³³¹ See Kirk, Daniel, IGO Interview Rep. at 2 (Mar. 26, 2013). When Felony Review CI’s a case, that means CPD needs to obtain additional evidence before a charging decision can be made. See O’Brien, Darren, Special Grand Jury Tr. at 19:1-12 (May 8, 2013); see Murray, Bernard, IGO Interview Rep. at 3 (Feb. 22, 2013); see Devine, Richard, IGO Interview Rep. at 2 (Apr. 9, 2013). According to Murray, it is common, especially in homicide cases, for a case to be CI’d. See Murray, Bernard, IGO Interview Rep. at 3 (Feb. 22, 2013). In those instances, the ASA would actually create a “to-do list” of steps that CPD should follow to obtain approval of charges. See Milan, Bob, Special Grand Jury Tr. at 10:21-11:5, 16:19-17:2 (Apr. 24, 2013).

However, a Felony Review ASA can also be requested by CPD to review a particular case for the sole purpose of providing guidance to detectives about that case, which is commonly referred to as an “advice.”³³² Generally speaking, CPD would request an “advice” from Felony Review when detectives were not ready to seek charges, but instead, wanted to know SAO’s opinion on whether and what charges may be appropriate for a particular case.³³³

a. SAO Felony Review Unit Contacted

On May 20, 2004, the day of the lineups, O’Brien visited Area 3 to interview witnesses and consult detectives regarding potential charges in the Koschman case.³³⁴ During his 2013 special grand jury testimony, O’Brien could not pinpoint an exact date that he was first contacted

³³² See O’Brien, Darren, Special Grand Jury Tr. at 19:13-17 (May 8, 2013). According to Hehner, approximately 20 percent of CPD calls to Felony Review are for “advices.” See Special Grand Jury Exhibit 151 at 11 (Hehner, Walt, IGO Interview Rep. (Mar. 11, 2013)). However, according to Kirk, calls for “advices” seldom occur. See Kirk, Daniel, IGO Interview Rep. at 2 (Mar. 26, 2013).

³³³ O’Brien, Darren, Special Grand Jury Tr. at 19:13-17 (May 8, 2013); Kirk, Daniel, IGO Interview Rep. at 2 (Mar. 26, 2013); Murray, Bernard, IGO Interview Rep. at 3 (Feb. 22, 2013); Milan, Bob, Special Grand Jury Tr. at 10:16-20 (Apr. 24, 2013).

³³⁴ See Special Grand Jury Exhibit 10 at CPD001127 (CPD001115-CPD001128) (Case Supplementary Report 3193543 (approved Nov. 10, 2004)). A difference of opinion exists as to whether it is unusual for the head of Felony Review to conduct a review himself. See Special Grand Jury Exhibit 122 at 9 (O’Leary, Rita, Kroll Interview Rep. (Oct. 5, 2012)) (O’Brien’s review of a case was not “an everyday occurrence”). According to Rybicki, he had never seen the Felony Review Chief come to a detective area to review a case, calling the occurrence unusual. See Rybicki, Richard, Special Grand Jury Tr. at 75:21-76:2 (Mar. 27, 2013). Rybicki acknowledged that, in this respect, the Koschman matter was treated differently than other cases because of the persons involved and because the case was “newsworthy.” See Rybicki, Richard, Special Grand Jury Tr. at 100:12-18 (Mar. 27, 2013); see also Rybicki, Richard, Special Grand Jury Tr. at 46:20-47:1 (Mar. 27, 2013) (He said whoever told him about calling in the State’s Attorney said that they did so because “they wanted to be thorough. They wanted, you know, independent review of what their investigation had led to so far. And that they were crossing all the T’s and dotting the I’s.”) According to current SAO Chief of Staff Kirk, it is not completely unheard of for the head of Felony Review to review a case, but that it was not typical and did not occur on a daily basis. See Kirk, Daniel, IGO Interview Rep. at 3 (Mar. 26, 2013). But see Devine, Richard, IGO Interview Rep. at 2 (Aug. 8, 2013) (stating he was not shocked or surprised to learn that O’Brien went to Area 3 to review the Koschman matter because in his (State’s Attorney Devine’s) opinion it was not unusual for the head of Felony Review to personally review a case); Milan, Bob, IGO Interview Rep. at 2 (Aug. 8, 2013) (stating that in his opinion it was not unusual for the head of Felony Review to personally review a case, and that when he (Milan) was the head of Felony Review, he personally reviewed cases approximately 12 to 24 times a year). O’Brien testified before the special grand jury that he took the Koschman matter himself “because [he] wanted to have firsthand information about the case by interviewing the witnesses [himself] to make sure [SAO] didn’t miss anything, and so that [he] could answer any questions of [his] bosses.” O’Brien, Darren, Special Grand Jury Tr. at 32:1-6 (May 8, 2013).

by Yawger regarding the Koschman case, but he testified that he was likely contacted by phone the day before the lineups (May 19, 2004), as well as the day of the lineups (May 20, 2004).³³⁵ According to both O'Brien and Yawger, this was the first contact CPD made with SAO regarding the Koschman case.³³⁶ O'Brien testified that he learned that Mayor Daley's relative was involved during these phone calls.³³⁷ Yawger told the special grand jury in July 2013 that he would not have called the head of Felony Review (O'Brien) if Vanecko had not been Mayor Daley's nephew.³³⁸

Yawger also told the special grand jury that he initially called O'Brien for an "advice" on the Koschman case, but then [Yawger] shifted gears and instead wanted O'Brien to charge Vanecko.³³⁹ Yawger explained to the IGO in 2011 that he wanted O'Brien to charge Vanecko

³³⁵ See O'Brien, Darren, Special Grand Jury Tr. at 30:10-24 (May 8, 2013).

³³⁶ See O'Brien, Darren, Special Grand Jury Tr. at 31:8-13 (May 8, 2013); *see also* Yawger, Ronald, IGO Interview Tr. at 11:15-24 (July 1, 2011) (SAO was unaware of case prior to his call to O'Brien, and O'Brien seemed as if he was hearing information for first time.); *see also* Yawger, Ronald, IGO Interview Tr. at 9:18-10:9 (July 1, 2011) (Yawger stated that he called the main line for the Felony Review unit); O'Brien, Darren, Special Grand Jury Tr. at 30:20-24 (May 8, 2013) ("I'm not sure if I was paged by the caller directly or received a call through the Felony Review dispatcher. I've given my pager number to many police personnel throughout my career.")

³³⁷ See O'Brien, Darren, Special Grand Jury Tr. at 31:1-13 (May 8, 2013). *See also* O'Brien, Darren, Special Grand Jury Tr. at 14:9-12 (May 8, 2013) (stating "Vanecko's Daley family relationship had no impact in forming my opinion that charges were not appropriate in this case.")

³³⁸ See Yawger, Ronald, Special Grand Jury Tr. at 126:7-15, 128:12-15 (July 15, 2013). According to Yawger, and others, he reached out to O'Brien directly to review the case because the case involved the nephew of Mayor Daley. See Yawger, Ronald, IGO Interview Tr. at 7:17-22 (July 1, 2011); *see also* Epach, Thomas, Special Grand Jury Tr. at 13:12-15 (May 8, 2013) (testifying that Yawger told him he called O'Brien directly); *see also* O'Brien, Darren, Special Grand Jury Tr. at 31:10-13 (May 8, 2013) ("I believe the reference to a Daley relative is why I, as opposed to one of the felony review team, went out on a call."); *see* Rybicki, Richard, Special Grand Jury Tr. at 76:5-7 (Mar. 27, 2013). Chasen claims that he "demanded" that O'Brien, rather than another ASA, review the case because he wanted an immediate answer, and as the head of Felony Review, O'Brien could provide an answer immediately. See Chasen, Michael, IGO Interview Rep. at 5 (Nov. 27, 2012); *see also* Kobel, Richard, IGO Interview Rep. at 2 (Jan. 17, 2013). Chasen could not recall any other time he requested the head of Felony Review to personally review a case, and acknowledged that the Koschman case may have been the first time he made such a demand. See Chasen, Michael, IGO Interview Rep. at 5 (Nov. 27, 2012). According to Giralamo, O'Brien sometimes reviewed high profile or "heater" cases, and he only recalled seeing O'Brien at Area 3 four or five times. See Giralamo, Anthony, IGO Interview Rep. at 6 (Dec. 21, 2012).

³³⁹ See Yawger, Ronald, Special Grand Jury Tr. at 127:6-13 (July 15, 2013); Yawger, Ronald, IGO Interview Tr. at 7:22-23 (July 1, 2011).

and that a “Judge [could] throw [the case] out” if there was not sufficient evidence to support such a charge.³⁴⁰ Before the special grand jury in 2013, Yawger explained his thought process by stating:

I just wanted — it’s not a good thing to say, but I just wanted to kick the can down the road. I mean, why would we [CPD] make this decision? I wanted out of this case. I wanted to get it over with. I figured just charge the guy and go to preliminary hearing, and it would have been thrown out . . . And then we’re done with it, it’s on somebody else’s hands, which is not the right thing to do.³⁴¹

However, according to O’Brien’s 2013 special grand jury testimony, Yawger’s call was merely for an “advice,” and he was never asked by anyone to approve charges in the Koschman case.³⁴²

Tom Epach (a former Cook County ASA) was the Executive Assistant to Superintendent Cline in 2004 and acted as a liaison between CPD and SAO; on occasion advocating on behalf of detectives when CPD thought a case should be charged.³⁴³ In May 2013, Epach testified before the special grand jury and stated that sometime after the May 20, 2004 lineups, he received a call from Yawger requesting that he (Epach) reach out to SAO to attempt to obtain approval for

³⁴⁰ Yawger, Ronald, IGO Interview Tr. at 8:4-7 (July 1, 2011).

³⁴¹ See Yawger, Ronald, Special Grand Jury Tr. at 127:13-24 (July 15, 2013).

³⁴² See O’Brien, Darren, Special Grand Jury Tr. at 19:17-18, 23:21-24:6, 53:5-17 (May 8, 2013). O’Brien testified that “If Yawger had requested charges against anyone in this case, I would have rejected them . . . I thought CPD did not have enough evidence to pursue charges.” See O’Brien, Darren, Special Grand Jury Tr. at 53:12-16 (May 8, 2013). As evidence that charges were not requested, O’Brien pointed to the fact that he never wrote up the case as a rejection, that CPD reports show that charges were never requested, and that Superintendent Cline made a statement to the press that CPD felt charges were not appropriate. See O’Brien, Darren, Special Grand Jury Tr. at 152:5-20 (May 8, 2013); Special Grand Jury Exhibit 10 at CPD001117 (CPD001115-CPD001128) (Case Supplementary Report 3193543 (approved Nov. 10, 2004)); Fran Spielman, *No Charges in Fatal Fight Involving Daley’s Nephew* (May 26, 2004) (NEWS000009-10) (Superintendent Cline reported as stating on Tuesday, May 25, 2004 that there was “insufficient evidence” to bring charges in connection with Koschman’s death). Regardless of whether O’Brien was called to Area 3 for approval of charges or for an “advice,” SAO had the authority to charge the case. See Milan, Bob, Special Grand Jury Tr. at 59:5-8 (Apr. 24, 2013).

³⁴³ See Epach, Thomas, Special Grand Jury Tr. at 7:23-8:8 (May 8, 2013); Kobel, Richard, IGO Interview Rep. at 5 (Jan. 17, 2013); Molloy, James, Kroll Interview Rep. at 6 (Dec. 7, 2012); Chasen, Michael, IGO Interview Rep. at 7 (Nov. 27, 2012).

charges against Vanecko.³⁴⁴ According to Epach, when Yawger contacted him, Yawger stated he had already requested involuntary manslaughter charges against Vanecko on May 20, 2004.³⁴⁵ Epach testified that Yawger told him that O'Brien refused Yawger's request when he (Yawger) requested charges, and that O'Brien told Yawger that SAO did not charge involuntary manslaughter cases if SAO thought the case would ultimately be dismissed.³⁴⁶ Epach testified that he called O'Brien to convince him to bring charges against Vanecko; however, according to Epach, O'Brien could not be persuaded to do so.³⁴⁷ According to Epach, he "told O'Brien [over the phone] that I [Epach] thought self-defense could be viewed as unreasonable in this case."³⁴⁸ O'Brien told the special grand jury that he does not recall any such request from Epach,³⁴⁹ while Yawger told the special grand jury that, to the best of his recollection, he did ask Epach to help him get the case charged.³⁵⁰

b. O'Brien's Interviews of Witnesses

On May 20, 2004, at Area 3, after the lineups were complete, O'Brien interviewed Koschman's friends (Copeland, Allen, Francis, and Hageline) and Vanecko's friends (the McCarthys and Denham), but he did not interview Connolly or Kohler (the bystander witnesses).³⁵¹ It is unclear who was interviewed first, as Yawger has stated that the Koschman group was interviewed first,³⁵² but O'Brien testified that he interviewed Vanecko's friends

³⁴⁴ See Epach, Thomas, Special Grand Jury Tr. at 10:6-12, 11:15-18 (May 8, 2013).

³⁴⁵ See Epach, Thomas, Special Grand Jury Tr. at 11:3-7, 11:11-14, 26:19-27:4 (May 8, 2013).

³⁴⁶ See Epach, Thomas, Special Grand Jury Tr. at 26:19-27:7, 77:21-78:4 (May 8, 2013).

³⁴⁷ See Epach, Thomas, Special Grand Jury Tr. at 15:9-16:14 (May 8, 2013).

³⁴⁸ See Epach, Thomas, Special Grand Jury Tr. at 16:5-7 (May 8, 2013).

³⁴⁹ See O'Brien, Darren, Special Grand Jury Tr. at 54:21-24, 55:3-5, 134:7-10 (May 8, 2013).

³⁵⁰ See Yawger, Ronald, Special Grand Jury Tr. at 130:23-131:2; 132:11-18 (July 15, 2013).

³⁵¹ During one of three interviews with the OSP, O'Brien stated that he recalled the lineups were in progress when he arrived at Area 3 on May 20, 2004. O'Brien, Darren, IGO Interview Rep. (Proffer) at 9 (Feb. 20, 2013).

³⁵² See Yawger, Ronald, IGO Interview Tr. at 13:10-17 (July 1, 2011).

first.³⁵³ The witnesses were interviewed individually,³⁵⁴ except for the McCarthys, who were interviewed at the same time accompanied by their attorney, Bill Dwyer.³⁵⁵

Before the special grand jury in July 2013, Yawger stated that he took notes, which he described as “doodling” to simply “highlight[] some of the stuff” the witnesses were saying during O’Brien’s interviews of Koschman’s friends, but that he did not take notes during the interviews of the McCarthys or Denham.³⁵⁶ Yawger’s GPR for the Koschman friends’ interviews totaled less than a single page for all four interviews,³⁵⁷ and no GPRs exist from the interviews of the McCarthys or Denham, even though O’Brien testified before the special grand jury in 2013 that he thinks Yawger took notes during all the May 20, 2004 witness interviews.³⁵⁸

According to Yawger, O’Brien “really went after” the McCarthys in his interview and threatened to stop the interview and bring them before the grand jury because O’Brien did not believe the McCarthys’ statements that “they did not see” what happened when Koschman was struck.³⁵⁹ O’Brien similarly testified before the special grand jury in 2013 that he believed it was a reasonable inference that the McCarthys and Denham were lying during their interviews to protect Vanecko.³⁶⁰ At one point, according to Yawger, the McCarthys’ attorney (Dwyer) even

³⁵³ See O’Brien, Darren, Special Grand Jury Tr. at 36:18-21 (May 8, 2013).

³⁵⁴ See Yawger, Ronald, IGO Interview Tr. at 15:2-7 (July 1, 2011).

³⁵⁵ See Yawger, Ronald, IGO Interview Tr. at 17:23-18:6 (July 1, 2011).

³⁵⁶ See Yawger, Ronald, Special Grand Jury Tr. at 65:7-66:1, 67:14-68:2 (July 15, 2013). In 2013, O’Brien testified before the special grand jury and said he relied on the detective participating in the interviews to record a summary of each witness statement, *see* O’Brien, Darren, Special Grand Jury Tr. at 17:15-18:16 (May 8, 2013), whereas Yawger told the special grand jury that “Darren O’Brien would never ask any policeman to take his notes, I guarantee you that,” *see* Yawger, Ronald, Special Grand Jury Tr. at 66:15-21 (July 15, 2013).

³⁵⁷ According to Yawger’s GPR, Allen told O’Brien that Koschman was punched in the cheek, while Copeland told O’Brien that Koschman was punched in the mouth. *See* Special Grand Jury Exhibit 17 (CPD001051) (General Progress Report (May 20, 2004)).

³⁵⁸ See O’Brien, Darren, Special Grand Jury Tr. at 36:13-15 (May 8, 2013). O’Brien also testified that he personally did not take notes during any of the interviews in the Koschman matter. *See* O’Brien, Darren, Special Grand Jury Tr. at 35:18-19 (May 8, 2013).

³⁵⁹ See Yawger, Ronald, IGO Interview Tr. at 18:19-19:20 (July 1, 2011); *see* Yawger, Ronald, Special Grand Jury Tr. at 53:19-56:1 (July 15, 2013).

³⁶⁰ O’Brien, Darren, Special Grand Jury Tr. at 37:20-38:1, 104:6-24 (May 8, 2013).

threatened to complain to the attorney disciplinary authorities about O'Brien.³⁶¹ Likewise, according to then First Assistant State's Attorney Robert Milan's 2013 special grand jury testimony, the McCarthys' attorney also called him after the May 20, 2004 interviews to complain about O'Brien's questioning, stating that O'Brien was "harsh on them" and called them "liars."³⁶²

As noted above, O'Brien did not interview Connolly or Kohler. O'Brien testified that instead of interviewing these bystander witnesses, he "relied upon CPD reports and conversations with Detective Yawger as to what they said."³⁶³ O'Brien testified it was not necessary to interview Kohler and Connolly because their versions of the incident were generally consistent with that of Koschman's friends, except as to whether Vanecko punched or pushed Koschman.³⁶⁴

c. The Charging Decision

i. O'Brien's Standard for Approving Charges

Under Illinois law, a finding of probable cause (defined as sufficient evidence to justify the reasonable belief that the defendant has committed or is committing a crime) is needed to

³⁶¹ Yawger, Ronald, IGO Interview Tr. at 19:16-20 (July 1, 2011); *see also* O'Brien, Darren, Special Grand Jury Tr. at 38:2-7 (May 8, 2013) (stating that he "recall[s] their attorney interrupted the interview several times and was angry with me for the manner in which I aggressively interviewed his clients. He threatened to remove his clients from the interview room.")

³⁶² Milan, Bob, Special Grand Jury Tr. at 51:14-20 (Apr. 24, 2013). Milan also testified before the special grand jury that Dwyer stated he wanted to file an Attorney Registration and Disciplinary Commission complaint against O'Brien based on his conduct at the interviews. Milan, Bob, Special Grand Jury Tr. at 51:14-20 (Apr. 24, 2013).

³⁶³ O'Brien, Darren, Special Grand Jury Tr. at 46:13-17 (May 8, 2013).

³⁶⁴ O'Brien, Darren, Special Grand Jury Tr. at 46:22-47:3 (May 8, 2013). O'Brien testified that "I do not know the line of vision that the two independent witnesses had at the time of the incident, but my impression was both described the incident as if they had a clear view." O'Brien, Darren, Special Grand Jury Tr. at 46:17-21 (May 8, 2013). Both Kohler and Connolly testified before the special grand jury in 2012 that they only saw the aftermath of the physical contact between Vanecko and Koschman and not the contact itself. *See* Connolly, Michael, Special Grand Jury Tr. at 9:9-13 (July 11, 2012); Kohler, Phillip, Special Grand Jury Tr. at 13:15-21 (Aug. 8, 2012).

return an indictment.³⁶⁵ However, prosecutors have what is commonly referred to as “prosecutorial discretion,” which under Illinois law, provides that a prosecutor is allowed to independently determine whether to charge an individual with a criminal offense and which charge(s) to bring.³⁶⁶

In his 2013 special grand jury testimony, O’Brien described his personal standard for approving charges:

To approve charges in my mind, I would need to know with no doubt that a crime was committed, that the CPD identified the right person as the offender, and that there was some admissible evidence against that person and no negative evidence. There were some cases that was [sic] rejected because the negative evidence was so bad the case could not be salvaged by any new evidence. Negative evidence is evidence that show the offender was innocent of the offense or that contradicted evidence of guilt.³⁶⁷

According to former SAO Criminal Prosecutions Chief Bernie Murray, O’Brien “demanded more from police” for all cases coming into SAO where charges were sought.³⁶⁸ According to O’Brien, his overarching charging policy is that he does “not risk charging a person

³⁶⁵ See, e.g., *People v. Creque*, 382 N.E.2d 793, 796, 72 Ill. 2d 515, 523 (1978); *People v. Jones*, 830 N.E.2d 541, 551-552, 215 Ill. 2d 261, 273-75 (2005).

³⁶⁶ See, e.g., *Schiller v. Mitchell*, 828 N.E.2d 323, 335 (Ill. App. Ct. 2d Dist. 2005).

³⁶⁷ O’Brien, Darren, Special Grand Jury Tr. at 24:16-25:3 (May 8, 2013).

³⁶⁸ Murray, Bernard, IGO Interview Rep. at 5 (Feb. 22, 2013). According to Bernie Murray, if a case did not meet probable cause standards or the standard of having a strong probability of success at trial, then the Felony Review ASA would formally reject charges. See Murray, Bernard, IGO Interview Rep. at 3 (Feb. 22, 2013). However, according to Milan, an ASA could reject a case “for whatever reason” if the evidence was insufficient “to sustain the burden beyond a reasonable doubt.” See Milan, Bob, Special Grand Jury Tr. at 11:6-10 (Apr. 24, 2013). For all felonies except for homicides, CPD may override SAO’s rejection of charges. See Kobel, Richard, IGO Interview Rep. at 5 (Jan. 17, 2013). If a Felony Review ASA rejects charges and a CPD watch commander disagrees, the latter may call the on-duty CPD assistant deputy superintendent (“ADS”) for a consultation. Detective Division Standard Operating Procedures Sec. 8.8 “Obtaining Approval for Felony Charges” at IG_002503 (1988) (IG_002422-IG_002630); Chasen, Michael, IGO Interview Rep. at 9-10 (Nov. 27, 2012). If the ADS believes charges are appropriate, he, in turn, can inform the ASA that the felony charges are approved. Detective Division Standard Operating Procedures Sec. 8.8, “Obtaining Approval for Felony Charges” at IG002503 (1988) (IG_002422-IG_002630); Chasen, Michael, IGO Interview Rep. at 9-10 (Nov. 27, 2012). When this happens, the case will typically go to a preliminary hearing, where SAO often has it dismissed. Chasen, Michael, IGO Interview Rep. at 10 (Nov. 27, 2012).

unless [he is] certain – or as certain as [he] could be of [the offender’s] guilt.”³⁶⁹

ii. Issues Allegedly Preventing Charges

According to O’Brien’s 2013 special grand jury testimony, after he finished interviewing witnesses on the day of the lineups (May 20, 2004), he spoke with Yawger about the case and whether charges would be appropriate.³⁷⁰ O’Brien testified that after reviewing the available evidence, it was his belief that the case was “nowhere near chargeable,” and he told Yawger such.³⁷¹ O’Brien’s assessment that the case could not be charged (as noted above, O’Brien asserts he was never formally asked by CPD to charge the case) was based primarily on his issues concerning the: (1) lack of witness identification of the offender, and (2) viability of the offender’s putative affirmative defense of self-defense.³⁷²

(A) Supposed Lack of Witness Identification of the Offender

As discussed above, before the May 20, 2004, lineups were conducted, CPD believed Vanecko was the person who had struck Koschman. Furthermore, O’Brien testified before the special grand jury that the identification of an offender can be made by process of elimination.³⁷³ Although the McCarthys and Denham told O’Brien that they did not strike Koschman,³⁷⁴ O’Brien asserted in his special grand jury testimony that he “could not conclude” whether the person who struck Koschman was Kevin McCarthy, Denham, or Vanecko because he could not rely on Kevin McCarthy’s and Denham’s statements that they did not strike Koschman.³⁷⁵ Additionally, even though O’Brien knew that Koschman’s friends informed police the night of

³⁶⁹ O’Brien, Darren, Special Grand Jury Tr. at 24:13-15 (May 8, 2013).

³⁷⁰ O’Brien, Darren, Special Grand Jury Tr. at 48:3-19 (May 8, 2013).

³⁷¹ O’Brien, Darren, Special Grand Jury Tr. at 49:13-18 (May 8, 2013).

³⁷² O’Brien, Darren, Special Grand Jury Tr. at 48:16-19 (May 8, 2013).

³⁷³ O’Brien, Darren, Special Grand Jury Tr. at 52:6-10 (May 8, 2013). According to Bernie Murray, there is no need for a positive ID at a lineup before charging a circumstantial case. Murray, Bernard, IGO Interview Rep. at 4 (Feb. 22, 2013).

³⁷⁴ O’Brien, Darren, Special Grand Jury Tr. at 38:16-19 (May 8, 2013).

³⁷⁵ O’Brien, Darren, Special Grand Jury Tr. at 52:11-22 (May 8, 2013). No witnesses indicated Bridget McCarthy (the only woman in the group) struck Koschman.

the incident that Kevin McCarthy was not the offender, O'Brien testified that "those same friends impliedly said it was also not Vanecko when they failed to pick him out of a lineup."³⁷⁶ When O'Brien was reminded by the OSP that witnesses had stated that the person who struck Koschman was the "tallest" or "largest" in the group, and even though Vanecko was both the largest (at approximately 230 pounds) and the tallest (at approximately 6'3"),³⁷⁷ person in his group, O'Brien speculated that because the incident occurred in April, the Vanecko group was likely wearing jackets the night of the incident, "which could possibly distort someone's impression of size."³⁷⁸

(B) O'Brien's Evaluation of Self-Defense

Under Illinois law, self-defense is an affirmative defense that must be raised by the defendant, not the prosecution.³⁷⁹ In Illinois, the law of self-defense is as follows:

A person is justified in the use of force against another when and to the extent that he reasonably believes that such conduct is necessary to defend himself or another against such other's imminent use of unlawful force. However, he is justified in the use of force which is intended or likely to cause death or great bodily harm only if he reasonably believes that such force is necessary to prevent imminent death or great bodily harm to himself or another,

³⁷⁶ O'Brien, Darren, Special Grand Jury Tr. at 52:23-53:4 (May 8, 2013).

³⁷⁷ Of note, Denham was 5'10" and 170 pounds, and Kevin McCarthy was 6'2" and 190 pounds. See Special Grand Jury Exhibit 40 (Denham Driver License Search Results) and Special Grand Jury Exhibit 39 (Kevin McCarthy Driver License Search Results).

³⁷⁸ O'Brien, Darren, Special Grand Jury Tr. at 50:22-51:3 (May 8, 2013). No witnesses have told police or testified before the special grand jury that the Vanecko group was wearing jackets, nor that jackets distorted their ability to perceive the height or weight of the persons involved in the altercation.

³⁷⁹ See *People v. Zapata*, 808 N.E.2d 1064, 1069-70 (Ill. App. Ct. 1st Dist. 2004); *People v. Moore*, 797 N.E.2d 217, 225 (Ill. App. Ct. 2d Dist. 2003). However, according to Kirk, Felony Review ASAs are trained to anticipate possible defenses, such as self-defense. Kirk, Daniel, IGO Interview Rep. at 5 (Mar. 26, 2013). The accused has the burden of producing evidence to raise the question of self-defense unless that issue arises from the state's proof. *People v. Haynes*, 260 N.E.2d 377, 379 (Ill. App. Ct. 1st Dist. 1970). Once a defendant raises the issue of self-defense, the state has the burden of proving beyond a reasonable doubt that the defendant did not act in self-defense, in addition to proving the elements of the charged offense. *People v. Zapata*, 808 N.E.2d 1064, 1069 (Ill. App. Ct. 1st Dist. 2004). If the state negates any one of the elements of self-defense, the defendant's claim of self-defense must fail. *People v. Young*, 807 N.E.2d 1125, 1134 (Ill. App. Ct. 1st Dist. 2004).

or the commission of a forcible felony.³⁸⁰

According to O'Brien's 2013 special grand jury testimony, he believes the law requires him "To . . . look at all the evidence, not just what a prospective offender might say. If any witness or possible offender provides evidence that a person was acting in self-defense and I conclude that that is true, I then consider whether the response to that threat was reasonable. If it is, then no crime has been committed and I obviously cannot charge anyone with an offense."³⁸¹

O'Brien also testified that "whoever pushed or punched Koschman did so because they were acting in response to Koschman's aggression."³⁸² In fact, according to O'Brien, regardless of whether Koschman was punched or pushed, either use of force would have been reasonable, in his opinion.³⁸³ However, O'Brien admitted under oath that none of the witnesses told him that Koschman threw punches or made physical contact with Vanecko immediately before Koschman was struck.³⁸⁴ In fact, O'Brien also testified that he did not remember the McCarthys or Denham ever telling CPD or him that during the altercation they or Vanecko felt threatened in a physical way or that as they walked away, "there was any danger to them" (i.e., they did not think that great bodily harm to themselves or others was imminent).³⁸⁵ According to O'Brien, when a person "[f]lees from the scene [as Vanecko did], such evidence may be an indicator of consciousness of guilt, but it could also mean the person did not want to be involved in law

³⁸⁰ 720 ILCS 5/7-1 (West 2004).

³⁸¹ O'Brien, Darren, Special Grand Jury Tr. at 26:7-17 (May 8, 2013). According to Hehner, SAO does approve charges for cases even if it is believed that a defendant is likely to raise self-defense at trial. Special Grand Jury Exhibit 151 at 11 (Hehner, Walt, IGO Interview Rep. (Mar. 11, 2013)). According to 2011 Area 5 CPD Commander Salemme, self-defense is one of the "favorite reasons" given by SAO for rejecting charges in a case. Special Grand Jury Exhibit 109 at 8 (Salemme, Joseph, Kroll Interview Rep. (Jan. 15, 2013)).

³⁸² O'Brien, Darren, Special Grand Jury Tr. at 26:18-27:4 (May 8, 2013) (concluding that Koschman's friends would not lie about Koschman being the aggressor); *see also* O'Brien, Darren, Special Grand Jury Tr. at 27:10-21 (May 8, 2013).

³⁸³ O'Brien, Darren, Special Grand Jury Tr. at 28:5-13 (May 8, 2013).

³⁸⁴ O'Brien, Darren, Special Grand Jury Tr. at 40:6-9 (May 8, 2013).

³⁸⁵ O'Brien, Darren, Special Grand Jury Tr. at 130:9-17 (May 8, 2013).

enforcement activity.”³⁸⁶ However, according to O’Brien, fleeing the scene could also “indicate the person fleeing may be fearful of being attacked again.”³⁸⁷

Additionally, even though O’Brien and CPD did not speak to Vanecko, according to O’Brien, he was nevertheless able to divine Vanecko’s actual state of mind based on not only what the witnesses told him, but also upon his “common sense as to what the average person’s state of mind would have been” under the circumstances.³⁸⁸ O’Brien explained to the special grand jury that the Koschman and Vanecko groups had “been yelling back and forth,”³⁸⁹ and thus, when Koschman continued the argument:

What options did the Vanecko group have? Run? They never would have been able to turn and run before Koschman was on them. Stand there and let Koschman strike them first? Not only would that be absurd, the law does not require such action. I believe it [striking Koschman] was more likely a reaction by someone in the Vanecko group throwing up his hands to prevent Koschman from getting to them rather than a punch. Vanecko’s group had been drinking, too, and I doubt any among them would have had the time to actually make a decision to throw a punch; however, I don’t know exactly what type of contact occurred.³⁹⁰

O’Brien summed up his stance on the issue of self-defense in this matter by stating:

I concluded that if it was Vanecko who punched or pushed Koschman, it was reasonable to believe that Vanecko felt either he or another in his group were being physically threatened by Koschman and acted accordingly. I believe Koschman was physically threatening, and concluded Koschman’s aggression led to him being pushed or punched.³⁹¹

³⁸⁶ O’Brien, Darren, Special Grand Jury Tr. at 29:13-17 (May 8, 2013).

³⁸⁷ O’Brien, Darren, Special Grand Jury Tr. at 29:18-19 (May 8, 2013).

³⁸⁸ O’Brien, Darren, Special Grand Jury Tr. at 40:21-41:9 (May 8, 2013).

³⁸⁹ O’Brien, Darren, Special Grand Jury Tr. at 45:18-19 (May 8, 2013).

³⁹⁰ O’Brien, Darren, Special Grand Jury Tr. at 45:22-46:12 (May 8, 2013).

³⁹¹ O’Brien, Darren, Special Grand Jury Tr. at 40:11-20 (May 8, 2013). *See also* O’Brien, Darren, Special Grand Jury Tr. at 48:16-49:-6 (May 8, 2013) (stating the Koschman case “was not a close call” when describing the reasons he felt charges in this matter were precluded). As part of his testimony

Additionally, O'Brien testified that he was unaware of the fact that the Vanecko group rendezvoused at the Pepper Canister after the incident on April 25, 2004 (an event that was uncovered by the OSP and revealed to him during an interview with the OSP).³⁹² In hindsight, according to O'Brien, after learning of the Pepper Canister meeting, he wishes he had asked the McCarthys and Denham why they met up and what they discussed.³⁹³ That is because, according to O'Brien, “[w]hen the parties to a violent act rendezvous after the act, the purpose of the meeting could be an important consideration if the purpose was to develop a consistent fictitious story about the incident.”³⁹⁴

O'Brien testified that when he left Area 3 after the May 20, 2004 lineups, he probably reported the results of his visit up SAO's chain of command, likely to Bernie Murray and Milan, but O'Brien stressed he “did not ask them what [he] should do [with the case].”³⁹⁵ O'Brien explained further that while he does not specifically remember speaking about the Koschman case with his superiors, he is “sure they all agreed that this case was not chargeable.”³⁹⁶ Milan recalled hearing the results of O'Brien's Felony Review visit, and testified that while he cannot remember how many times he spoke with State's Attorney Richard Devine about the Koschman case in 2004, he “would bet the ranch” that he discussed the matter, including O'Brien's

before the special grand jury, O'Brien read a statement which, in part, stated, “I also considered any disparity in size between Koschman and any of the larger males in Vanecko's group as well as the fact that Vanecko left the scene after the incident. Both are considerations in any self-defense evaluation, though they are not necessarily dispositive.” *See O'Brien, Darren, Special Grand Jury Tr. at 47:8-15 (May 8, 2013).* Regarding his consideration of the size disparity between Vanecko and Koschman, O'Brien testified that, “what would the alternative be for Vanecko or somebody to sit there and say he's going to hit me. He's smaller than me. I probably should let them strike first. I don't think the law requires that.” *See O'Brien, Darren, Special Grand Jury Tr. at 169:21-170:2 (May 8, 2013).*

³⁹² O'Brien, Darren, Special Grand Jury Tr. at 56:6-9 (May 8, 2013).

³⁹³ O'Brien, Darren, Special Grand Jury Tr. at 56:11-15 (May 8, 2013).

³⁹⁴ O'Brien, Darren, Special Grand Jury Tr. at 29:20-30:1 (May 8, 2013).

³⁹⁵ O'Brien, Darren, Special Grand Jury Tr. at 54:6-11 (May 8, 2013). During Milan's special grand jury testimony, he described O'Brien as “one of the finest men” and “one of the finest lawyers” he knows. *See Milan, Bob, Special Grand Jury Tr. at 51:22-24 (Apr. 24, 2013).*

³⁹⁶ O'Brien, Darren, Special Grand Jury Tr. at 151:3-14 (May 8, 2013).

findings, with State's Attorney Devine once or maybe twice during that period.³⁹⁷

Furthermore, current State's Attorney Anita Alvarez told the OSP she never discussed the Koschman case with O'Brien or State's Attorney Devine in 2004, despite her being in the supervisory chain of command, and State's Attorney Alvarez speculated that she was likely bypassed because she was not part of SAO's "good old boy network."³⁹⁸ According to State's Attorney Alvarez, if she had been in charge of SAO in 2004, she not only would have wanted to have been made aware of the Koschman matter, but she would have wanted to have discussed it with O'Brien and CPD personnel, as well as had an opportunity to personally review the files – something she believes should have probably occurred at SAO in 2004.³⁹⁹

According to the current First Assistant State's Attorney Shauna Boliker, she was surprised SAO did not conduct a more extensive review of the Koschman case in 2004.⁴⁰⁰ Boliker would have expected SAO "higher ups" to have been heavily involved with reviewing the case, due to the fact that SAO knew its actions were going to be scrutinized because of the Mayor's nephew's (Vanecko's) involvement in the matter.⁴⁰¹

³⁹⁷ Milan, Bob, Special Grand Jury Tr. at 40:2-13, 60:17-23 (Apr. 24, 2013). However, Milan also testified that his knowledge of the Koschman case was derived from what O'Brien told him, and that he (Milan) did not have independent knowledge of the facts, and did not interview witnesses or review CPD reports. *See* Milan, Bob, Special Grand Jury Tr. at 40:22-41:5, 43:5-10, 54:7-10, 118:3-5 (Apr. 24, 2013). Once the *Sun-Times* began covering the Koschman story in 2011, Milan testified that he recalls discussing the case with State's Attorney Devine (and O'Brien) approximately "a half a dozen" times since 2011. Milan, Bob, Special Grand Jury Tr. at 38:7-19, 84:7-85:7 (Apr. 24, 2013). State's Attorney Devine's best recollection was that he was informed of SAO's involvement in the Koschman case by Milan, after O'Brien had become involved in the matter. *Compare* Devine, Richard, IGO Interview Rep. at 2 (Dec. 20, 2011) (informed by Milan or Bernie Murray) *with* Devine, Richard, IGO Interview Rep. at 3 (Apr. 9, 2013) (does not think that Bernie Murray notified him of the Koschman matter). Milan also likely told him of O'Brien's findings. Devine, Richard, IGO Interview Rep. at 3 (Apr. 9, 2013). State's Attorney Devine could not recall reviewing any written materials relating to the matter. *See* Devine, Richard, IGO Interview Rep. at 2 (Dec. 20, 2011); Devine, Richard, IGO Interview Rep. at 3 (Aug. 8, 2013). State's Attorney Devine never issued instructions to Felony Review in connection with the matter; nor did he recall any formal meetings with top supervisors relating to the Koschman case. *See* Devine, Richard, IGO Interview Rep. at 2 (Dec. 20, 2011).

³⁹⁸ Alvarez, Anita, IGO Interview Rep. at 1 (Apr. 29, 2013).

³⁹⁹ Alvarez, Anita, IGO Interview Rep. at 9 (Apr. 29, 2013).

⁴⁰⁰ Boliker, Shauna, IGO Interview Rep. at 7 (Mar. 25, 2013).

⁴⁰¹ Boliker, Shauna, IGO Interview Rep. at 7 (Mar. 25, 2013).

d. Felony Review Folder

As part of the Felony Review process, the reviewing ASA is required to create what is referred to as a Felony Review folder.⁴⁰² ASAs use the folders to record certain key case information learned from their review of the evidence, as well as from their interviews of witnesses or the offender himself.⁴⁰³ In 2004, besides retaining the hard copy Felony Review folder, Felony Review cases were also logged into the SAO’s “Prosecutor’s Management Information System” (PROMIS).⁴⁰⁴

In this case, neither O’Brien’s Felony Review folder (or folders) from his May 20, 2004 interviews, nor the matter’s related electronic records, exist.⁴⁰⁵ Specifically, O’Brien testified

⁴⁰² Furthermore, according to Kirk, Felony Review ASAs were required to turn in a Felony Review folder for every case they reviewed. *See Kirk, Daniel, IGO Interview Rep. at 2 (Mar. 26, 2013).* Indeed, according to Hehner, Felony Review folders for “advice” cases were to be kept in the event CPD called SAO for charges at a later date. Special Grand Jury Exhibit 151 at 3 (Hehner, Walt IGO Interview Rep. (Mar. 11, 2013)); *see also* Boliker, Shauna, IGO Interview Rep. at 6-7 (Mar. 25, 2013); Alvarez, Anita, IGO Interview Rep. at 5 (Apr. 29, 2013). The ASA used the folder to record details of the case: the nature of the ASA’s review, including whether the review was a rejection of charges, approval of charges, a continuing investigation, or an “advice.” *See Special Grand Jury Exhibit 151 at 2-4 (Hehner, Walt, IGO Interview Rep. (Mar. 11, 2013)); O’Brien, Darren, Special Grand Jury Tr. at 20:15-21:9 (May 8, 2013); Kirk, Daniel, IGO Interview Rep. at 2 (Mar. 26, 2013); Milan, Bob, Special Grand Jury Tr. at 12:20-14:4 (Apr. 24, 2013).* The purpose of the Felony Review folder is to provide ASAs with a guide for the preliminary hearings as the case continues toward trial. *Kirk, Daniel, IGO Interview Rep. at 2 (Mar. 26, 2013).*

⁴⁰³ The Felony Review folder is approximately the size of a legal pad with carbon copy sheets that were colored white and yellow. *See O’Brien, Darren, Special Grand Jury Tr. at 20:15-23 (May 8, 2013); Milan, Bob, Special Grand Jury Tr. at 14:9-21 (Apr. 24, 2013); O’Brien, Darren, IGO Interview Rep. (Proffer) at 3 (Feb. 5, 2013); Special Grand Jury Exhibit 151 at 2 (Hehner, Walt, IGO Interview Rep. (Mar. 11, 2013)).* The ASA would write on the white sheet and the writing would imprint on the yellow sheet behind it as well as the outer folder. *Milan, Bob, Special Grand Jury Tr. at 14:9-21 (Apr. 24, 2013).* Therefore, the information recorded in the Felony Review folder would appear on three physical papers: (1) the white sheet, where the information was originally written; (2) the yellow sheet, where the information was imprinted from the white sheet; and (3) the outer folder, where the information was imprinted from the white sheet. *See Milan, Bob, Special Grand Jury Tr. at 14:9-21 (Apr. 24, 2013).*

⁴⁰⁴ Special Grand Jury Exhibit 151 at 3-4 (Hehner, Walt, IGO Interview Rep. (Mar. 11, 2013)).

⁴⁰⁵ O’Brien, Darren, Special Grand Jury Tr. at 57:24-59:4 (May 8, 2013). Several witnesses have stated that it is extremely uncommon for Felony Review folders to get lost. *See, e.g., Gilger, James, Special Grand Jury Tr. at 110:16-111:12 (Jan. 16, 2013)* (It is “very uncommon” for a Felony Review file to be lost, and in the hundreds of felony cases he had investigated, no other Felony Review file had ever been lost); Spanos, Nicholas, Special Grand Jury Tr. at 61:13-19 (Feb. 6, 2013) (Spanos agreed that it was

before the special grand jury in 2013 that he is sure he brought a Felony Review folder or folders⁴⁰⁶ with him to Area 3 on May 20, 2004.⁴⁰⁷ O'Brien further testified that after he completed the May 20, 2004 witness interviews, he likely brought the Felony Review folder back to his office to await further contact from CPD regarding any new developments in the case.⁴⁰⁸ According to O'Brien's special grand jury testimony, he likely kept the Koschman folder in his office desk drawer for some time, but "[w]hen nothing more happened in the case, [he] threw the folder away."⁴⁰⁹

Even if O'Brien destroyed the hard copy Felony Review folder, PROMIS should have retained an electronic record of the matter (even if O'Brien was only called for an "advice").⁴¹⁰ In fact, Milan confirmed that "advices" "should have been input[ted]" into the PROMIS

unusual for a Felony Review file to be missing and confirmed that he has never had any other case in which the Felony Review file was missing).

⁴⁰⁶ O'Brien, Darren, Special Grand Jury Tr. at 33:3-8 (May 8, 2013) (stating that due to the number of witnesses he interviewed for the Koschman matter on May 20, 2004, it was possible he used four or five Felony Review folders because each folder only had room for biographical information for two witnesses).

⁴⁰⁷ O'Brien, Darren, Special Grand Jury Tr. at 32:14-21 (May 8, 2013). However, O'Brien previously informed certain SAO staff that he did not recall creating a Felony Review folder for the Koschman matter. For example, according to Boliker, O'Brien informed her (and other SAO staff) that he did not recall whether he created a Felony Review folder when he went to Area 3 on May 20, 2004. *See* Boliker, Shauna, IGO Interview Rep. at 6 (Mar. 25, 2013); *see also* Kirk, Daniel, IGO Interview Rep. at 4 (Mar. 26, 2013). State's Attorney Alvarez told the OSP that SAO still does not know for certain whether the Felony Review file for the Koschman matter ever existed. Alvarez, Anita, IGO Interview Rep. at 5 (Apr. 29, 2013).

⁴⁰⁸ O'Brien, Darren, Special Grand Jury Tr. at 32:22-33:2 (May 8, 2013).

⁴⁰⁹ O'Brien, Darren, Special Grand Jury Tr. at 58:23-59:4 (May 8, 2013). O'Brien could not provide a concrete time period in which he threw away the Koschman Felony Review folder. He has said he "probably" kept the Koschman Felony Review folder for "a couple of years" before throwing it away. O'Brien, Darren, Special Grand Jury Tr. at 86:5-11 (May 8, 2013). However, he has also said that he may have thrown away the Felony Review folder when he cleaned out his desk at the time he left the position as head of Felony Review in 2008. O'Brien, Darren, Special Grand Jury Tr. at 14:21-22, 90:16-19 (May 8, 2013).

⁴¹⁰ Special Grand Jury Exhibit 151 at 3 (Hehner, Walt, IGO Interview Rep. (Mar. 11, 2013)); Boliker, Shauna, IGO Interview Rep. at 2 (Mar. 25, 2013); Milan, Bob, Special Grand Jury Tr. at 21:20-22:4 (Apr. 24, 2013); Kirk, Daniel, IGO Interview Rep. at 2 (Mar. 26, 2013).

database.⁴¹¹ Indeed, during his special grand jury testimony, O'Brien confirmed that while he was Chief of the Felony Review unit, he made substantial efforts to ensure that the data entry employees entered advice calls in SAO's computer system.⁴¹² However, no electronic Felony Review records for the Koschman case have ever been discovered.

Additionally, in or around February 2011, and in response to a *Chicago Sun-Times* ("Sun-Times") Freedom of Information Act ("FOIA")⁴¹³ request received by SAO in January 2011, O'Brien was instructed by either John Brassil (SAO's Chief of the Felony Review unit) or Fabio Valentini (SAO's Chief of the Criminal Prosecutions Bureau) to search for his May 20, 2004 Koschman Felony Review folder(s).⁴¹⁴ Several other SAO employees were instructed to undertake similar efforts.⁴¹⁵ Furthermore, on March 22, 2013, at the OSP's direction, and in an effort to locate an electronic version of the Koschman Felony Review folder, an investigator from Kroll met with representatives from SAO to search O'Brien's shared drive from SAO back-up tapes. The searches performed by Kroll did not yield any files related to the Koschman felony review.⁴¹⁶ Despite these efforts, and as noted above, the Koschman Felony Review folder (both hard copy and electronic versions) has never been located, and thus was unavailable for the

⁴¹¹ Milan, Bob, Special Grand Jury Tr. at 25:23-26:8 (Apr. 24, 2013). Hehner also confirmed that advices should have been recorded on SAO's computer system. Special Grand Jury Exhibit 151 at 4 (Hehner, Walt, IGO Interview Rep. (Mar. 11, 2013)).

⁴¹² O'Brien, Darren, Special Grand Jury Tr. at 22:19-23:2 (May 8, 2013).

⁴¹³ The purpose of the Illinois Freedom of Information Act is to serve the "public policy of the State of Illinois that access by all persons to public records promotes the transparency and accountability of public bodies at all levels of government." 5 ILCS 140/1 (West 2011).

⁴¹⁴ O'Brien, Darren, Special Grand Jury Tr. at 58:15-22 (May 8, 2013); Special Grand Jury Exhibit 151 at 7 (Hehner, Walt, IGO Interview Rep. (Mar. 11, 2013)); Alvarez, Anita, IGO Interview Rep. at 5 (Apr. 29, 2013); Kirk, Daniel, IGO Interview Rep. at 4 (Mar. 26, 2013).

⁴¹⁵ Boliker, Shauna, IGO Interview Rep. at 6 (Mar. 25, 2013); Special Grand Jury Exhibit 151 at 5 (Hehner, Walt, IGO Interview Rep. (Mar. 11, 2013)).

⁴¹⁶ The OSP also attempted to retrieve e-mails from SAO personnel from 2004. Due to the passage of time and a migration to a different e-mail system in 2010, those e-mails no longer exist. See Cook County Bureau of Technology, Chief Information Officer Lydia Murray correspondence (Jan. 4, 2013) (CCSAO_033293). While e-mails were backed up to tape and stored off-site for a period of one year; SAO's backup tapes prior to 2008 were routinely overwritten. See Lydia Murray correspondence (Jan. 4, 2013) (CCSAO_033293). Additionally, although Cook County Bureau of Technology officials located a number of e-mail backup tapes, none pre-dated 2008. See Murray, Lydia, IGO Interview Rep. at 1-2 (Feb. 27, 2013).

OSP to review and consider during its investigation.⁴¹⁷

5. Press Inquiries

Following the 2004 decision by CPD and SAO not to charge Vanecko, the media began to report Vanecko's connection to the incident. On May 22, both the *Chicago Tribune* and the *Sun-Times* published articles reporting that the Mayor's nephew had been questioned in connection with the death of David Koschman.⁴¹⁸ John Gorman, Press Secretary for SAO in 2004, is quoted in the *Chicago Tribune* article as stating, "We were consulted about this by the police and agreed that no charges would be placed against any individual in this case at this time. There were four guys, and Vanecko was one of them."⁴¹⁹ According to Gorman, he likely got this information directly from someone in the Felony Review unit — possibly O'Brien.⁴²⁰

On May 22, 2004, Hal Dardick of the *Chicago Tribune* submitted a FOIA request seeking "all police reports relating to the April 24 [sic] incident that led to the death of David Koschman. . . ."⁴²¹ CPD denied the request on several grounds, including that disclosure would have "interfere[d] with pending or actually and reasonably contemplated law enforcement proceedings. . . ."⁴²² One consequence of an open investigation is that it provides a grounds for

⁴¹⁷ Special Grand Jury Exhibit 151 at 4 (Hehner, Walt, IGO Interview Rep. (Mar. 11, 2013)); Alvarez, Anita, IGO Interview Rep. at 5 (Apr. 29, 2013). Furthermore, and in response to the OSP's request, SAO searched again in 2013, but the result was the same – no relevant Koschman files or paperwork were found. See Valentini letter (Apr. 11, 2013) (CCSAO_033623-CCSAO_033624).

⁴¹⁸ See Jeff Coen and Carlos Sadovi, *Daley Nephew at Fatal Fight Scene*, (May 22, 2004) (CCSAO_008311-CCSAO_008312); Frank Main and Fran Spielman, *Mayor's Nephew Quizzed in Fatal Fight*, (May 22, 2004) (CCSAO_008316-CCSAO_008317).

⁴¹⁹ See Jeff Coen and Carlos Sadovi, *Daley Nephew at Fatal Fight Scene*, at CCSAO_008311, (May 22, 2004) (CCSAO_008311-CCSAO_008312).

⁴²⁰ See Gorman, John, IGO Interview Rep. at 3 (Jan. 25, 2013).

⁴²¹ See CPD FOIA Requests 2004-Present at CCSAO_002646 (CCSAO_002644-CCSAO_002666); Sandoval, Matthew, Kroll Interview Rep. (Proffer) at 5 (Jan. 11, 2013). The request was stamped "received" by CPD on May 25, 2004.

⁴²² See CPD FOIA Requests 2004-Present at CCSAO_002646 (CCSAO_002644-CCSAO_002666); 5 ILCS 140/7(c)(i) (West 2004). CPD FOIA Unit Officer Matthew Sandoval stated that he pulled reports for Dardick, but those reports may have never been picked up. See Sandoval, Matthew, Kroll Interview Rep. (Proffer) at 5 (Jan. 11, 2013).

denial of a FOIA request.⁴²³

On May 26, 2004, *Sun-Times* reporter Fran Spielman published an article, “*No Charges in Fatal Fight Involving Daley’s Nephew. Did Clout Play Role? ‘Of Course Not,’ Police Chief Says.*”⁴²⁴ The article quotes then Superintendent Cline as making several remarks about the Koschman investigation, which remained open at the time. The article quotes Superintendent Cline as saying, “The state’s attorney’s office and the Police Department both agree at this time, there’s no basis for criminal charges based on the witness statements and all of the evidence we have,” and that a charge of involuntary manslaughter “doesn’t fit, based on everything we’ve looked at so far. . . . If new evidence came up, we could change. But, based on all of the evidence we have now — all the witnesses brought in and lineups conducted — there’s no basis for criminal charges.”⁴²⁵ Following the report of Superintendent Cline’s statement, it appears the

⁴²³ See 5 ILCS 140/7(c)(i) and (viii) (West 2004).

⁴²⁴ See Spielman, *No Charges in Fatal Fight Involving Daley’s Nephew. Did Clout Play Role? ‘Of Course Not,’ Police Chief Says* (May 26, 2004) (NEWS000009-NEWS000010).

⁴²⁵ See Spielman, *No Charges in Fatal Fight Involving Daley’s Nephew. Did Clout Play Role? ‘Of Course Not,’ Police Chief Says* at NEWS000009 (May 26, 2004) (NEWS000009-NEWS000010). On February 28, 2011, the *Sun-Times* published an article entitled, “*Questions in Death Involving Daley Nephew,*” which quoted former Superintendent Cline as stating, “At the best, it was mutual combatants... If the other person is the aggressor, then Vanecko has the right to defend himself.” (NEWS000021). When interviewed by the OSP, former Superintendent Cline again used the phrase “mutual combatants” to describe the incident on April 25, 2004. Cline, Phillip, IGO Interview Rep. at 7 (Jan. 2, 2013); O’Brien, Darren, Special Grand Jury Tr. at 28:14-16 (May 8, 2013). In Illinois, the concept of “mutual combat” can sometimes arise when a defendant charged with first-degree murder seeks a jury instruction on the lesser included offense of second-degree murder. See *People v. Young*, 618 N.E.2d 1026, 1037, 248 Ill. App. 3d 491, 505 (Ill. App. Ct. 1st Dist. 1993). The Illinois Supreme Court defines “mutual combat” as “a fight or struggle which both parties enter willingly or where two persons, upon a sudden quarrel and in hot blood, mutually fight upon equal terms and where death results from the combat.” *People v. Austin*, 549 N.E.2d 331, 334, 133 Ill.2d 118, 125 (1989). When determining whether evidence of mutual combat exists, “the provocation must be proportionate to the manner in which the accused retaliated,” *id.* at 335, and mere words generally are not sufficient to show provocation. *People v. Brown*, 584 N.E.2d 355, 367, 222 Ill. App. 3d 703, 720 (Ill. App. Ct. 1st Dist. 1991).

Allen testified before the special grand jury in 2012, that “there was never a point when Koschman was squaring off to fight anyone.” See Allen, Scott, Special Grand Jury Tr. at 11:3-5 (Aug. 8, 2012); see also Francis, David, Special Grand Jury Tr. at 14:4-8 (Aug. 8, 2012) (“Koschman never raised his fists or appeared to be squaring off to fight anyone. I never thought anyone would start throwing fists.”) Allen also testified that Koschman was unprepared to defend himself and Koschman was “[a]bsolutely defenseless.” See Allen, Scott, Special Grand Jury Tr. at 38:23-39:4 (Aug. 8, 2012). Connolly additionally testified before the special grand jury that, “I wouldn’t characterize [Koschman] as

media did not publish another article regarding the Koschman case until 2011.

6. Det. Yawger Meets with Nanci Koschman and Her Lawyer

On or around July 12, 2004, Nanci Koschman (David Koschman's mother), accompanied by her attorney, Loretto Kennedy, met with Yawger at Area 3 headquarters.⁴²⁶ According to what Kennedy told the OSP in 2013, Ms. Koschman arranged the meeting in order to learn more about what occurred the night her son was struck (Apr. 25, 2004).⁴²⁷ During the meeting Yawger told Ms. Koschman that witnesses had told CPD that her son, David, was the aggressor in the incident.⁴²⁸ Kennedy recalled this news making Ms. Koschman very upset.⁴²⁹

In his 2011 interview with the IGO, Yawger recalled this 2004 meeting with Ms. Koschman (and her attorney).⁴³⁰ According to Yawger, during the meeting he explained to Ms. Koschman and her attorney that CPD knew who the offender was, but that CPD could not "get him charged."⁴³¹ Furthermore, Yawger recalled that he could not provide Ms. Koschman or her lawyer the name of the offender (Vanecko), because the offender had not been charged or

being physically aggressive. Would not characterize him as physically aggressive. He didn't have his fists raised and didn't appear to be squaring off to fight anyone. Koschman was not attempting to strike anyone." See Connolly, Michael, Special Grand Jury Tr. at 8:12-22 (July 11, 2012). Kohler similarly testified, "I don't recall Koschman clenching fists or actually touching anyone in the other group." See Kohler, Phillip, Special Grand Jury Tr. at 8:20-9:2 (July 11, 2012). Additionally, as noted above, O'Brien testified before the special grand jury that none of the witnesses told him that Koschman "threw punches or made physical contact with Vanecko immediately before Koschman was struck." O'Brien, Darren, Special Grand Jury Tr. at 40:6-9 (May 8, 2013).

⁴²⁶ Kennedy, Loretto, IGO Interview Rep. at 1 (Jan. 2, 2013); Kennedy, Loretto, IGO Interview Rep. at 1 (Jan. 18, 2013). Kennedy told the OSP that Nanci Koschman's brother-in-law, Richard Pazderski, also attended the meeting with Yawger. Kennedy, Loretto, IGO Interview Rep. at 1 (Jan. 2, 2013). See also Yawger, Ronald, Special Grand Jury Tr. at 77:2-11 (July 15, 2013).

⁴²⁷ Kennedy, Lorreto, IGO Interview Rep. at 1 (Jan. 2, 2013). Kennedy told the OSP the meeting lasted no more than 30 minutes. Kennedy, Loretto, IGO Interview Rep. at 1 (Jan. 2, 2013).

⁴²⁸ Kennedy, Loretto, IGO Interview Rep. at 2-3 (Jan. 2, 2013).

⁴²⁹ Kennedy, Loretto, IGO Interview Rep. at 2 (Jan. 2, 2013).

⁴³⁰ Yawger, Ronald, IGO Interview Tr. at 35:13-14 (July 1, 2011).

⁴³¹ Yawger, Ronald, IGO Interview Tr. at 35:22-24 (July 1, 2011).

identified by witnesses.⁴³² However, Yawger told the IGO in 2011 that he did inform Ms. Koschman and her attorney that the offender was a “pretty prominent figure” and “not a regular guy walking down the street.”⁴³³

7. Det. Yawger Submits His Reports

Despite concluding his investigation on May 20, 2004, Yawger did not submit his case supp reports documenting the lineups until November 8, 2004, and his case supp report documenting the investigation’s conclusions until November 10, 2004.⁴³⁴ Detectives and police personnel nearly universally commented that a six-month delay in submission of reports is “a long time” and “unusual.”⁴³⁵ During his interview with the OSP in 2012, former Superintendent Cline stated it was odd the report was not written until six months later in November 2004.⁴³⁶ During his interview with IGO investigators in 2011, Yawger could not explain the delay in submitting his reports, stating, “No, I have no idea. Because those reports had been, were done that night [May 20, 2004], they had to be done, they had to be done and in.”⁴³⁷ In addition, Rita O’Leary’s case supp report documenting her interviews of Connolly and Kevin McCarthy on April 25, 2004, was submitted on May 20, 2004, but not approved until November 10, 2004.⁴³⁸ Detectives similarly opined that such a delay between submission of a report and approval was

⁴³² Yawger, Ronald, IGO Interview Tr. at 37:13-23 (July 1, 2011); *see also* Kennedy, Loretto, IGO Interview Rep. at 2 (Jan. 2, 2013); Kennedy, Loretto, IGO Interview Rep. at 1 (Jan. 18, 2013).

⁴³³ Yawger, Ronald, IGO Interview Tr. at 37:15-18 (July 1, 2011); Kennedy, Loretto, IGO Interview Rep. at 2-3 (Jan. 2, 2013).

⁴³⁴ See Special Grand Jury Exhibit 13 (CPD001111-CPD001114) (Case Supplementary Report 3222388 (approved Nov. 10, 2004)); Special Grand Jury Exhibit 12 (CPD001105-CPD001108) (Case Supplementary Report 3222163 (approved Nov. 8, 2004)); Special Grand Jury Exhibit 10 (CPD001115-CPD001128) (Case Supplementary Report 3193543 (approved Nov. 10, 2004)).

⁴³⁵ See Flynn, Patrick, Special Grand Jury Tr. at 41:1-10 (Mar. 13, 2013); Chasen, Michael, IGO Interview Rep. at 8 (Nov. 27, 2012) (“Chasen stated that he was not sure why the reports took so long to be completed (referencing Exhibit 6), and he stated that it was unusual.”)

⁴³⁶ See Cline, Philip, IGO Interview Rep. at 4 (Dec. 28, 2012).

⁴³⁷ See Yawger, Ronald, IGO Interview Tr. at 91:11-13 (July 1, 2011).

⁴³⁸ Special Grand Jury Exhibit 7 at CPD001054 (CPD001054-CPD001060) (Case Supplementary Report 3215651 (approved Nov. 10, 2004)).

also unusual.⁴³⁹

On November 10, 2004, Yawger submitted his concluding case supp report, using the PC login of his partner Giralamo.⁴⁴⁰ The report concludes:

Based upon the evidence examined in this incident, the interviews of all parties involved, and the line ups conducted, the following was concluded; the investigation of this incident did not reveal any unjustifiable behavior on behalf of the subject who either pushed or punched David Koschman as David Koschman was clearly the aggressor in this incident. Also, the actual identity of the subject who either pushed or punched David Koschman could not positively be determined.

Upon the completion of these interviews, and after conferring with ASA Darren O'Brien, it was decided that no charges would, or could be sought due to the fact that the victim in this incident, David Koschman, was clearly the aggressor as corroborated by all of the witnesses interviewed, in that David Koschman continued to attack the group of people consisting of Bridget McCarthy, Kevin McCarthy, Craig Denham, and Richard Vanecko resulting in the victim either being pushed or punched in self defense, which subsequently caused David Koschman to fall to the ground, striking his head, and causing his death.

Due to the above information, R/D's request this Involuntary Manslaughter investigation remain in PROGRESS.

The final case supp's conclusion is at odds with Yawger's request to O'Brien in May 2004, to charge the case; as well as Yawger's request to Epach to ask O'Brien to charge the case. Indeed, despite what Yawger's final case supp says, during his 2013 testimony before the special grand jury, he stated that he really did not know if Vanecko acted in self-defense.⁴⁴¹ And although, following the submission and approval of Yawger's reports, the Koschman case — per

⁴³⁹ See Clemens, Robert, Special Grand Jury Tr. at 119:15-120:1 (Apr. 24, 2013); Special Grand Jury Exhibit 123 at 6 (O'Leary, Robert, Kroll Interview Rep. (Oct. 8, 2012)); Giralamo, Anthony, IGO Interview Rep. at 4 (Dec. 21, 2012).

⁴⁴⁰ See Special Grand Jury Exhibit 10 (CPD001115-CPD001128) (Case Supplementary Report 3193543 (approved Nov. 10, 2004)); Yawger, Ronald, Special Grand Jury Tr. at 30:10-17 (July 15, 2013) (stating that he used Giralamo's PC login because Giralamo was not only out of town, but he was the one who initiated the original case supp; therefore, for Yawger to be able to update and edit the case supp created by Giralamo, he needed to use his partner's PC login).

⁴⁴¹ See Yawger, Ronald, Special Grand Jury Tr. at 155:1-156:16 (July 15, 2013).

CPD — remained open and “in progress” from November 2004 until 2011, no investigative activity at all took place during this time.

C. The 2011 CPD Re-investigation

1. January 4, 2011, *Sun-Times* FOIA Request

On January 4, 2011, *Sun-Times* reporter Tim Novak submitted a FOIA request to the Chicago Police Department seeking:

...copies of all police reports regarding an altercation or fight at 35 W. Division at 3:15 a.m. April 25, 2004.

The incident involved David Koschman, 21, of Mount Prospect, who later died of head injuries on May 6, 2004.

The police reports should contain a narrative describing the incident, as well as any other additional reports involving interviews with witnesses to the incident.

Please also include the names of any witnesses, including people who were interviewed by police officers.⁴⁴²

During his interview with the OSP in 2013, Superintendent Weis, CPD Superintendent in 2011, explained that he first learned of the FOIA request and the fact that the Koschman case remained “open”⁴⁴³ from CPD’s General Counsel Debra Kirby.⁴⁴⁴ According to Superintendent

⁴⁴² See Novak FOIA Request at IG_004500 (Jan. 4, 2011) (IG_004496-IG_004517).

⁴⁴³ According to Kobel, a case may be: (1) “closed, non-criminal” (for example, if a person died in a non-arson fire); (2) “cleared, closed” (for example, all offenders are in custody); (3) “cleared, open” (when some offenders remain not in custody); or (4) “cleared, closed/open, exceptional” (the offender is still outstanding but no charges will be filed). Kobel, Richard, IGO Interview Rep. at 5 (Jan. 17, 2013). According to Kobel, the Koschman case “could have been categorized as ‘cleared, open, exceptional’ because an offender identification was not made and no charges were sought. If an offender was identified and no charges were brought, it would have been ‘cleared, closed, exceptional.’” See Kobel, Richard, IGO Interview Rep. at 5 (Jan. 17, 2013). According to Area 3 Det. Sobolewski, “normally” a case would have been closed after the lineups and felony reviews interviews, stating, “there would be no reason to keep it open. Once you present the evidence to the State’s Attorney’s office, they determine whether charges are appropriate or not. They make that decision and we have nothing to do with that decision. And if they will not prosecute, you can close the case and bar the prosecution.” According to Sobolewski, the case should have been clear, closed after the lineups — meaning detectives know who the offender is but cannot prove it. Nevertheless, Sobolewski stated it was normal practice to also leave homicide cases open where the perpetrator had not been identified. Sobolewski, Andrew, IGO Interview Tr. at 55:5-57:2 (Aug. 5, 2011).

Weis, he was “shocked” the request involved an open 2004 investigation.⁴⁴⁵ When Superintendent Weis asked Kirby why the case was still open, Kirby informed him “things just happen.”⁴⁴⁶ Superintendent Weis recalled telling his Chief of Staff, Michael Masters, that this matter made CPD look bad and to get the Koschman case resolved.⁴⁴⁷ According to Masters, Superintendent Weis believed the case should be re-investigated and asked then Chief of Detectives Tom Byrne for recommendations on how the re-investigation should be conducted.⁴⁴⁸

Byrne subsequently directed Deputy Chief of Detectives Dean Andrews to review the findings of the 2004 investigation.⁴⁴⁹ According to then-Area 3 Commander Gary Yamashiroya, he received a request from either Andrews or Byrne to produce the original homicide file for the Koschman case, so Yamashiroya instructed Area 3 Homicide Lt. Denis Walsh⁴⁵⁰ to locate the

⁴⁴⁴ See Weis, Jody, IGO Interview Rep. at 1 (May 28, 2013). As discussed in more detail below, CPD’s Office of Legal Affairs would be notified of FOIA requests sent by members of the media. According to Superintendent Weis’ Chief of Staff, Michael Masters, Kirby attempted to notify Superintendent Weis in person shortly after receiving the FOIA request. Prior to notifying Superintendent Weis, Kirby stopped by Masters’s office in order to give him a “thirty second rundown.” According to Masters, Kirby told him that the FOIA requested information relating to a case from 2003 or 2004 and the name “Vanecko” may have come up during their discussion. See Masters, Michael, IGO Interview Rep. at 1 (May 16, 2013).

⁴⁴⁵ See Weis, Jody, IGO Interview Rep. at 1 (May 28, 2013).

⁴⁴⁶ See Weis, Jody, IGO Interview Rep. at 1 (May 28, 2013); Masters, Michael, IGO Interview Rep. at 2 (May 16, 2013) (stating that during a conversation with Superintendent Weis, Masters, and Kirby, “The question as to why the case was still open was posed, but neither Masters nor Superintendent Weis received a satisfactory response.”) When interviewed by the OSP in 2013, Kirby did not recall any specific conversations with Superintendent Weis about the Koschman matter. See Kirby, Debra, Kroll Interview Rep. at 4 (Feb. 15, 2013).

⁴⁴⁷ According to Superintendent Weis, he was focused on why the case was left pending and not properly closed in 2004. Superintendent Weis felt someone should have made the decision to close the case in 2004 and recalled then Superintendent Cline saying in 2004 there was insufficient evidence to charge the case. In Superintendent Weis’ opinion, the Koschman case was simple and could have been wrapped up in a month. See Weis, Jody, IGO Interview Rep. at 1-2 (May 28, 2013).

⁴⁴⁸ See Masters, Michael, IGO Interview Rep. at 2 (May 16, 2013).

⁴⁴⁹ See Special Grand Jury Exhibit 120 at 4 (Byrne, Thomas, Kroll Interview Rep. (Jan. 9, 2013)).

⁴⁵⁰ At the time of the April 25, 2004 Koschman incident, Walsh was a lieutenant in CPD’s 18th District, heading the Entertainment District Detail, a portion of which included Rush Street and Division Street. See O’Donnell, William, IGO Interview Rep. at 2 (Oct. 4, 2012); see Walsh, Denis, IGO Interview Rep. (Proffer) at 2 (Aug. 14, 2013). During his interview with the OSP, Walsh stated that the

file.⁴⁵¹ “Within ‘a few days,’” Walsh reported back to Yamashiroya that the Koschman homicide file could not be located.⁴⁵² After Andrews requested that Area 3 make an additional effort to find the file, Yamashiroya found a manila folder with reports relating to Koschman in his own personal credenza.⁴⁵³ Though, as detailed below, the manila folder Yamashiroya found was not the original Koschman homicide file. After reviewing the file found by Yamashiroya,⁴⁵⁴ Andrews recommended the case be re-assigned to Area 5 detectives.⁴⁵⁵

2. Reassignment to Area 5 Detectives

According to Andrews, after reviewing the police reports from 2004, he determined that certain investigative steps had not been taken and that certain information was missing.⁴⁵⁶ For example, Andrews concluded that despite multiple witnesses’ description of the “big guy” striking Koschman, the reports did not document heights and weights of any of the people in Vanecko’s group.⁴⁵⁷ During his interview with the OSP in January 2013, Andrews stated, “[i]f

first time he heard about the Koschman matter, or Mayor Daley’s nephew’s involvement, was in January 2011. Walsh, Denis, IGO Interview Rep. (Proffer) at 10 (Aug. 14, 2013).

⁴⁵¹ See Special Grand Jury Exhibit 148 at 3 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)).

⁴⁵² See Special Grand Jury Exhibit 148 at 3 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)).

⁴⁵³ See Special Grand Jury Exhibit 148 at 3 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)).

⁴⁵⁴ Andrews also reviewed certain police reports electronically via CHRIS. CPD maintains access logs which record the dates and times that users (as tracked by user PC Login number) access or print a case supp report logged into CHRIS. These logs are generated by running a report called a CLEAR report. According to CLEAR reports showing those who accessed Yawger’s concluding case supp report (Case Supplementary Report 3193543) and Rita O’Leary’s case supp report (Case Supplementary Report 3215651), Andrews accessed those police reports on January 11, 2011. See Special Grand Jury Exhibit 97 at CPD093727-CPD092730, CPD093737-CPD093739 (CPD093713-CPD093743) (CLEAR Report for Case Supp 3193543 and CLEAR Report for Case Supp 3215651).

⁴⁵⁵ See Special Grand Jury Exhibit 115 at 5 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)); See Weis, Jody, IGO Interview Rep. at 1 (May 28, 2013); Masters, Michael, IGO Interview Rep. at 2 (May 16, 2013).

⁴⁵⁶ See Special Grand Jury Exhibit 115 at 5 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)).

⁴⁵⁷ See Special Grand Jury Exhibit 115 at 5 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)).

that's not there, I don't know what else isn't there, so I want it re-investigated.”⁴⁵⁸ Andrews further stated his goals were to determine a correct classification for the case and whether there was sufficient evidence to name an offender.⁴⁵⁹ As a result, Andrews directed that witnesses be re-interviewed. Similarly, Byrne described the re-investigation as necessary because a “nexus” to Vanecko was present and “[i]t looked like all the parties involved were there. It was about connecting the dots.”⁴⁶⁰

According to Andrews, he chose Area 5 for the re-investigation because he was previously assigned there and was familiar with Area 5 detectives.⁴⁶¹ Area 5 Commander Joseph Salemme subsequently chose Det. James Gilger, and his partner, Det. Nick Spanos, to conduct the re-investigation because he was told to select his “best detective.”⁴⁶²

On January 13, 2011, Peterson and Andrews held a meeting at CPD’s headquarters at 3510 South Michigan Avenue to officially re-assign the Koschman case to Area 5 detectives.⁴⁶³

⁴⁵⁸ See Special Grand Jury Exhibit 115 at 5 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)). Yawger’s concluding police report in 2004 lists height and weight information for Koschman, Kevin McCarthy, and Vanecko. Special Grand Jury Exhibit 10 (CPD 001115-CPD001128) (Case Supplementary Report 3193543 (approved Nov. 10, 2004)). Andrews nevertheless explained during his interview with the OSP that he felt the descriptions in the report’s narrative are too limited and stated, “I need heights and weights, I need numbers.” Special Grand Jury Exhibit 115 at 8 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)).

⁴⁵⁹ See Special Grand Jury Exhibit 115 at 5 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)).

⁴⁶⁰ See Special Grand Jury Exhibit 120 at 5 (Byrne, Thomas, Kroll Interview Rep. (Jan. 9, 2013)).

⁴⁶¹ See Special Grand Jury Exhibit 115 at 5 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)). Prior to the January 13, 2011, meeting, Gilger and Andrews had a history of working together. In August 2003, Gilger was detailed to CPD’s intelligence unit where Andrews was commander. Gilger, James, Special Grand Jury Tr. at 87:23-88:21 (Jan. 16, 2013). Later, when Gilger was detailed to Area 5, Andrews was again his commander. Gilger, James, Special Grand Jury Tr. at 87:23-88:21 (Jan. 16, 2013). Andrews and Cirone were personal friends. Special Grand Jury Exhibit 115 at 14 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)). Gilger and Salemme also had a prior history of working together. As Gilger testified, “[w]e’re very tight,” having known each other for “about 25 years or even longer probably.” Gilger, James, Special Grand Jury Tr. at 89:1-7 (Jan. 16, 2013).

⁴⁶² See Special Grand Jury Exhibit 109 at 4 (Salemme, Joseph, Kroll Interview Rep. (Jan. 15, 2013)); Special Grand Jury Exhibit 115 at 8 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)). Nevertheless, Area 5 Sgt. Thomas Mills stated during his interview with the OSP that “this information [the decision to select Gilger] was ‘likely run up the chain of command.’” See Special Grand Jury Exhibit 108 at 2 (Mills, Thomas, Kroll Interview Rep. (Aug. 20, 2012)).

⁴⁶³ See Gilger, James, Special Grand Jury Tr. at 75:22-76:14, 77:3-78:21 (Jan. 16, 2013).

Peterson, Byrne, Andrews, Yamashiroya, Walsh, Salemme, Cirone, and Gilger all attended the meeting, which occurred in Byrne's office.⁴⁶⁴ Office of Legal Affairs attorney Bill Bazarek also attended for at least a portion of the meeting.⁴⁶⁵ The meeting lasted approximately a half-hour to an hour.⁴⁶⁶

According to Andrews, he informed those present that the case was being re-assigned to Area 5 detectives in order to have a "fresh set of eyes"⁴⁶⁷ investigate. Andrews told Area 5 detectives what evidence he thought was missing and instructed them to re-interview witnesses.⁴⁶⁸ According to Salemme, along with explaining the re-assignment, Andrews "may have said he reviewed the file and he thought it was either chargeable or clear, closed exceptional."⁴⁶⁹ He had some feeling after reviewing it."⁴⁷⁰ According to Salemme, the meeting also included a brief summary of the previous investigation along the lines of "Vanecko is a

⁴⁶⁴ See Special Grand Jury Exhibit 115 at 7 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)); Special Grand Jury Exhibit 116 at 2 (Peterson, Steven, IGO Interview Rep. (Feb. 4, 2013)); Special Grand Jury Exhibit 148 at 4 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)); *but see* Special Grand Jury Exhibit 109 at 3 (Salemme, Joseph, Kroll Interview Rep. (Jan. 15, 2011)) (meeting occurred in Andrews' office). See Gilger, James, Special Grand Jury Tr. at 75:22-76:14; 77:3-78:21 (Jan. 16, 2013). Yamashiroya and Walsh attended from Area 3 in order to provide the case file and because the case originated as an Area 3 homicide case. Although both representatives from Area 3 and Area 5 were aware of the pending re-assignment prior to the meeting, Area 3 Commander Yamashiroya voiced some reluctance to transfer a case previously assigned to Area 3. See Special Grand Jury Exhibit 115 at 7 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)); Cirone, Sam, Kroll Interview Rep. (Proffer) at 5 (Mar. 22, 2013); Bazarek, William, Kroll Interview Rep. at 4 (Mar. 13, 2013); Special Grand Jury Exhibit 109 at 4 (Salemme, Joseph, Kroll Interview Rep. (Jan. 15, 2013)). The case was nevertheless re-assigned to Area 5.

⁴⁶⁵ See Bazarek, William, Kroll Interview Rep. at 3 (Mar. 13, 2013).

⁴⁶⁶ See Special Grand Jury Exhibit 148 at 4 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 15, 2013)) (20-30 minutes); Special Grand Jury Exhibit 115 at 7 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)) (30 minutes); Special Grand Jury Exhibit 109 at 3 (Salemme, Joseph, Kroll Interview Rep. (Jan. 15, 2013)) (45-60 minutes).

⁴⁶⁷ Special Grand Jury Exhibit 116 at 3 (Peterson, Steven, IGO Interview Rep. (Feb. 4, 2013)).

⁴⁶⁸ See Special Grand Jury Exhibit 115 at 7 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)).

⁴⁶⁹ A case may be clear, closed exceptionally where the offender is identified but there is some bar to law enforcement bringing charges. See Kobel, Richard, IGO Interview Rep. at 5 (Jan. 17, 2013).

⁴⁷⁰ Special Grand Jury Exhibit 109 at 5 (Salemme, Joseph, Kroll Interview Rep. (Jan. 15, 2013)); Special Grand Jury Exhibit 115 at 5 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)) (Andrews decided the Koschman matter needed to be re-investigated after he reviewed the 2004 investigation).

suspect, he's related to Daley, the investigation stopped at some point.”⁴⁷¹

During the meeting, according to Gilger, he asked those present whether he should contact Yawger and was instructed to not contact him.⁴⁷² When interviewed by the OSP, Andrews stated that no such instruction was given and that there was an “expectation” that Gilger would have communicated with detectives involved in the 2004 investigation.⁴⁷³ Similarly, Salemme stated during his interview with the OSP in January 2013 that he presumed someone had contacted Yawger to ask about the location of the original homicide file and that he knew that Gilger and Yawger were playing “phone tag” at one point, but was unsure whether they had ever spoken.⁴⁷⁴ Peterson also indicated that the decision of whether to contact the detectives who worked on the case in 2004 was left up to Gilger and Spanos.⁴⁷⁵ During his interview with the OSP, Yamashiroya further described yet another scenario, stating that at the meeting there was “some talk about talking to Detective Yawger” and that Walsh was going to reach out to him.⁴⁷⁶ During Walsh’s interview with the OSP, he recalled that during this meeting

⁴⁷¹ See Special Grand Jury Exhibit 109 at 3 (Salemme, Joseph, Kroll Interview Rep. (Jan. 15, 2013)); see also Gilger, James Special Grand Jury Tr. at 95:20-96:7 (Jan. 16, 2013) (stating the group discussed “Basically that Vanecko had been brought in, lineups had been done and he was never picked out. Never gave a statement. And basically they asked me to reinvestigate the case.”). Within CPD, ostensibly there were several procedures that may have caught an open case such as the Koschman investigation. One such process is a “homicide audit” or a “homicide audit report” — in essence a process whereby a homicide file would be examined for deficiencies. According to Andrews, because the Koschman investigation was classified as an involuntary manslaughter investigation in 2004, it would not have been the subject of a homicide audit. See Special Grand Jury Exhibit 115 at 9 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)). Superintendent Weis and Masters further expressed disappointment that the Koschman investigation had remained open since 2004, given the institution of a process as part of Superintendent Weis’ administration whereby detective area commanders and detective division personnel were responsible for identifying and accounting for open homicide investigations. See Weis, Jody, IGO Interview Rep. at 2 (May 28, 2013); Masters, Michael, IGO Interview Rep. at 2 (May 16, 2013).

⁴⁷² See Gilger, James, Special Grand Jury Tr. at 83:13-15 (Jan. 16, 2013).

⁴⁷³ See Special Grand Jury Exhibit 115 at 8 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)).

⁴⁷⁴ See Special Grand Jury Exhibit 109 at 5 (Salemme, Joseph, Kroll Interview Rep. (Jan. 15, 2013)).

⁴⁷⁵ See Special Grand Jury Exhibit 116 at 3 (Peterson, Steven, IGO Interview Rep. (Feb. 4, 2013)).

⁴⁷⁶ Yamashiroya said he recalled some discussion at the meeting about the need to speak with Yawger but did not know if anyone from Area 5 ever spoke with him. See Special Grand Jury Exhibit 148 at 5 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)).

he was ordered by a superior to talk to Yawger about CPD's 2004 investigation, which he did sometime later that month.⁴⁷⁷

In lieu of the original homicide file, which could not be located, Yamashiroya brought the file he found in his credenza to turn over to Area 5 detectives at the January 2011 meeting.⁴⁷⁸ According to Salemme, the fact that the original investigative file was missing was discussed at the meeting, though others present did not recall any such discussion.⁴⁷⁹ Area 5 detectives left the meeting with the assignment to re-investigate Koschman's death.⁴⁸⁰

3. Area 5's Investigation

Before the special grand jury in January 2013, Gilger testified that the "very first thing" detectives did as part of the re-investigation was visit SAO's criminal offices at 2650 South California Avenue to request the felony review file for the case.⁴⁸¹ Gilger's motivation for attempting to find the file was to see if O'Brien had recorded any witness statements from his interviews on May 20, 2004.⁴⁸² Gilger requested the felony review file from Brassil, then the head of the Felony Review unit. Brassil and another ASA looked up the Koschman case in

⁴⁷⁷ Walsh, Denis, IGO Interview Rep. (Proffer) at 7, 9 (Aug. 14, 2013).

⁴⁷⁸ See Special Grand Jury Exhibit 148 at 4 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)); Special Grand Jury Exhibit 109 at 5 (Salemme, Joseph, Kroll Interview Rep. (Jan. 15, 2013)); Cirone, Sam, Kroll Interview Rep. (Proffer) at 5 (Mar. 22, 2013).

⁴⁷⁹ See Special Grand Jury Exhibit 109 at 5, 9 (Salemme, Joseph, Kroll Interview Rep. (Jan. 15, 2013)). Cirone stated he was unsure whether there was any discussion of what was missing, but he "assume[d] there was." See Cirone, Sam, Kroll Interview Rep. (Proffer) at 5 (Mar. 22, 2013). Andrews stated he could not recall such a discussion. See Special Grand Jury Exhibit 115 at 7 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)). During his interview, Yamashiroya indicated there was no discussion at the January 13, 2011 meeting regarding why the original case file could not be located. See Special Grand Jury Exhibit 148 at 5 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)).

⁴⁸⁰ According to Cirone, who supervised both Gilger and Spanos, the detectives worked exclusively on the re-investigation during this time period, and did not receive any other assignments. See Cirone, Sam, Kroll Interview Rep. (Proffer) at 7 (Mar. 22, 2013). Additionally, Gilger and Spanos were instructed to keep the re-investigation confidential. See Gilger, James, Special Grand Jury Tr. at 82:4-21 (Jan. 16, 2013); Cirone, Sam, Kroll Interview Rep. (Proffer) at 7 (Mar. 22, 2013).

⁴⁸¹ See Gilger, James, Special Grand Jury Tr. at 106:17-107:2, 107:19-22, 109:13-110:3 (Jan. 16, 2013).

⁴⁸² See Gilger, James, Special Grand Jury Tr. at 106:17-107:2, 107:19-22 (Jan. 16, 2013).

SAO's database, "PROMIS," but could not find any files.⁴⁸³ Brassil informed Gilger he would attempt to locate the file but called him a couple of days later, saying SAO did not have a felony review file for the Koschman case.⁴⁸⁴

Gilger and Spanos conducted their first witness interview that Sunday night, January 16, 2011, when they interviewed Koschman's friend, Sazian.⁴⁸⁵ Because Sazian was not present for the altercation on April 25, 2004, he did not provide much information regarding the incident itself.⁴⁸⁶ Nevertheless, detectives asked Sazian whether he would submit to a polygraph examination, to which Sazian agreed.⁴⁸⁷

On the following Monday afternoon, January 17, 2011, Gilger and Spanos interviewed three of Koschman's friends: Allen, Copeland, and Hageline.⁴⁸⁸ Gilger and Spanos first interviewed Copeland at his house at approximately 8:30 p.m.⁴⁸⁹ According to the first line of Gilger's GPR, Copeland "related essentially the same account as earlier reported."⁴⁹⁰ According to Gilger's GPR of Copeland's interview, Koschman's friends were all trying to keep Koschman away "from starting anymore trouble,"⁴⁹¹ when Koschman broke free and "walk[ed] back

⁴⁸³ See Gilger, James, Special Grand Jury Tr. at 110:6-8 (Jan. 16, 2013).

⁴⁸⁴ See Gilger, James, Special Grand Jury Tr. at 110:8-12 (Jan. 16, 2013).

⁴⁸⁵ See Special Grand Jury Exhibit 75 (CPD001259) (General Progress Report re Sazian interview (approved Feb. 28, 2011)).

⁴⁸⁶ See Special Grand Jury Exhibit 75 (CPD001259) (General Progress Report re Sazian interview (approved Feb. 28, 2011)).

⁴⁸⁷ See Special Grand Jury Exhibit 75 (CPD001259) (General Progress Report re Sazian interview (approved Feb. 28, 2011)).

⁴⁸⁸ According to a General Progress Report dated January 17, 2011, Gilger may have attempted to interview Francis at approximately 6:30 p.m. and learned that Francis lived in Colorado. See General Progress Report re Francis (approved Feb. 28, 2011) (CPD001247).

⁴⁸⁹ See Special Grand Jury Exhibit 76 (CPD001252-CPD001254) (General Progress Report re Copeland interview (approved Feb. 28, 2011)).

⁴⁹⁰ See Special Grand Jury Exhibit 76 (CPD001252-CPD001254) (General Progress Report re Copeland interview (approved Feb. 28, 2011)).

⁴⁹¹ Based upon the GPR of this interview, Gilger's case supp report states, "Copeland stated that they were trying to pull KOSCHMAN away from starting anymore [sic] trouble" before he was struck. See Special Grand Jury Exhibit 15 at CPD001231 (CPD001199-CPD001234) (Case Supplementary Report

towards the other group and. . . the largest of the male whites” in the other group punched Koschman.⁴⁹² Copeland further told Gilger he thought Koschman was “knocked out” by the punch.⁴⁹³

At approximately 9:30 p.m. on January 17, 2011, Gilger interviewed Allen (who was living in Colorado at the time) by phone.⁴⁹⁴ According to Gilger’s GPR, Allen stated that after the initial bump “everyone started arguing and yelling ‘screw you’” and that the people in the other group were “the aggressors.”⁴⁹⁵ Gilger’s GPR of the Allen interview also reads that Koschman “was in the thick of the argument and was also yelling.”⁴⁹⁶ According to Gilger’s GPR, Allen also stated that he saw Koschman get punched by the offender, who was “clearly the

8585610 (approved Feb. 28, 2011)). During his testimony before the special grand jury in 2012, Copeland testified this statement was not an accurate reflection of what happened the night of the incident, stating, “No. Again, I mean, I do remember, you know, gesturing and nudging him to kind of move away, but physically pulling him back, I don’t remember doing that.” *See* Copeland, James, Special Grand Jury Tr. at 12:16-19 (Aug. 8, 2012).

⁴⁹² *See* Special Grand Jury Exhibit 76 at CPD001252 (CPD001252-CPD001254) (General Progress Report re Copeland interview (approved Feb. 28, 2011)). Based upon the GPR of this interview, Gilger’s case supp report states, “Copeland stated when KOSCHMAN walked up to this group.” *See* Special Grand Jury Exhibit 15 at CPD001231 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 858620 (approved Feb. 28, 2011)). Before the special grand jury, Copeland clarified that the statement that Koschman “walked up to this group” was inaccurate because, “he was — he didn’t walk up and immediately get punched. He did make his way back over, and then we came back. And we were kind of in — the whole — both groups were kind of in the same area. And the punch occurred shortly after that.” *See* Copeland, James, Special Grand Jury Tr. at 13:10-16 (Aug. 8, 2012).

⁴⁹³ *See* Special Grand Jury Exhibit 76 at CPD001252 (CPD001252-CPD001254) (General Progress Report re Copeland interview (approved Feb. 28, 2011)).

⁴⁹⁴ *See* Special Grand Jury Exhibit 77 (CPD001257-CPD001258) (General Progress Report re Allen interview (approved Feb. 28, 2011)).

⁴⁹⁵ *See* Special Grand Jury Exhibit 77 at CPD001257 (CPD001257-CPD001258) (General Progress Report re Allen interview (approved Feb. 28, 2011)).

⁴⁹⁶ Based upon the GPR of this interview, Gilger’s case supp report states, “Allen stated he saw Koschman in the thick of the argument, who was also yelling.” *See* Special Grand Jury Exhibit 15 at CPD001231 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 858620 (approved Feb. 28, 2011)). Allen testified before the special grand jury in 2012 that the statement was inaccurate, “[b]ecause it’s not like he was in the thick of the argument. It was one giant argument and we were all yelling, so no, I would not — I did not say that.” *See* Allen, Scott, Special Grand Jury Tr. at 29:13-16 (Aug. 8, 2012).

biggest guy of the three.”⁴⁹⁷

Finally, at approximately 10:30 p.m., Gilger interviewed Hageline (who was living in California at the time) by phone. According to Gilger’s GPR, Hageline “saw [Koschman] get punched in the face, once in the face.”⁴⁹⁸ During his testimony before the special grand jury in 2012, Hageline clarified that, “I had stepped away from the two groups to get a cab because I didn’t believe that the situation was — was going to resolve itself, so I was just stepping away to get my friends in a cab. Shortly thereafter, maybe a second or two, I had seen some kind of movement and it looked like a punch, but I didn’t have a clear view of it. It was just something kind of like over my shoulder. But it seemed to be a punch.”⁴⁹⁹

Gilger and Spanos interviewed Koschman’s other friend on the scene, Francis, by telephone on January 18, 2011. Because Francis was living in Colorado, Gilger and Spanos interviewed him by phone.⁵⁰⁰ Gilger’s GPR of their interview with Francis states that he saw Koschman accidentally bump into the other group.⁵⁰¹ According to the GPR, after both groups started yelling at each other, Copeland and Francis attempted to break things up since he knew Koschman was “a little mad” and had “a lil temper.”⁵⁰² The GPR further states that everyone

⁴⁹⁷ See Special Grand Jury Exhibit 77 at CPD001258 (CPD001257-CPD001258) (General Progress Report re Allen interview (approved Feb. 28, 2011)). According to Allen’s 2012 testimony before the special grand jury, he himself was not at times entirely cooperative with CPD in 2011, in that, while being interviewed by police during the re-investigation, he impolitely criticized CPD’s work on the Koschman matter. See Allen, Scott, Special Grand Jury Tr. at 14:19-15:3, 45:7-46:6 (Aug. 8, 2012).

⁴⁹⁸ See Special Grand Jury Exhibit 78 at CPD001255 (CPD001255-CPD001256) (General Progress Report re Hageline interview (approved Feb. 28, 2011)). Gilger’s case supp report states, “Hageline observed KOSCHMAN get punched once in the face, and he fell backwards and hit his head on the street.” See Special Grand Jury Exhibit 15 at CPD001232 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 858620 (approved Feb. 28, 2011)). Hageline clarified before the special grand jury that this statement was not accurate because Hageline “had stepped away from the group” and did not actually see Koschman being punched in the face. See Hageline, Shaun, Special Grand Jury Tr. at 25:20-21 (Aug. 8, 2012).

⁴⁹⁹ See Hageline, Shaun, Special Grand Jury Tr. at 15:2-11 (Aug. 8, 2012).

⁵⁰⁰ See Gilger, James, Special Grand Jury Tr. at 133:10-17 (Jan. 16, 2013).

⁵⁰¹ See Special Grand Jury Exhibit 79 at CPD001250 (CPD001250-CPD001251) (General Progress Report re Francis interview (approved Feb. 28, 2011)).

⁵⁰² See Special Grand Jury Exhibit 79 at CPD001250 (CPD001250-CPD001251) (General Progress Report re Francis interview (approved Feb. 28, 2011)).

was walking away and Francis thought the altercation was over, when Koschman “went at this guy.”⁵⁰³ Francis testified before the special grand jury in 2012 that he was not sure whether that statement was accurate stating, “I mean, I kind of don’t know what ‘go after’ means. I mean, he kept talking to him. He didn’t go after him in the terms of — in the sense that he was, like, trying to fight him or anything like that.”⁵⁰⁴ According to the GPR, Francis next saw Koschman get punched⁵⁰⁵ such that “it looked like he was knocked off of his feet.”⁵⁰⁶ As with Sazian, detectives asked Copeland, Allen, Hageline, and Francis whether they would submit to polygraph examinations, and all agreed.⁵⁰⁷ Ultimately, detectives did not require polygraphs of any of the witnesses.

Detectives also interviewed the two bystander witnesses, Kohler and Connolly, on January 18 and 19, 2011 respectively.⁵⁰⁸ During his interview with Area 5 detectives on January 18, Kohler told detectives for the first time that based on seeing photos in a *Sun-Times* article, he recognized Vanecko as a high school classmate of his at Loyola Academy, but did not recognize Vanecko on the night of the incident.⁵⁰⁹ According to Gilger’s GPR of his interview with

⁵⁰³ See Special Grand Jury Exhibit 79 at CPD001251 (CPD001250-CPD001251) (General Progress Report re Francis interview (approved Feb. 28, 2011)).

⁵⁰⁴ See Francis, David, Special Grand Jury Tr. at 24:18-22 (Aug. 8, 2012).

⁵⁰⁵ Before the special grand jury, Francis testified that he could not remember whether he actually saw Koschman punched. See Francis, David, Special Grand Jury Tr. at 25:10-12 (Aug. 8, 2012).

⁵⁰⁶ See Special Grand Jury Exhibit 79 at CPD001251 (CPD001250-CPD001251) (General Progress Report re Francis interview (approved Feb. 28, 2011)).

⁵⁰⁷ See Special Grand Jury Exhibit 76 at CPD001254 (CPD001252-CPD001254) (General Progress Report re Copeland interview (approved Feb. 28, 2011)); Special Grand Jury Exhibit 77 at CPD001258 (CPD001257-CPD001258) (General Progress Report re Allen interview (approved Feb. 28, 2011)); Special Grand Jury Exhibit 15 at CPD001232 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 858620 (approved Feb. 28, 2011)); Special Grand Jury Exhibit 79 at CPD001251 (CPD001250-CPD001251) (General Progress Report re Francis interview (approved Feb. 28, 2011)).

⁵⁰⁸ See Special Grand Jury Exhibit 15 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 858620 (approved Feb. 28, 2011)).

⁵⁰⁹ See Special Grand Jury Exhibit 80 at CPD001249 (CPD001248-CPD001249) (General Progress Report 323454 (approved Feb. 28, 2011)). In 2004, Kohler told Giralamo he had never seen anyone in Vanecko’s group prior to the incident. See General Progress Report (approved May 13, 2004) (CPD001588).

Kohler, Kohler related that “pushing and shoving happened between the two groups.”⁵¹⁰ Kohler testified before the special grand jury in 2012 that he did not believe that statement was accurate, stating, “I believe I stated that they were arguing, but I don’t think I said anything about pushing or shoving at that point.”⁵¹¹ Similar to what he told Giralamo in 2004, Gilger’s GPR records Kohler as indicating Koschman “jumped into the middle of the argument” and fell backwards.⁵¹² Kohler clarified in his special grand jury testimony in 2012 that Koschman “jumped in and it was immediate that he came back out,” that “[a]lmost immediately after Koschman moved between the two groups, he came flying back and fell straight back like a dead weight. It was like an explosion.”⁵¹³

According to Gilger’s GPR of his interview with Connolly, Connolly stated the two groups were beginning to argue when Connolly and Kohler arrived.⁵¹⁴ The GPR indicates Connolly stated Koschman was “doing most of the talking,” the argument “got really heated,” and Koschman “appeared to be pushed by one of the other guys.”⁵¹⁵ The GPR states that Connolly saw Koschman “get pushed by someone, tripped on the back of the curb, [and] fell backwards.”⁵¹⁶ During his testimony before the special grand jury in 2012, Connolly clarified that, “It was an assumption on my part it was a push because I was — my view was impeded by the other people in the group when David stepped onto the sidewalk. And then he was — I interpreted it to be a push that caused him to fall backwards. … But I did not see a push or a

⁵¹⁰ See Special Grand Jury Exhibit 80 at CPD001248 (CPD001248-CPD001249) (General Progress Report 323454 (approved Feb. 28, 2011)).

⁵¹¹ See Kohler, Phillip, Special Grand Jury Tr. at 6:17-19 (Aug. 8, 2012).

⁵¹² See Special Grand Jury Exhibit 80 at CPD001248 (CPD001248-CPD001249) (General Progress Report 323454 (approved Feb. 28, 2011)).

⁵¹³ See Kohler, Phillip, Special Grand Jury Tr. at 12:18-19 (Aug. 8, 2012); Kohler, Phillip, Special Grand Jury Tr. at 9:5-16 (July 11, 2012).

⁵¹⁴ See Special Grand Jury Exhibit 81 at CPD001245 (CPD001245-CPD001246) (General Progress Report re: Connolly interview (approved Feb. 28, 2011)).

⁵¹⁵ See Special Grand Jury Exhibit 81 at CPD001246 (CPD001245-CPD001246) (General Progress Report re: Connolly interview (approved Feb. 28, 2011)).

⁵¹⁶ See Special Grand Jury Exhibit 81 at CPD001246 (CPD001245-CPD001246) (General Progress Report re: Connolly interview (approved Feb. 28, 2011)).

punch. I was blocked. My vision was blocked. I interpreted it to be a push.”⁵¹⁷

On January 21, 2011, Gilger ran into O’Brien in the hallway outside the library at SAO’s offices at 2650 South California Avenue and had a one- or two-minute conversation about the Koschman case.⁵¹⁸ Specifically, they discussed issues with the case, including self-defense or lack of identification, or both.⁵¹⁹ Although reflected in the case supp concluding the 2011 re-investigation, the OSP has found no GPR memorializing this encounter.

On January 24, 2011, Gilger and Spanos went to the home of Kevin and Bridget McCarthy in an attempt to interview them.⁵²⁰ Kevin McCarthy instructed his wife not to speak with the detectives.⁵²¹ Kevin McCarthy then related that he and his wife were represented by counsel and that they stood by their statements from 2004.⁵²² On January 27, 2011, Gilger attempted to interview Denham by phone.⁵²³ Denham told detectives he did not have anything to add to his prior statement to police in 2004 and related “essentially the same account” that the group had been drinking, Vanecko pushed him as they both ran down the street, and he did not witness Vanecko or Kevin McCarthy punch anyone.⁵²⁴

Gilger and Spanos also attempted to interview Vanecko. On January 24, 2011, they

⁵¹⁷ See Connolly, Michael, Special Grand Jury Tr. at 9:15-10:1 (Aug. 8, 2012).

⁵¹⁸ See Special Grand Jury Exhibit 15 at CPD001204 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)); O’Brien, Darren, Special Grand Jury Tr. at 57:7-18 (May 8, 2013).

⁵¹⁹ See Special Grand Jury Exhibit 15 at CPD001204 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)); O’Brien, Darren, Special Grand Jury Tr. at 57:7-18 (May 8, 2013).

⁵²⁰ See Special Grand Jury Exhibit 15 at CPD001204 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

⁵²¹ See Special Grand Jury Exhibit 15 at CPD001204 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

⁵²² See Special Grand Jury Exhibit 15 at CPD001204 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

⁵²³ See Special Grand Jury Exhibit 83 (CPD001244) (General Progress Report re: Denham interview (approved Feb. 28, 2011)).

⁵²⁴ Special Grand Jury Exhibit 83 (CPD001244) (General Progress Report re: Denham interview (approved Feb. 28, 2011)).

attempted to locate Vanecko at [REDACTED] South Michigan Avenue, his last known address, but were informed by a doorman that Vanecko no longer lived there.⁵²⁵ On February 9, 2011, Gilger spoke with Vanecko's attorney, Marc Martin.⁵²⁶ Gilger told Martin that Spanos and he wanted to speak with Vanecko about the 2004 incident, but Martin explained that his client would not be making any statements.⁵²⁷ Gilger requested that Vanecko either come to Area 5 headquarters or call him on the telephone in order to personally invoke his right to remain silent.⁵²⁸ Martin agreed.⁵²⁹ Later that day, Gillespie called Gilger and told him that he, and not Martin, would be representing Vanecko.⁵³⁰ Gillespie indicated that he would speak with his client about coming into Area 5 to make a statement.⁵³¹

Afterward, Gilger sent an e-mail to Walsh to give him "an update on the Vanecko case . . .".⁵³² In his e-mail, Gilger described his conversation with Gillespie, including that he had told him "if this is self-defense, we need to know this."⁵³³ The e-mail further states, "I told Gillespie that Felony Review is already involved in this case, which they are, and will possibly be asked to review the case, which I know is going to be a rejection."⁵³⁴ According to Gilger, he

⁵²⁵ Special Grand Jury Exhibit 15 at CPD001204-CPD001205 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

⁵²⁶ Special Grand Jury Exhibit 15 at CPD001206 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

⁵²⁷ Special Grand Jury Exhibit 15 at CPD001206 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

⁵²⁸ Special Grand Jury Exhibit 15 at CPD001206 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

⁵²⁹ Special Grand Jury Exhibit 15 at CPD001206 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

⁵³⁰ Special Grand Jury Exhibit 15 at CPD001206 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

⁵³¹ Special Grand Jury Exhibit 15 at CPD001206 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

⁵³² Special Grand Jury Exhibit 86 (CPD000464) (Gilger e-mail (Feb. 9, 2011)).

⁵³³ Special Grand Jury Exhibit 86 (CPD000464) (Gilger e-mail (Feb. 9, 2011)).

⁵³⁴ Special Grand Jury Exhibit 86 (CPD000464) (Gilger e-mail (Feb. 9, 2011)).

meant that the Felony Review unit “know[s] I’m working on the case. As a matter of fact, they [SAO’s Felony Review unit] even consulted with Darren O’Brien on the case, so they’re involved in that respect. That’s what I meant here.”⁵³⁵ Gilger testified that what he meant by “which I know is going to be a rejection” was that based upon O’Brien’s decision in 2004 — and without a statement from Vanecko, no identification of the offender in a lineup, and Vanecko’s friends refusing to provide additional statements in 2011 — charges would be rejected.⁵³⁶ A few days later, Martin called Gilger and told him that Vanecko would not be coming in.⁵³⁷

4. Draft Reports

On February 10, 2011, Gilger initiated a draft report in CHRIS (CPD’s system for electronically storing police reports) that would form the basis of his final case supp report.⁵³⁸ By February 11, 2011, Gilger had drafted the narrative section of his report concluding the 2011 re-investigation.⁵³⁹ Gilger testified that this draft was a working version of the final report, but

⁵³⁵ Gilger, James, Special Grand Jury Tr. at 12:16-13:4 (Jan. 23, 2013). O’Brien was not part of SAO’s Felony Review unit in 2011. *See* O’Brien, Darren, IGO Interview Rep. at 2 (Feb. 5, 2013).

⁵³⁶ *See* Gilger, James, Special Grand Jury Tr. at 14:21-16:14 (Jan. 23, 2013) (“Well, based on what I had so far. You know, if I couldn’t get Richard Vanecko in there to give me a statement, what do I have? I don’t have any — I don’t have any statement from the defendant in this case. I have no identification in a lineup. And the witnesses that are on Vanecko’s side are asking for their lawyer, and they’re not cooperating with me either.”)

⁵³⁷ *See* Special Grand Jury Exhibit 15 at CPD001206 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)). To be clear, Vanecko was not legally or constitutionally obligated to make any statement to CPD.

⁵³⁸ *See* Case Statuses for HK323454 at CPD006061-CPD006062 (Sept. 23, 2011) (CPD006052-CPD006064). Cirone officially reassigned the case within CHRIS on February 9, 2011. *See* Case Statuses for HK323454 at CPD006052 (Sept. 23, 2011) (CPD006052-CPD006064). Ultimately, because Gilger’s final case supp report restated much of the narrative of police reports from 2004, it had to be split into two separate case supp reports, Case Supplementary Reports 8585610 and 8585620, in order to enter it into CHRIS. *See* Special Grand Jury Exhibit 116 at 5 (Peterson, Steve, IGO Interview Rep. (Feb. 4, 2013); Special Grand Jury Exhibit 108 at 4 (Mills, Thomas, Kroll Interview Rep. (Aug. 20, 2012)).

⁵³⁹ On February 11, 2011, Area 5 Det. Leal sent two files via e-mail to Gilger — “HK323454 narrative.doc” and “HK323454.pdf.” Special Grand Jury Exhibit 89 at CPD016769 (CPD016769-CPD016827) (Leal e-mail (Feb. 11, 2011)). According to both Leal and Gilger, Leal sent this e-mail while helping Gilger transfer a draft narrative from a thumb drive to CHRIS. Leal, Emiliano, Kroll Interview Rep. at 3 (Dec. 6, 2012); Gilger, James, Special Grand Jury Tr. at 22:8-23:6 (Jan. 23, 2013). Detectives often draft their report narratives outside of CHRIS — saving it to a thumb drive, for example — because of deficiencies with CHRIS. Gilger, James, Special Grand Jury Tr. at 23:11-21 (Jan. 23,

that it reflected “what [his] thinking was” up to that date.⁵⁴⁰ Spanos echoed this sentiment during his testimony before the special grand jury.⁵⁴¹

The February 11, 2011, draft narrative concluded as follows:

In conclusion, interviews with eyewitnesses after the incident described a tall, or taller, male white subject who punched KOSCHMAN. At the time of the incident, Richard VANECKO was 6'02" and approximately 230 pounds, which is clearly taller and heavier than Craig DENHAM, and clearly heavier than Kevin MCCARTHY. When initially interviewed, Scott ALLEN and James COPELAND stated the male white (VANECKO) who punched the victim, and the male white (DENHAM) who was arguing with KOSCHMAN, ran away together. When interviewed, HAGELINE thought the person who punched KOSCHMAN was the tallest of the three subjects that morning. The interview with DENHAM, who admitted that he and VANECKO left in a cab together and later said VANECKO was pushing him down the street before entering this cab, confirmed this fact. Interviews were conducted with Bridget and Kevin MCCARTHY and Craig DENHAM, who confirmed the fact that VANECKO and DENHAM left together. And finally, when asked to give a statement to Area 3 Detectives following his lineup, VANECKO declined on the advice of his attorney, which only cast additional suspicion on him as the person who punched David KOSCHMAN.

Though [sic] the course of this lengthy investigation, it was clearly obvious that Richard VANECKO punched David KOSCHMAN, in spite of the fact that none of the eyewitnesses ever identified him as such.

In view of the above, the R/Ds request this be classified as

2013). Compare Special Grand Jury Exhibit 89 at CPD016770-CPD016798 (CPD016769-CPD016827) (Draft Case Supplementary Report 323454 (Feb. 11, 2011)) with Special Grand Jury Exhibit 15 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

The OSP attempted to obtain e-mails from CPD for 2004 but was unsuccessful. CPD's e-mail archives date back only to 2009. See Ofc. Anthony Isla correspondence (Mar. 12, 2013) (CPD097080). As a result, in responding to the OSP's subpoena request for responsive e-mails, CPD was able to retrieve documents dating back only that far. See Anthony Isla correspondence (Mar. 12, 2013) (CPD097080).

⁵⁴⁰ See Gilger, James, Special Grand Jury Tr. at 33:23-34:2 (Jan. 23, 2013).

⁵⁴¹ See Spanos, Nicholas, Special Grand Jury Tr. at 86:4-10 (Feb. 6, 2013).

CLEARED, EXCEPTIONALLY, CLOSED.⁵⁴²

Gilger's February 11, 2011, draft narrative contains no reference to Vanecko acting in self-defense.⁵⁴³ Additionally, though the draft contained a placeholder for what Gilger hoped would be a report of his interview of Vanecko ("On 14 Feb 2011 at XXXX hours, Richard VANECKO") (ellipses in original), it contained no similar placeholder for a section concerning self-defense.⁵⁴⁴ The draft narrative also does not reference the January 21, 2011, encounter between Gilger and O'Brien.⁵⁴⁵

As indicated in this draft, by February 11, 2011, Gilger had concluded that Vanecko had punched Koschman.⁵⁴⁶ Moreover, Gilger and Spanos did not undertake any additional witness interviews or gather any additional evidence as part of their re-investigation after this date, according to their reports.⁵⁴⁷ Although both Gilger and Spanos admitted that this draft reflected their beliefs as of February 11, 2011, their subsequent testimony characterized it as "just a draft."⁵⁴⁸ Gilger stated: "I don't always put everything in there that I ultimately want to have in the report. . . . There were things I was going to add, and there was [sic] probably things I was

⁵⁴² Special Grand Jury Exhibit 89 at CPD016798 (CPD016769-CPD016827) (Draft Case Supplementary Report 323454 (Feb. 11, 2011)).

⁵⁴³ Special Grand Jury Exhibit 89 at CPD016770-CPD016798 (CPD016769-CPD016827) (Draft Case Supplementary Report 323454 (Feb. 11, 2011)).

⁵⁴⁴ Special Grand Jury Exhibit 89 at CPD016798 (CPD016769-CPD016827) (Draft Case Supplementary Report 323454 (Feb. 11, 2011)). The draft narrative concludes with the case being "cleared/closed exceptionally." According to Kobel, the "cleared/closed exceptionally" designation means the offender is still outstanding but no charges will be filed. *See* Kobel, Richard, IGO Interview Rep. at 5 (Jan. 17, 2013).

⁵⁴⁵ Special Grand Jury Exhibit 89 at CPD016770-CPD016798 (CPD016769-CPD016827) (Draft Case Supplementary Report 323454 (Feb. 11, 2011)).

⁵⁴⁶ Special Grand Jury Exhibit 89 at CPD016798 (CPD016769-CPD016827) (Draft Case Supplementary Report 323454 (Feb. 11, 2011)).

⁵⁴⁷ *See* Special Grand Jury Exhibit 15 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

⁵⁴⁸ Gilger, James, Special Grand Jury Tr. at 22:3-4, 89:11-24 (Jan. 23, 2013); Spanos, Nicholas, Special Grand Jury Tr. at 94:24 (Feb. 6, 2013).

going to take out, you know. But at that point when I typed it in, that's what I had so far.”⁵⁴⁹ For example, Gilger testified that although he had not yet included anything about self-defense, he was planning on doing so.⁵⁵⁰

There is evidence suggesting that portions of Gilger’s case supp report concluding the 2011 re-investigation were drafted or edited by his supervisors. Approximately 16 days after Gilger wrote the draft narrative described above, and without any intervening investigative work performed, on Sunday, February 27, 2011, at 9:54 p.m., Sgt. Sam Cirone sent an e-mail with no subject description from his personal e-mail account, “[REDACTED]@aol.com” to Andrews’ personal e-mail account, “[REDACTED]@yahoo.com,” and Salemme at his departmental e-mail account.⁵⁵¹

The entirety of the e-mail’s body was as follows:

CORRECTION #1

On 21 Jan 2011, Det. GILGER spoke with ASA Darren O’Brien at the Cook County courthouse located at 2650 S. California. Det. GILGER informed ASA O’Brien that the R/Ds had re-investigated this incident and informed ASA O’Brien of the current progress of the investigation. ASA O’Brien stated he was consulted by Area 3 Detectives on possible charges, but after the consultation between his office and the police department, it was agreed that charges were not warranted because of self-defense.

CORRECTION #2

In view of the above, and based on the fact that David KOSCHMAN broke away from his group of friends and aggressively went after VANECKO, stating, “Fuck you! I’ll kick your ass!” These aggressive actions caused VANECKO to take action and defend himself and his friends from being attacked. Due to the aforementioned reasons and through the course of this investigation, it is clear that Richard VANECKO, alone, punched David KOSCHMAN, which caused him to fall backwards and injure his head, which ultimately caused his death.

⁵⁴⁹ Gilger, James, Special Grand Jury Tr. at 37:11-19 (Jan. 23, 2013).

⁵⁵⁰ Gilger, James, Special Grand Jury Tr. at 38:8-20 (Jan. 23, 2013).

⁵⁵¹ See Special Grand Jury Exhibit 90 (CPD000391) (Cirone e-mail (Feb. 27, 2011)); Special Grand Jury Exhibit 115 at 13 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)); Cirone, Sam, Kroll Interview Rep. (Proffer) at 11 (Mar. 22, 2013).

Based on this, the R/Ds request this be classified as CLEARED, EXCEPTIONALLY, CLOSED.⁵⁵²

When interviewed pursuant to a proffer agreement in 2013, Cirone explained he sent the e-mail because in order to “exceptionally clear/close” a case, it must be reviewed by a commander and must go “up the food chain.”⁵⁵³ According to Cirone, he typed the e-mail in his office with Gilger present and used his personal e-mail account because “it was probably the account [he] had open.”⁵⁵⁴ With regard to how he received his supervisors’ “corrections” to Gilger’s draft report, Cirone stated during his interview with the OSP that he may have received a “marked on” copy from Andrews or Salemme,⁵⁵⁵ or he may received the edits via e-mail or a phone call.⁵⁵⁶ Cirone could not identify who actually crafted the language contained under “Correction #1” and “Correction #2” in the e-mail.⁵⁵⁷ Because the OSP’s investigation was unable to locate any drafts of Gilger’s report between the February 11, 2011 draft narrative sent by Det. Emiliano Leal and this February 27, 2011, e-mail with “corrections,” sent 16 days later, it is unclear what version Andrews and Salemme may have edited. As stated above, the February 11, 2011 draft lacked any mention of Gilger’s meeting with O’Brien or self-defense — the subject of both “corrections” in the February 27, 2011 e-mail. Thus, the precise extent of

⁵⁵² See Special Grand Jury Exhibit 90 (CPD000391) (Cirone e-mail (Feb. 27, 2011)).

⁵⁵³ Cirone, Sam, Kroll Interview Rep. (Proffer) at 11 (Mar. 22, 2013). When asked during his interview with the OSP why Gilger’s report was being edited late at night on a Sunday, Cirone stated there was no urgency to finish the reports by Monday and he was unaware of any pressure to wrap up the re-investigation prior to Superintendent Weis leaving office. See Cirone, Sam, Kroll Interview Rep. (Proffer) at 11-12 (Mar. 22, 2013).

⁵⁵⁴ See Cirone, Sam, Kroll Interview Rep. (Proffer) at 11 (Mar. 22, 2013).

⁵⁵⁵ See Cirone, Sam, Kroll Interview Rep. (Proffer) at 11 (Mar. 22, 2013). Between February 10, 2011, and February 28, 2011, Gilger printed out his draft case supp report approximately 11 times, although he denied sharing a draft with anyone except Spanos before it was complete. See Gilger, James, Special Grand Jury Tr. at 58:10-59:6, 59:11-60:2 (Jan. 23, 2013).

⁵⁵⁶ See Cirone, Sam, Kroll Interview Rep. (Proffer) at 11 (Mar. 22, 2013). Between 9:55 p.m. and 10:28 p.m., Andrews and Cirone exchanged several text messages and spoke for approximately 11 minutes at 10:02 p.m. AT&T Phone Records for Dean Andrews (Feb. 27, 2011) (ATT005708, ATT005721). Cirone stated he could not recall what Andrews or Salemme said in response to sending this e-mail. See Cirone, Sam, Kroll Interview Rep. (Proffer) at 11 (Mar. 22, 2013).

⁵⁵⁷ See Cirone, Sam, Kroll Interview Rep. (Proffer) at 12 (Mar. 22, 2013).

Andrews' or Salemme's edits are unknown.

When interviewed by the OSP in 2013, Andrews somewhat recalled receiving the February 27, 2011 e-mail, although he was unsure why Cirone sent the e-mail to his personal e-mail address and could not recall receiving any e-mails similar to this.⁵⁵⁸ Andrews stated the e-mail would have been part of the review process for the report (which was submitted and approved the next day).⁵⁵⁹ With regard to the substance of the changes, Andrews believed he "probably asked for some minor changes," including that the narrative should be more specific and should document the exchange between Koschman and Vanecko.⁵⁶⁰ According to Andrews, he did not discuss the final report with Byrne or seek approval from a supervisor to clear/close the case exceptionally.⁵⁶¹

When interviewed by the OSP in 2013, Salemme did not recall the February 27, 2011 e-mail, nor did he know why the corrections were being suggested.⁵⁶² Prior to being shown the e-mail during his interview, Salemme said his editing of the report was limited to minor issues such as spelling and typos.⁵⁶³

About 30 minutes after the e-mail containing "Correction #1" and "Correction #2," at approximately 10:22 p.m., Cirone sent another e-mail, this time only to Andrews, containing the following language:

R/Ds concluded that David KOSCHMAN, having yelled "Fuck you! I'll kick your ass!", by breaking away from his group of

⁵⁵⁸ See Special Grand Jury Exhibit 115 at 13-14 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)).

⁵⁵⁹ See Special Grand Jury Exhibit 115 at 13 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)).

⁵⁶⁰ See Special Grand Jury Exhibit 115 at 13 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)).

⁵⁶¹ See Special Grand Jury Exhibit 115 at 14 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)). During his interview with the OSP in 2013, Salemme further reiterated that Andrews made the final decision to close the re-investigation exceptionally, and that the decision was not run by Byrne. See Special Grand Jury Exhibit 109 at 13 (Salemme, Joseph, Kroll Interview Rep. (Jan. 15, 2013)).

⁵⁶² Special Grand Jury Exhibit 109 at 13 (Salemme, Joseph, Kroll Interview Rep. (Jan. 15, 2013)). With regard to the e-mail addresses listed on the e-mail, Salemme assumed that "[REDACTED]@aol.com" belonged to Cirone, but did not know whose e-mail address "[REDACTED@yahoo.com]" was. See Special Grand Jury Exhibit 109 at 13 (Salemme, Joseph, Kroll Interview Rep. (Jan. 15, 2013)).

⁵⁶³ See Special Grand Jury Exhibit 109 at 6 (Salemme, Joseph, Kroll Interview Rep. (Jan. 15, 2013)).

friends and aggressively going after VANECKO was clearly the assailant in this incident. These aggressive actions caused VANECKO to take action and defend himself. This investigation has shown that Richard VANECKO, alone, punched David KOSCHMAN, which caused him to fall backwards and injure his head, which ultimately caused his death.

Based on this, the R/Ds request this case be classified as CLEARED CLOSED/EXCEPTIONALLY.⁵⁶⁴

The language contained in this e-mail would eventually appear verbatim in Gilger's report.⁵⁶⁵ A few minutes later, Andrews e-mailed in response: "Very nicely done."⁵⁶⁶

5. February 28, 2011

On Monday afternoon, February 28, 2011, Gilger submitted his concluding case supp report for the Koschman re-investigation.⁵⁶⁷ Gilger submitted his case supp reports at the beginning of his shift that day at 3:17 p.m. (Case Supp 8585610) and 3:18 p.m. (Case Supp 8585620).⁵⁶⁸ Four minutes later, Sgt. Thomas Mills approved the report in CHRIS.⁵⁶⁹ Gilger testified that Mills knew nothing about the Koschman re-investigation.⁵⁷⁰ When asked how a sergeant with no familiarity with the re-investigation was able to approve a 36-page report in four minutes, Gilger testified that Salemme probably just directed Mills to approve the report.⁵⁷¹ As Gilger described, "when the commander tells you just to approve the report, you know, [the

⁵⁶⁴ See Cirone E-mail (Feb. 27, 2011) (AOL001831).

⁵⁶⁵ See Special Grand Jury Exhibit 15 at CPD001206-CPD001207 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

⁵⁶⁶ See Andrews E-mail (Feb. 27, 2011) (YAH001496).

⁵⁶⁷ See Special Grand Jury Exhibit 15 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

⁵⁶⁸ Special Grand Jury Exhibit 15 at CPD001199, CPD001208 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

⁵⁶⁹ Special Grand Jury Exhibit 15 at CPD001199, CPD001208 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

⁵⁷⁰ Gilger, James, Special Grand Jury Tr. at 61:15-62:2 (Jan. 23, 2013).

⁵⁷¹ Gilger, James, Special Grand Jury Tr. at 62:7-63:7 (Jan. 23, 2013).

approving sergeant] is doing what he has been instructed to do.”⁵⁷²

The final paragraphs of Gilger’s report summarizes the conclusions of the re-investigation into Koschman’s death:

In conclusion, interviews with eyewitnesses after the incident stated the tallest of the three male subjects punched KOSCHMAN. At the time of the incident, Richard VANECKO was 6’02” and approximately 230 pounds, which is clearly taller and heavier than Craig DENHAM, and clearly heavier than Kevin MCCARTHY. When initially interviewed, Scott ALLEN and James COPELAND stated the male white since identified as (VANECKO) who punched the victim, and the male white since identified as (DENHAM) who was arguing with KOSCHMAN, ran away together. When interviewed, HAGELINE stated the male white who punched KOSCHMAN, was the tallest of the three subjects in their group. The interview with DENHAM, who admitted that he and VANECKO left in a cab together and later said VANECKO was pushing him down the street before entering this cab, confirmed this fact. Interviews were conducted with Bridget and Kevin MCCARTHY⁵⁷³ and Craig DENHAM, who also confirmed the fact that VANECKO and DENHAM left together.

R/Ds concluded that David KOSCHMAN, having yelled, “Fuck you! I’ll kick your ass!” by breaking away from his group of friends and aggressively going after VANECKO was clearly the assailant in this incident. These aggressive actions caused VANECKO to take action and defend himself. This investigation has shown that Richard VANECKO, alone, punched David KOSCHMAN, which caused him to fall backwards and injure his head, which ultimately caused his death.

Based on this, the R/Ds request this case be classified as CLEARED CLOSED/EXCEPTIONALLY.⁵⁷⁴

As previously noted, this conclusion was edited and approved by Gilger’s supervisors, including

⁵⁷² Gilger, James, Special Grand Jury Tr. at 63:14-16 (Jan. 23, 2013).

⁵⁷³ As previously noted, Kevin and Bridget McCarthy did not agree to be re-interviewed during the 2011 reinvestigation. Thus, in coming to their conclusion, Gilger and Spanos relied on the interviews given by the McCarthys in 2004. See, e.g., Gilger, James, Special Grand Jury Tr. at 144:10-147:7 (Jan. 23, 2013).

⁵⁷⁴ Special Grand Jury Exhibit 15 at CPD001206-CPD001207 (CPD001199-CPD001235) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

Cirone and Andrews, the night before. Whereas detectives and SAO in 2004 were unable to determine if Koschman was punched and by whom, the re-investigation concluded Vanecko had punched Koschman, but that Vanecko acted in self-defense.

According to those involved, the decision to identify Vanecko as the offender was made by Gilger and Spanos, and their supervisors supported that decision.⁵⁷⁵ Just as police determined a re-investigation was necessary to connect the dots, CPD personnel in 2011 concluded that Vanecko was the offender through process of elimination or “connecting the dots.”⁵⁷⁶ According to Gilger, in his opinion it was “obvious” that Vanecko was the offender.⁵⁷⁷

Unlike the detectives in 2004, Gilger and Spanos determined that it was a punch that caused Koschman to fall, rather than a push. According to Gilger, “a punch was thrown. . . . that’s my investigation of the case, I feel it was a punch rather than a shove.”⁵⁷⁸ Similarly, Spanos indicated detectives were able to determine a punch was thrown based upon witness interviews and reviewing the case file from 2004.⁵⁷⁹

Ultimately, however, Gilger’s report concluded that Vanecko acted in self-defense. Specifically, Gilger and Spanos concluded that, “David KOSCHMAN, having yelled, ‘Fuck you! I’ll kick your ass!’ by breaking away from his group of friends and aggressively going after VANECKO was clearly the assailant in this incident. These aggressive actions caused

⁵⁷⁵ Cirone, Sam, Kroll Interview Rep. (Proffer) at 9 (Mar. 22, 2013); Special Grand Jury Exhibit 115 at 5, 7 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)).

⁵⁷⁶ Special Grand Jury Exhibit 120 at 10 (Byrne, Thomas, Interview Rep. (Jan. 9, 2013)); Cirone, Sam, Kroll Interview Rep. (Proffer) at 6 (Mar. 22, 2013); Special Grand Jury Exhibit 116 at 4 (Peterson, Steven, IGO Interview Rep. (Feb. 4, 2013)).

⁵⁷⁷ Gilger, James, Special Grand Jury Tr. at 27:4-30:3 (Jan. 23, 2013). According to Gilger and Sgt. Cirone, Vanecko was identified as the offender “for the report” or “for reporting purposes” only. Cirone, Sam, Kroll Interview Rep. (Proffer) at 6, 13 (Mar. 22, 2013); Gilger, James, Special Grand Jury Tr. at 42:10-18 (Jan. 23, 2013). Spanos testified before the special grand jury that “just because we [Gilger and he] identified him [Vanecko] by process of eliminations [sic] through our investigation doesn’t give us [CPD] probable cause to arrest him. . . .” Spanos, Nicholas, Special Grand Jury Tr. at 142:22-143:2 (Feb. 6, 2013).

⁵⁷⁸ Gilger, James, Special Grand Jury Tr. at 32:7-12 (Jan. 23, 2013).

⁵⁷⁹ Spanos, Nicholas, Special Grand Jury Tr. at 89:19-90:3 (Feb. 6, 2013).

VANECKO to take action and defend himself.”⁵⁸⁰ The report’s conclusion that Vanecko acted in self-defense appears to be based on several faulty premises worth noting.

First, Gilger’s report attributed a statement to Koschman in support of the conclusion that Vanecko acted in self-defense. Namely, the report concluded that Koschman yelled “Fuck you! I’ll kick your ass.”⁵⁸¹ Upon review of the rest of that police report, that phrase is nowhere attributed to Koschman or any other witness. Nor is that phrase attributed to Koschman in any of the detectives’ handwritten notes or GPRs from 2011. The closest source appears to be a statement recorded in Yawger’s interview of Kevin McCarthy on May 19, 2004, during which Kevin McCarthy reportedly stated “at this time the primary kid (Koschman) and another kid were still swearing, calling himself, Craig, and Richard names, and saying things like ‘I’ll kick your ass,’ etc.”⁵⁸² Kevin McCarthy admittedly lied to police in 2004 when he told police he did not know anyone involved in the altercation.⁵⁸³

Second, Gilger’s report concluded that “by breaking away from his group of friends and aggressively going after VANECKO [Koschman] was clearly the assailant in this incident.” This conclusion also does not seem supported by other portions of the police reports or the detectives’ own handwritten notes. For example, in Gilger’s handwritten GPRs of his January 17, 2011, interview with Allen, Gilger recorded that Allen informed him that Vanecko’s group “were the aggressors.”⁵⁸⁴ As Gilger acknowledged during his special grand jury testimony, the failure to include this statement was a fairly important omission that was contrary to his ultimate conclusion.⁵⁸⁵ Similarly, Gilger’s report attributes a statement to Copeland that Koschman

⁵⁸⁰ See Special Grand Jury Exhibit 15 at CPD001206 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

⁵⁸¹ See Special Grand Jury Exhibit 15 at CPD001206 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

⁵⁸² See Special Grand Jury Exhibit 10 at CPD001125 (CPD001115-CPD001128) (Case Supplementary Report 3193543 (approved Nov. 10, 2004)); General Progress Report at CPD001102 (May 19, 2004) (CPD001100-CPD001103).

⁵⁸³ McCarthy, Kevin, Special Grand Jury Tr. at 53:5-6 (Aug. 15, 2012).

⁵⁸⁴ See Special Grand Jury Exhibit 77 at CPD001257 (CPD001257-CPD001258) (General Progress Report re: Allen interview (approved Feb. 28, 2011)).

⁵⁸⁵ See Gilger, James, Special Grand Jury Tr. at 83:18-85:3 (Jan. 23, 2013).

“broke free” from his friends prior to being punched that is nowhere to be found in Gilger’s handwritten GPRs.⁵⁸⁶ Rather, Gilger admitted that his conclusion that Koschman ran back and lunged at Vanecko’s group was based “predominantly” on police reports from 2004.⁵⁸⁷

Third, Gilger’s report concluded that Koschman’s actions “caused VANECO to take action and defend himself.” This conclusion that Vanecko acted in defense of himself, or what may have caused any of Vanecko’s actions, does not appear to have any basis in the witness interviews recorded in Gilger’s report. Detectives never spoke with Vanecko or took any kind of statement regarding his involvement in the incident on April 25, 2004. Moreover, Kevin McCarthy, Bridget McCarthy, and Denham all stated they did not see the moments preceding the impact in interviews with Yawger in 2004 and stood by these statements in 2011.⁵⁸⁸ During his special grand jury testimony, Gilger also acknowledged he was “suspicious” of the McCarthys’ and Denham’s claims that they had their backs turned prior to the punch.⁵⁸⁹

Finally, there also appear to be circumstances that detectives either ignored or failed to consider. In evaluating whether Vanecko may have acted in self-defense or in defense of others, Gilger’s report did not reference the height and weight disparity between Vanecko and Koschman. As recorded in Gilger’s report, Vanecko stood 6’3” and weighed 230 pounds in 2004 — compared with Koschman’s height of 5’5” and weight of 125 pounds.⁵⁹⁰ Such a disparity could be relevant to an evaluation of self-defense. Despite the re-investigation’s focus on obtaining “heights and weights,” there is no mention of this disparity in height and weight between the offender and the victim. In fact, detectives may have believed a disparity in size

⁵⁸⁶ See Gilger, James, Special Grand Jury Tr. at 82:2-83:17 (Jan. 23, 2013); Special Grand Jury Exhibit 15 at CPD001231 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)); Special Grand Jury Exhibit 76 (CPD001252-CPD001254) (General Progress Report re: Copeland interview (approved Feb. 28, 2011)).

⁵⁸⁷ See Gilger, James, Special Grand Jury Tr. at 130:19-23 (Jan. 23, 2013).

⁵⁸⁸ See Special Grand Jury Exhibit 10 at CPD001123 (CPD001115-CPD001128) (Case Supplementary Report 3193543 (approved Nov. 10, 2004)); Special Grand Jury Exhibit 15 at CPD001204-CPD001205 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

⁵⁸⁹ See Gilger, James, Special Grand Jury Tr. at 157:6-11 (Jan. 23, 2013).

⁵⁹⁰ See Special Grand Jury Exhibit 15 at CPD001208 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

“does not matter.”⁵⁹¹ As another example, an affirmative defense such as self-defense must be raised by a putative defendant and necessarily negates any issue of lack of identification — i.e., one cannot say they did not strike the victim, but if they did, they acted in self-defense.⁵⁹²

Several other aspects of Gilger’s report call into question its reliability. On page 13 of Case Supplementary Report 8585610, Gilger supplies for the first time an explanation for why no work was performed on the Koschman investigation between April 25, 2004, and May 6, 2004. Following a recitation of Rita O’Leary’s April 25, 2004, telephone interview of Michael Connolly and immediately preceding the pronouncement of Koschman’s death, the report states, “Efforts were being made to interview the additional witnesses that were at the scene of the incident.”⁵⁹³ During his testimony before the special grand jury, Gilger stated, “Well, I’m guessing they were probably going to try to find the phone numbers, or the — or find the addresses. The names and — well, they already had the names, but probably phone numbers or addresses.”⁵⁹⁴ Neither Andrews, Salemme, nor Cirone knew the basis for Gilger’s statement that efforts were being made to interview the additional witnesses that were at the scene of the incident.⁵⁹⁵ The OSP’s investigation has not uncovered any efforts on behalf of anyone at CPD to interview additional witnesses between April 25, 2004, and May 6, 2004.

Additionally, despite drawing very different conclusions from Yawger, detectives in 2011 expressed differing conclusions regarding the thoroughness of CPD’s investigation in 2004. According to Andrews, the 2004 investigation was thorough, as nothing “substantially different”

⁵⁹¹ Cirone, Sam, Kroll Interview Rep. (Proffer) at 12 (Mar. 22, 2013).

⁵⁹² See *People v. Zapata*, 808 N.E.2d 1064, 1069-70 (Ill. App. Ct. 1st Dist. 2004); *People v. Moore*, 797 N.E.2d 217, 225 (Ill. App. Ct. 2d Dist. 2003). Under Illinois law, self-defense is an “affirmative defense under which a defendant admits to the offense but denies responsibility.” *People v. McLennan*, 957 N.E.2d 1241, 1245 (Ill. App. Ct. 2d Dist. 2011). As stated by the court in *People v. Urioste*, 736 N.E.2d 706, 714 (Ill. App. Ct. 5th Dist. 2000), “where a defendant contests guilt based upon self-defense, compulsion, entrapment, necessity, or a plea of insanity, identity ceases to be the issue.”

⁵⁹³ See Special Grand Jury Exhibit 15 at CPD001220 (CPD001199-CPD01234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

⁵⁹⁴ Gilger, James, Special Grand Jury Tr. at 120:22-121:2 (Jan. 23, 2013).

⁵⁹⁵ See Special Grand Jury Exhibit 115 at 11 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)); Special Grand Jury Exhibit 109 at 7 (Salemme, Joseph, Kroll Interview Rep. (Jan. 15, 2013)); Cirone, Sam, Kroll Interview Rep. (Proffer) at 15 (Mar. 22, 2013).

was uncovered in 2011.⁵⁹⁶ Byrne indicated he did not know why the investigation was not closed in 2004, but refused to criticize the 2004 investigation since he was not present when decisions were made.⁵⁹⁷ Even further up the chain of command, Peterson opined that the 2004 investigation by CPD was not a thorough investigation and involved “poor, shoddy detective work.”⁵⁹⁸ Perhaps most tellingly, Gilger testified it was “absurd” to reject charges on the basis of self-defense where one cannot even identify the offender.⁵⁹⁹ As noted previously, despite identifying Vanecko as the person who punched Koschman, detectives in 2011 reached the same conclusion of self-defense as detectives in 2004, without any additional evidence supporting such a conclusion.⁶⁰⁰

The same day that Gilger submitted his final case supplementary report concluding that the case should be cleared/closed exceptionally, Tim Novak, Chris Fusco, and Carol Marin, reporters from the *Sun-Times*, published the first in a series of articles about Koschman’s death entitled “Who Killed David Koschman? A Watchdog’s Investigation.”⁶⁰¹ The front-page article detailed its findings regarding red flags or inconsistencies with the 2004 investigation into Koschman’s death and revealed that CPD had conducted a re-investigation in 2011.⁶⁰² Notable in this article are reports by witnesses Hageline and Copeland that CPD and SAO descriptions in earlier statements by those entities of Koschman as an aggressor in the incident is “not how it

⁵⁹⁶ See Special Grand Jury Exhibit 115 at 11 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)).

⁵⁹⁷ See Special Grand Jury Exhibit 120 at 7 (Byrne, Thomas, Kroll Interview Rep. (Jan. 9, 2013)).

⁵⁹⁸ See Peterson, Steven, IGO Interview Tr. at 50:15-22, 83:18-84:6, 102:2-4, 108:2-3 (Jan. 10, 2012); Peterson, Steven, IGO Interview Rep. at 8 (Feb. 4, 2013).

⁵⁹⁹ See Gilger, James, Special Grand Jury Tr. at 150:22-151:5 (Jan. 16, 2013).

⁶⁰⁰ See Special Grand Jury Exhibit 15 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)).

⁶⁰¹ Special Grand Jury Exhibit 142 (NEWS000022-NEWS000027) (Novak, Fusco, Marin, *Who Killed David Koschman? A Watchdog’s Investigation* (Feb. 28, 2011)).

⁶⁰² Special Grand Jury Exhibit 142 (NEWS000022-NEWS000027) (Novak, Fusco, Marin, *Who Killed David Koschman? A Watchdog’s Investigation* (Feb. 28, 2011)).

happened.”⁶⁰³

The *Sun-Times* on February 28, 2011, also reported that Deputy Police Superintendent Ernest Brown stated that “the investigation into David Koschman’s death was never technically re-opened.”⁶⁰⁴ According to quotes attributed to Brown, the case had only remained open due to an “administrative oversight.”⁶⁰⁵ He is reported as stating that the goal of the re-investigation was to conduct a “comprehensive review of the entire investigative process as it stood.”⁶⁰⁶ He went on to tell the *Sun-Times* that this review “revealed that the facts of that investigation remained unchanged since it was initially investigated.”⁶⁰⁷ Brown told the *Sun-Times* that the case would be “closed shortly.”⁶⁰⁸

6. Case Officially Closed

On March 1, 2011, the *Sun-Times* published two more articles regarding Koschman’s

⁶⁰³ See Special Grand Jury Exhibit 142 at NEWS000027 (NEWS000022-NEWS000027) (Novak, Fusco, Marin, *Who Killed Daivd Koschman? A Watchdog’s Investigation* (Feb. 28, 2011)) (reporting SAO’s press statement that “All witnesses who were questioned indicated that Koschman was the aggressor and had initiated the physical confrontation by charging at members of the other group after they were walking away” and Superintendent Cline’s statement “At the best, it was mutual combatants....If the other person is the aggressor, then Vanecko has the right to defend himself.”)

⁶⁰⁴ Spielman, Fusco, Novak, *Police Brass: No Special Treatment* (Feb. 28, 2011) (NEWS000014-NEWS000015).

⁶⁰⁵ Spielman, Fusco, Novak, *Police Brass: No Special Treatment* (Feb. 28, 2011) (NEWS000014-NEWS000015).

⁶⁰⁶ Spielman, Fusco, Novak, *Police Brass: No Special Treatment* (Feb. 28, 2011) (NEWS000014-NEWS000015).

⁶⁰⁷ Spielman, Fusco, Novak, *Police Brass: No Special Treatment* (Feb. 28, 2011) (NEWS000014-NEWS000015).

⁶⁰⁸ Spielman, Fusco, Novak, *Police Brass: No Special Treatment* (Feb. 28, 2011) (NEWS000014-NEWS000015). As CPD concluded its re-investigation, IGO opened up its own investigation on February 28, 2011, amid the allegations of police misconduct. Specifically, the IGO began to look into allegations that unknown CPD employees obstructed justice and “covered up a homicide investigation involving a nephew of the mayor.” IGO Case Initiation Rep. at IG_007245 (Feb. 28, 2011) (IG_007244-IG_007344). The IGO’s investigation was motivated by the initial article published in the *Sun-Times*, and more specifically, by the report that there were inconsistencies between statements witnesses made to *Sun-Times* reporters versus statements recorded in CPD police reports.

death, including an editorial piece calling for the appointment of a special prosecutor.⁶⁰⁹ The same day, Gilger submitted another report officially closing the Koschman re-investigation in CHRIS.⁶¹⁰ As with Gilger's police report submitted on February 28, 2011, detectives classified the case as "CLEARED CLOSED/EXCEPTIONALLY."

According to CPD policy, "[a]n exceptional clearance is the solving of a criminal offense when the offender was not arrested, was not charged, or was not turned over to the court for prosecution due to unusual circumstances. Detectives must identify the offender, exhaust all investigative leads, and do everything possible to clear a case by arrest before exceptionally clearing the case."⁶¹¹ Detective Division Special Order 96-5 further provides guidance based upon the federal Uniform Crime Reporting handbook concerning when a case can be cleared/closed exceptionally, stating, "Detectives must list in their Supplementary Report the facts that support their decision to exceptionally clear a case. Below are some guidelines for the four questions, which must be answered "yes.""

1. The investigation must identify the offender.

2. The investigation must disclose enough information to support an arrest, charge, and turning over to a court for prosecution.

3. The offender's exact location is known; an arrest could be made now.

4. There is a reason outside of law enforcement control, which

⁶⁰⁹ Novak, Fusco, Marin, *Years After Death Involving Daley's Nephew, Mom's Anguish Won't End* (Mar. 1, 2011) (NEWS000030-NEWS000033); Chicago Sun-Times, *Editorial: Chicago Police Must Get to Bottom of This* (Mar. 1, 2011) (NEWS000028-NEWS000029).

⁶¹⁰ See Special Grand Jury Exhibit 102 (CPD001182-CPD001186) (Case Supplementary Report 8616466 (approved Mar. 1, 2011)). Coinciding with the Koschman investigation being cleared/closed exceptionally was the departure of Superintendent Weis and a transition in CPD administration. Superintendent Weis stepped down as CPD Superintendent on March 1, 2011. According to Peterson and Masters, the period surrounding the submission of Gilger's report was a period of transition. Special Grand Jury Exhibit 116 at 4-5 (Peterson, Steven, IGO Interview Rep. (Feb. 4, 2013); Masters, Michael, IGO Interview Rep. at 9 (May 16, 2013)). The next day, on March 2, 2011, Terry Hilliard took over as interim CPD Superintendent and served in that capacity until the new administration took office.

⁶¹¹ See Special Grand Jury Exhibit 74 at CPD002830-CPD002831 (CPD002822-CPD002842) (CPD Detective Division Special Order 96-5).

prevents an arrest, charge, and prosecution.”⁶¹²

Thus, under Detective Division policy, in order to exceptionally clear/close the Koschman investigation in 2011, detectives needed to identify an offender.⁶¹³ Similarly, the investigation would have had to disclose enough evidence to support an arrest, charge, and turning over of the case to court for prosecution. In light of these requirements, Gilger testified the Koschman investigation was closed in violation of Special Order 96-5 based upon his belief in a lack of sufficient information to support an arrest, charge, and turning over of the case for prosecution.⁶¹⁴

Special Order 96-5 further dictates who must approve exceptional clearances in homicide cases. The order provides that “[i]n murder investigations, if the Felony Review Unit has rejected charges against the offender, the detective will list in the Supplementary Report the reasons for the rejection and the facts which support the arrest of the offender. The detective will request an exceptional clearance for the case. Approval for exceptionally cleared homicide cases is the responsibility of the area commander and the appropriate field group deputy chief.”⁶¹⁵ As Deputy Chief Andrews acknowledged, his role as the only person authorized to approve the exceptional clear/closing of the Koschman investigation.⁶¹⁶ According to Andrews, he did not discuss the fact that the case would be exceptionally cleared/closed with any of his supervisors or

⁶¹² See Special Grand Jury Exhibit 74 at CPD002832-CPD002833 (CPD002822-CPD02842) (CPD Detective Division Special Order 96-5) (emphasis added).

⁶¹³ See Special Grand Jury Exhibit 115 at 6 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)).

⁶¹⁴ See Gilger, James, Special Grand Jury Tr. at 98:20-99:3, 108:19-109:1 (Jan. 23, 2013); see also Sullivan, Karen, Kroll Interview Rep. at 3 (Feb. 5, 2013).

⁶¹⁵ See Special Grand Jury Exhibit 74 at CPD002833-CPD002834 (CPD002822-CPD02842) (CPD Detective Division Special Order 96-5).

⁶¹⁶ See Special Grand Jury Exhibit 115 at 8 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)); see also Cirone, Sam, Kroll Interview Rep. (Proffer) at 13 (Mar. 22, 2013). In light of Andrews’ sole authority to approve the exceptional clear/closing of the Koschman matter, on March 10, 2011, nine days after Gilger officially closed Area 5’s re-investigation, Walsh submitted a memorandum to Andrews attaching police reports concluding the re-investigation for Andrews’ review and approval. See Walsh Memo to Andrews (Mar. 10, 2011) (CPD060760-CPD060770). Walsh’s memorandum stated that “The analysis of the investigation supports the findings. The offender has been identified and it has been determined that the offender was taking actions to defend himself. The case will be Exceptionally Cleared/Closed, Other Exceptional Clearance.” See Walsh Memo to Andrews at CPD060760 (Mar. 10, 2011) (CPD060760-CPD060770).

anyone else in the command staff, including Byrne or Masters.⁶¹⁷

In 2011, despite Superintendent Weis' stated desire to have the case presented to SAO for a charging decision, CPD never officially presented the case for charges or submitted it to SAO's Felony Review unit.⁶¹⁸

⁶¹⁷ See Special Grand Jury Exhibit 115 at 8, 14 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)). Andrews additionally stated that as of January 2013, he had not reported (to the Uniform Crime Reports published by the FBI) the Koschman investigation as a cleared case, and would not do so until the OSP concluded its investigation. Andrews explained, however, that this was significant only for statistical purposes. Special Grand Jury Exhibit 115 at 14-15 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)).

The case was also reclassified from an involuntary manslaughter to second-degree murder. Andrews indicated that as part of the re-investigation, his goals were to determine both whether there was sufficient evidence to name an offender and a correct classification for the case. See Special Grand Jury Exhibit 115 at 5 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)). Since detectives were able to name an offender, all that remained was determining a proper classification. Last active in 2004, the Koschman investigation was left open as an involuntary manslaughter investigation. See Special Grand Jury Exhibit 10 at CPD001128 (CPD001115-CPD001128) (Case Supplementary Report 3193543 (approved Nov. 10, 2004)). In 2011, following some internal debate among Peterson, Byrne, Andrews, and Salemme, the case was reclassified as second-degree murder. See Special Grand Jury Exhibit 15 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)); Special Grand Jury Exhibit 115 at 11 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)); Special Grand Jury Exhibit 120 at 9 (Byrne, Thomas, Kroll Interview Rep. (Jan. 9, 2013)); Special Grand Jury Exhibit 116 at 6 (Peterson, Steven, IGO Interview Rep. (Feb. 4, 2013); Special Grand Jury Exhibit 109 at 10 (Salemme, Joseph, Kroll Interview Rep. (Jan. 15, 2013))). According to Special Order 96-5, it is CPD policy that, "Detectives will not reclassify offenses or incidents unless there is adequate justification; they will document such justification in the Supplementary Report. Detectives will base reclassifications upon facts, not upon unsubstantiated assumptions or opinions." Special Grand Jury Exhibit 74 at CPD002828 (CPD002822-CPD002842) (CPD Detective Division Special Order 96-5). Nevertheless, in practice, it appears reclassification is largely for statistical purposes and specifically in this case was largely "academic." Special Grand Jury Exhibit 109 at 10 (Salemme, Joseph, Kroll Interview Rep. (Jan. 15, 2013)).

⁶¹⁸ Compare Weis, Jody, IGO Interview Tr. at 23:7-15 (Nov. 14, 2011) ("I don't know if, what detective presented it to her but I, I, I recall that the case was presented to the State's Attorney and I don't know if it was Felony Review or whomever and I believe the decision was made that they were not going to charge and then I think Anita may have changed her mind after that but my recollection was that the facts were presented to the State's Attorney, someone there, and the decision was made not to charge, that it was not a crime"); Weis, Jody, IGO Interview Rep. at 1 (May 28, 2013) (Superintendent Weis stated he wanted new detectives from a different detective area to look into the Koschman matter from "A to Z" and get the case to SAO's Felony Review unit for a decision); with Spanos, Nicholas, Special Grand Jury Tr. at 77:9-18 (Feb. 6, 2013); Gilger, James, Special Grand Jury Tr. at 11:23-12:2 (Jan. 23, 2013); Special Grand Jury Exhibit 115 at 12 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)); Special Grand Jury Exhibit 120 at 10 (Byrne, Thomas, Kroll Interview Rep. (Jan. 9, 2013)) ("In 2004 the state's attorney did not charge; it was not presented in 2011"); Kirk, Daniel, IGO Interview Rep. at 5 (Mar. 26, 2013). At the same time, there is some indication that SAO asked CPD "to be looped in" regarding the progress of the

7. The Missing CPD Koschman Homicide File

At CPD, every homicide case is supposed to have a corresponding permanent master homicide case file (“homicide file”). CPD does not have an established policy for how (nor where) homicide files are to be kept; instead, each detective area is left to develop its own protocol and filing system.⁶¹⁹ Homicide files typically contain, often in chronological order, the key CPD documentation (e.g., original GPRs, finalized and approved case supps, etc.)⁶²⁰ that has been created since the inception of the case. While CPD homicide files are not kept under lock and key,⁶²¹ they are typically housed together in an organized fashion at the detective area, and access to them is generally restricted to those detectives (and their superiors) assigned to the particular matter. Detectives consider homicide files to be “sacrosanct,” and therefore, they should not be left out in the open unattended.⁶²²

a. Creating and Maintaining Homicide Files at Area 3

At Area 3, the detective area which handled the 2004 Koschman homicide investigation, the filing methodology for homicide cases has changed slightly throughout the relevant time period (2004-2011).⁶²³ Det. Nicholas Rossi, who has been employed at Area 3 since 1995 and whose primary duties since 2004 include organizing (e.g., indexing) and maintaining the Area’s

re-investigation and was getting police reports as the re-investigation progressed. Special Grand Jury Exhibit 109 at 7-8 (Salemme, Joseph, Kroll Interview Rep. (Jan. 15, 2013)). According to Andrews, SAO received case supplementary reports and was kept up to date on the status of the re-investigation and its progress. Special Grand Jury Exhibit 115 at 12 (Andrews, Dean, Kroll Interview Rep. (Jan. 30, 2013)).

⁶¹⁹ Chasen, Michael, IGO Interview Rep. at 1 (Nov. 27, 2012); Rossi, Nicholas, Kroll Interview Rep. (Proffer) at 3 (Feb. 13, 2013); Molloy, James, Kroll Interview Rep. at 3 (Dec. 7, 2012).

⁶²⁰ Rossi, Nicholas, Kroll Interview Rep. (Proffer) at 4 (Feb. 13, 2013).

⁶²¹ Clemens, Robert, Special Grand Jury Tr. at 26:15-23 (Apr. 24, 2013) (describing how detectives could remove files by checking them out through a log); Day, Edward, IGO Interview Rep. at 2 (Nov. 29, 2012) (describing how cabinets were not locked); Rybicki, Richard, Special Grand Jury Tr. at 28:1-6 (Mar. 27, 2013) (describing how cabinets were rarely locked).

⁶²² See, e.g., Clemens, Robert, Kroll Interview Rep. at 3 (Apr. 10, 2013). Before the special grand jury, Yawger testified that it is “very uncommon” for a homicide file to go missing as happened with the Koschman case and that he had never had a homicide file “go missing.” See Yawger, Ronald, Special Grand Jury Tr. at 160:13-19 (July 15, 2013).

⁶²³ Rossi, Nicholas, Kroll Interview Rep. (Proffer) at 3 (Feb. 13, 2013).

homicide files, explained to the OSP some of the differences he has observed.⁶²⁴ For example, according to Rossi, since at least 2011, Area 3 (now consolidated with other detective areas into Area North) has created and stored homicide files in white three-ring binders.⁶²⁵ Rossi recalled that Area 3 homicide files were historically maintained in blue (and periodically black) folders in which the documents were secured with metal fasteners and clips, as opposed to three-ring binders.⁶²⁶ Others recall blue three-ring binders being used in 2004 as well.⁶²⁷ According to Rossi, the different-colored folders or binders do not signify anything, and were simply the result of CPD purchasing decisions made over the years.⁶²⁸

Furthermore, in 2004, Area 3's homicide files were primarily stored on a bookcase and in file cabinets located in the sergeants' office.⁶²⁹ Generally speaking, homicide files were arranged in chronological order and were labeled by RD # and by the name of the subject whose death was being investigated.⁶³⁰ According to CPD personnel, if Area 3 detectives needed to access a permanent homicide file, they were required to log such use by both "checking out" and "checking in" the homicide file by recording their name on a piece of paper kept in the

⁶²⁴ Rossi, Nicholas, Kroll Interview Rep. (Proffer) at 3 (Feb. 13, 2013).

⁶²⁵ Rossi, Nicholas, Kroll Interview Rep. (Proffer) at 3 (Feb. 13, 2013); *see also* Special Grand Jury Exhibit 148 at 7 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)).

⁶²⁶ Rossi, Nicholas, Kroll Interview Rep. (Proffer) at 3 (Feb. 13, 2013); Sobolewski, Andrew, IGO Interview Tr. at 42-45 (Aug. 5, 2011); Redman, Charles, IGO Interview Rep. (Proffer) at 2-3 (Oct. 31, 2012) (homicide files were not kept in three-ring binders, but were kept in a file with two posts on top). Walsh, Denis, IGO Interview Rep. (Proffer) at 3, 10 (Aug. 14, 2013) (stating that based on his knowledge of how Area 3 homicide files were stored in 2004, none were ever kept in blue three-ring binders, but instead were organized in a flip-folder that had a blue cardboard cover).

⁶²⁷ Rossi, Nicholas, Kroll Interview Rep. (Proffer) at 3 (Feb. 13, 2013); *see also* Skelly, Thomas, Kroll Interview Rep. at 4 (Nov. 15, 2012).

⁶²⁸ Rossi, Nicholas, Kroll Interview Rep. (Proffer) at 3 (Feb. 13, 2013).

⁶²⁹ Skelly, Thomas, Kroll Interview Rep. at 4 (Nov. 15, 2012); Day, Edward, IGO Interview Rep. at 2 (Nov. 29, 2012); Rossi, Nicholas, Kroll Interview Rep. (Proffer) at 2 (Feb. 13, 2013); Rybicki, Richard, Special Grand Jury Tr. at 108:9-17 (Mar. 27, 2013).

⁶³⁰ Rossi, Nicholas, Kroll Interview Rep. (Proffer) at 3 (Feb. 13, 2013).

sergeants' office.⁶³¹ However, adherence to such a procedure does not appear to have been consistent.⁶³² Lastly, homicide files for open cases were to be indefinitely retained in the sergeants' office.⁶³³

b. The Various Versions of the Koschman Homicide File

The subsections below explore issues related to the various versions of the Koschman homicide file that were discovered in, or after, January 2011.

i. Commander Yamashiroya's Credenza File

In response to the January 4, 2011, FOIA request the *Sun-Times* submitted to CPD, Andrews ordered Yamashiroya to gather the Koschman homicide file so it could be provided to those at Area 5 who would be handling the re-investigation. In response, Yamashiroya instructed Walsh to locate Area 3's Koschman homicide file.⁶³⁴ A few days later, Walsh reported to Yamashiroya that he was unable to locate the file.⁶³⁵

In response, Yamashiroya reported to Byrne and Andrews that the Koschman homicide file could not be found.⁶³⁶ According to Yamashiroya, Andrews instructed Yamashiroya to make another effort to find the homicide file.⁶³⁷ Yamashiroya complied and even conducted his own personal search (which according to Yamashiroya, occurred approximately one day after

⁶³¹ Clemens, Robert, Special Grand Jury Tr. at 26:15-23 (Apr. 24, 2013); Day, Edward, IGO Interview Rep. at 2 (Nov. 29, 2012); Sobolewski, Andrew, IGO Interview Rep. at 42:9-20 (Aug. 5, 2011); Molloy, James, Kroll Interview Rep. at 3 (Dec. 7, 2012).

⁶³² Yawger, Ronald, IGO Interview Tr. at 56:21-57:1 (July 1, 2011).

⁶³³ Redman, Charles, IGO Interview Rep. (Proffer) at 2 (Oct. 31, 2012). Closed homicide files were stored permanently at the investigating detective area or at CPD's Records Division. Molloy, James, Kroll Interview Rep. at 3 (Dec. 7, 2012); Special Grand Jury Exhibit 120 at 5 (Byrne, Thomas, Kroll Interview Rep. (Jan. 9, 2013)).

⁶³⁴ Special Grand Jury Exhibit 148 at 3 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)); Walsh, Denis, IGO Interview Rep. (Proffer) at 3 (Aug. 14, 2013) (stating that he (Walsh) enlisted some of his Area 3 colleagues to help him search for the Koschman homicide file).

⁶³⁵ Special Grand Jury Exhibit 148 at 3 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)); see Walsh, Denis, IGO Interview Rep. (Proffer) at 3 (Aug. 14, 2013).

⁶³⁶ Special Grand Jury Exhibit 148 at 3 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)).

⁶³⁷ Special Grand Jury Exhibit 148 at 3 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)).

Walsh informed him he could not locate the Koschman homicide file).⁶³⁸ According to Yamashiroya, during his search, he discovered a manila folder in his office credenza which contained copies of certain CPD reports from the Koschman case.⁶³⁹ However, the file found in Yamashiroya's office credenza was not the original, nor complete, Koschman homicide file; for example, it did not contain original GPRs or an index.⁶⁴⁰

ii. Original Koschman Homicide File (Blue Three-Ring Binder)

Because Yamashiroya and Walsh did not find the original Area 3 Koschman homicide file during their searches in January 2011, Area 5's re-investigation (conducted by detectives Gilger and Spanos) started (on January 13, 2011) and ended (on February 28, 2011) without detectives ever receiving or reviewing the original file.⁶⁴¹

⁶³⁸ Special Grand Jury Exhibit 148 at 3-4 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)).

⁶³⁹ Special Grand Jury Exhibit 148 at 3 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)). Yamashiroya's office previously belonged to Byrne when he was Area 3 Commander. Special Grand Jury Exhibit 148 at 3 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)). According to Yamashiroya, Walsh was present when he found the file in his office credenza. Special Grand Jury Exhibit 148 at 3 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)); Walsh, Denis, IGO Interview Rep. (Proffer) at 8 (Aug. 14, 2013) (stating that he does not recall if he was present when Yamashiroya found the credenza file). Former Area 3 Commander Chasen did not recall having his own personal Koschman file in his office, but presumes he did because it was a "heater case," which required him to keep his superiors apprised. Chasen, Michael, IGO Interview Rep. at 9 (Nov. 27, 2012).

⁶⁴⁰ Special Grand Jury Exhibit 148 at 4 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)); Special Grand Jury Exhibit 109 at 9 (Salemme, Joseph, Kroll Interview Rep. (Jan. 15, 2013)). Furthermore, as part of its investigation, the OSP retrieved and reviewed the file found in Yamashiroya's office credenza and discovered it contained three documents that have not been discovered elsewhere. The first is a CPD CLEAR report run by Yawger (who is identified by his PC Login ID number "PC0N556") on April 25, 2004, at 11:43 a.m. (approximately eight hours after the incident on Division Street) accessing criminal arrest records for Kevin McCarthy. *See* McCarthy, Kevin CLEAR Rep. (Apr. 25, 2004) (CPD001679). The second is the Rita O'Leary draft case supp, which according to Rita O'Leary she typed on April 25, 2004 (the final case supp was not submitted until she returned from furlough on May 20, 2004), with Yawger's handwritten notes. *See* Special Grand Jury Exhibit 14 at CPD001619 (CPD001616-CPD001619) (Draft Case Progress Report 323454 (drafted Apr. 25, 2004)). The third is a document entitled "Koschman Report Summary," which appears to be a rough summary of the investigative steps Area 3 took in 2004 related to the Koschman matter. *See* Koschman Report Summary HK323454 at CPD004594 (CPD004491-CPD004659).

⁶⁴¹ At the time Gilger and Spanos conducted their 2011 re-investigation, they only had the benefit of Yamashiroya's credenza file, as well as any 2004 CPD reports existing in CHRIS. *See* Gilger, James, Special Grand Jury Tr. at 84:12-85:14, 91:3-6 (Jan. 16, 2013).

On June 29, 2011, four months after Gilger and Spanos finished their investigation, Walsh reportedly “found” the original Koschman homicide file.⁶⁴² According to Walsh, he located the original blue binder Koschman homicide file “on a wooden shelf in [Area 3’s] Violent Crimes Sergeants office.”⁶⁴³ The blue binder was reportedly sitting (conspicuously displayed) on a shelf (that had been searched previously) near other Area 3 homicide files which were all housed in white, as opposed to blue, three-ring binders.⁶⁴⁴ During Walsh’s interview

⁶⁴² Walsh, Denis, IGO Interview Rep. (Proffer) at 4 (Aug. 14, 2013); *see also* Internal memorandum from Walsh to Byrne re Koschman File (June 30, 2011) (CPD007132). Yawger testified before the special grand jury that, in 2004, “manila-type expandable” files were used to keep original homicide files and that when he last saw the original homicide file for the Koschman case, it was not in a blue binder. Yawger, Ronald, Special Grand Jury Tr. at 133:20-135:4, 135:23-136:2 (July 15, 2013).

⁶⁴³ Walsh, Denis, IGO Interview Rep. (Proffer) at 4 (Aug. 14, 2013); Internal memorandum from Walsh to Byrne re Koschman File (June 30, 2011) (CPD007132). Besides containing original GPRs, another distinction between the blue binder Walsh reported finding and the other Koschman case files the OSP has discovered during its investigation is that the blue binder contains a table of contents and an investigative file inventory – something to be expected in an original Area 3 homicide file. According to Rossi, he likely created this particular table of contents and inventory. Rossi, Nicholas, Kroll Interview Rep. (Proffer) at 4-6 (Feb. 13, 2013). It should be noted that the documents in the Koschman blue binder homicide file are not in the same order as its table of contents, which indicates that the file may have been rearranged at some point. Walsh told the OSP during his interview that, after he discovered the Koschman blue binder homicide file, he never altered or rearranged it in any way. Walsh, Denis, IGO Interview Rep. (Proffer) at 11 (Aug. 14, 2013). Finally, the blue binder homicide file also contained a single undated GPR that on the front side had Giralamo’s PC Login username and password, as well as the word “Vanecko” and the phone number “908-3121.” On the back side of the GPR the words, “V Dailey Sister Son” are written. Special Grand Jury Exhibit 92 (CPD001052-CPD001053) (General Progress Report for HK323454). According to phone record subscriber information obtained through a special grand jury subpoena, the phone number “312-908-3121” was associated with Northwestern University in 2004; however, according to the subpoena response, the phone number was not attributed to a particular individual. (*See* AT&T Phone Records (ATT003455-ATT003457)). Yawger testified before the special grand jury in 2013 that he authored this GPR and that he “scribbled” the phrase “V Dailey Sister Son” on the back of the GPR on May 13, 2004, when he was told of Vanecko’s involvement during his interview of Bridget McCarthy. Yawger, Ronald, Special Grand Jury Tr. at 73:7-17 (July 15, 2013).

However, the blue binder does not contain the GPRs from Rita O’Leary’s April 25, 2004, witness interviews, nor Yawger’s GPRs from O’Brien’s May 20, 2004, interviews of the McCarthys and Denham.

⁶⁴⁴ Special Grand Jury Exhibit 116 at 3, (Peterson, Steven, IGO Interview Rep. (Feb. 4, 2013)); Peterson, Steven, IGO Interview Rep. at 37 (Jan 10, 2012); *see also* Special Grand Jury Exhibit 146 at 9 (photograph of the wooden bookshelf where the Koschman blue binder homicide file was allegedly found amongst the white binders).

with the OSP, he stated that Area 3 Sgt. Thomas Flaherty⁶⁴⁵ was the only other person in the sergeants' office when he (Walsh) discovered the original blue binder Koschman homicide file.⁶⁴⁶ Flaherty told the OSP that, although he could not recall the exact date,⁶⁴⁷ he was indeed in the sergeants' office when Walsh retrieved a blue binder from the bookshelf which Walsh immediately told him was the missing Koschman homicide file.⁶⁴⁸

According to a June 30, 2011, memorandum authored by Walsh to Byrne,⁶⁴⁹ on June 29,

⁶⁴⁵ Flaherty and Walsh are both former Area 4 violent crimes detectives, and from approximately 1996 through 1998 they were CPD partners. *See* Walsh, Denis, IGO Interview Rep. (Proffer) at 2; 4 (Aug. 14, 2013); Flaherty, Thomas, Kroll Interview Rep. at 1-2 (Aug. 21, 2013).

⁶⁴⁶ Walsh, Denis, IGO Interview Rep. (Proffer) at 3-4 (Aug. 14, 2013).

⁶⁴⁷ Flaherty explained to the OSP that Walsh instructed him to independently record the date and time Walsh found the blue binder on the bookshelf, an instruction Flaherty told the OSP he did not follow. Flaherty, Thomas, Kroll Interview Rep. at 2 (Aug. 21, 2013).

⁶⁴⁸ Flaherty, Thomas, Kroll Interview Rep. at 2 (Aug. 21, 2013). According to CPD records, Flaherty was assigned to Area 3 and working the third watch on June 29, 2011. *See* CPD Attendance & Assignment Record, Det. Div. Area 4 at CPD097424 (CPD097424-CPD097431) (June 29, 2011). Furthermore, the OSP, in an attempt to corroborate or potentially disprove Walsh's and Flaherty's statements made to the OSP surrounding Walsh's finding of the Koschman homicide file on June 29, 2011, sought cell phone records and cell phone tower information via special grand jury subpoenas and court orders. The available responsive records the OSP received and reviewed in response to these efforts did not contradict the statements Walsh or Flaherty made to the OSP when interviewed in 2013. Additionally, according to Flaherty, he was alone in the sergeants' office when he observed Walsh walk into the room and watched him pull a blue binder from the bookshelf. Flaherty, Thomas, Kroll Interview Rep. at 2 (Aug. 21, 2013). Flaherty recalled Walsh exclaiming profanities indicating Walsh's surprise that he had just discovered the missing Koschman homicide file. Flaherty, Thomas, Kroll Interview Rep. at 2 (Aug. 21, 2013). Flaherty stated that Walsh informed him that the binder he had found was the missing file "everyone was looking for". Flaherty, Thomas, Kroll Interview Rep. at 2 (Aug. 21, 2013). Flaherty told the OSP that he (Flaherty) did not examine the binder Walsh had discovered, nor did he ever speak to Walsh again about the blue binder Koschman homicide file. Flaherty, Thomas, Kroll Interview Rep. at 2 (Aug. 21, 2013). Flaherty explained to the OSP that before Walsh discovered the binder, he (Flaherty) knew the Koschman homicide file was missing, but that he was never personally asked to search for it. Flaherty, Thomas, Kroll Interview Rep. at 2 (Aug. 21, 2013). Flaherty further explained that he (Flaherty) never spoke to Yamashiroya about Walsh discovering the blue binder. Flaherty, Thomas, Kroll Interview Rep. at 2 (Aug. 21, 2013).

⁶⁴⁹ According to Yamashiroya, Walsh first reported the discovery of the blue binder Koschman homicide file to him, and then to Byrne. Special Grand Jury Exhibit 148 at 6 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)); *see* Walsh, Denis, IGO Interview Rep. (Proffer) at 5 (Aug. 14, 2013). Yamashiroya stated that Walsh called him at home the night Walsh discovered the missing Koschman homicide file. Yamashiroya, Gary, Kroll Interview Rep. at 1 (Aug. 21, 2013). According to Yamashiroya, he (Yamashiroya) then called Byrne. Yamashiroya, Gary, Kroll Interview Rep. at 2 (Aug. 21, 2013). During his interview with the OSP, Walsh stated that when he first reported the discovery of

2011 at 9:39 p.m., Walsh “while looking for another file . . . located a blue binder/file that contained what is believed to be the original file” for the Koschman homicide investigation.⁶⁵⁰ Walsh’s June 30, 2011 memorandum makes no mention of Flaherty’s presence when he (Walsh) found the blue binder Koschman homicide file on June 29, 2011.⁶⁵¹ During his interview with the OSP, Walsh stated that, in his opinion, there was no reason to memorialize in his June 30, 2011 memorandum the fact that Flaherty was present when the blue binder was discovered.⁶⁵² According to Walsh, he “did not think Tom’s [Flaherty] presence was germane. Tom didn’t find [the missing blue binder]. I found it and Tom was there when I found it.”⁶⁵³ But according to Yamashiroya, had he known someone else besides Walsh was present in the sergeants’ office at

the blue binder to Yamashiroya that he (Walsh) informed him (Yamashiroya) that Flaherty was in the sergeants’ office when he (Walsh) found the blue binder. *See* Walsh, Denis, IGO Interview Rep. (Proffer) at 7 (Aug. 14, 2013). However, according to Yamashiroya, he does not remember Walsh ever telling him that anyone else was present in the sergeants’ office when he (Walsh) discovered the missing Koschman homicide file. (Yamashiroya, Gary, Kroll Interview Rep. at 1-2 (Aug. 21, 2013)). Walsh also told the OSP that he “probably” also informed Byrne and Andrews that Flaherty was present when he (Walsh) found the blue binder. Walsh, Denis, IGO Interview Rep. (Proffer) at 7 (Aug. 14, 2013). Furthermore, according to Walsh, after he discovered the Koschman blue three-ring homicide binder, he asked Byrne to take and maintain the file, but Byrne refused and ordered Walsh to keep it. Walsh, Denis, IGO Interview Rep. (Proffer) at 5 (Aug. 14, 2013). In response, according to Walsh, he then locked the file in a cabinet in his Area 3 office and later took the file home and placed it in his personal safe for some period of time, until William Bazarek (First Assistant General Counsel to CPD) told him that keeping an original homicide file at his home was not a good decision. Walsh, Denis, IGO Interview Rep. (Proffer) at 5 (Aug. 14, 2013). Byrne instructed Walsh to record the discovery of the Koschman homicide file in a memorandum. Special Grand Jury Exhibit 120 at 12 (Byrne, Thomas, Kroll Interview Rep. (Jan. 9, 2013)). According to Yamashiroya, he (Yamashiroya) told Walsh a memorandum should be written to document the finding of the missing Koschman binder. Yamashiroya, Gary, Kroll Interview Rep. at 2 (Aug. 21, 2013). Yamashiroya signed and approved the Walsh to Byrne June 30, 2011 memorandum authored by Walsh. *See* Yamashiroya, Gary, Kroll Interview Rep. at 2 (Aug. 21, 2013); Internal memorandum from Walsh to Byrne re Koschman File (June 30, 2011) (CPD007132).

⁶⁵⁰ Internal memorandum from Walsh to Byrne re Koschman File (June 30, 2011) (CPD007132); Walsh, Denis, IGO Interview Rep. (Proffer) at 4 (Aug. 14, 2013). Witnesses have confirmed that the collective understanding at CPD is that Walsh found the original Koschman homicide file when he discovered the blue binder in June 2011. *See, e.g.*, Peterson, Steven, IGO Interview Tr. at 36-37 (Jan 10, 2012); Cirone, Sam, Kroll Interview Rep. (Proffer) at 15 (Mar. 22, 2013); Special Grand Jury Exhibit 148 at 6 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)).

⁶⁵¹ Internal memorandum from Walsh to Byrne re Koschman File (June 30, 2011) (CPD007132).

⁶⁵² Walsh, Denis, IGO Interview Rep. (Proffer) at 4 (Aug. 14, 2013).

⁶⁵³ Walsh, Denis, IGO Interview Rep. (Proffer) at 6 (Aug. 14, 2013).

the exact moment Walsh found the binder, he (Yamashiroya) “would have [] suggested [that fact] be included” in the Walsh to Byrne June 30, 2011 memorandum.⁶⁵⁴

Former Deputy Superintendent Peterson stated “common sense” dictates that someone had to have placed (after the original search efforts in January 2011⁶⁵⁵ were unsuccessful) the blue binder Koschman homicide file on the shelf (next to all the white binders) knowing it would be found.⁶⁵⁶ When interviewed by the OSP, Walsh stated the blue three-ring binder was “clearly” “put there” by someone to be easily discovered.⁶⁵⁷

Even though, according to Walsh, as soon as he discovered the missing Koschman original homicide file, he knew an internal investigation would be conducted into the incident,⁶⁵⁸ it was not until July 20, 2011, approximately three weeks after Walsh reported finding the blue binder Koschman homicide file, that he initiated, upon a superior’s instruction, a written CPD Internal Affairs Department (“IAD”) complaint.⁶⁵⁹ In the complaint, he stated that he had located what he believed was the original Koschman homicide file in an area that “had been [previously] searched numerous times in an effort to locate said file.”⁶⁶⁰ As Walsh reported, the original Koschman homicide file “believed to have been lost was obviously not lost” and instead had been “removed and returned in violation of department rules and regulations” by an

⁶⁵⁴ See Yamashiroya, Gary, Kroll Interview Rep. at 2 (Aug. 21, 2013).

⁶⁵⁵ Walsh, Denis, IGO Interview Rep. (Proffer) at 4 (Aug. 14, 2013) (stating that he had “given up” looking for the missing Koschman homicide file in January or February 2011).

⁶⁵⁶ Peterson, Steven, IGO Interview Tr. at 61 (Jan 10, 2012).

⁶⁵⁷ Walsh, Denis, IGO Interview Rep. (Proffer) at 4 (Aug. 14, 2013).

⁶⁵⁸ See Walsh, Denis, IGO Interview Rep. (Proffer) at 4 (Aug. 14, 2013).

⁶⁵⁹ Walsh, Denis, IGO Interview Rep. (Proffer) at 5-6 (Aug. 14, 2013); Walsh memorandum re Initiation of CL # 1047119 (July 20, 2011) (CPD005770). During his interview with the OSP, Walsh could not recall which of his superiors ordered him to file the IAD complaint, but Walsh stated it was either Byrne, Andrews, or Yamashiroya. Walsh, Denis, IGO Interview Rep. (Proffer) at 6 (Aug. 14, 2013). According to Yamashiroya, it was Byrne that ordered Walsh to secure a CR # so an internal investigation could be conducted into the missing (now found) Koschman homicide file. Yamashiroya, Gary, Kroll Interview Rep. at 2 (Aug. 21, 2013).

⁶⁶⁰ Walsh memorandum re Initiation of CL # 1047119 (July 20, 2011) (CPD005770).

“Unknown Chicago Police Officer.”⁶⁶¹ Despite what Walsh wrote, during his interview with the OSP, he stated he did not necessarily agree with his superior’s order for him to file an IAD complaint, noting that “on its face is there a real rule violation?”⁶⁶² IAD categorized its investigation as a “misuse of Department records.”⁶⁶³

On August 24, 2011, and in response to Walsh’s complaint, IAD Sgt. Richard Downs interviewed Walsh.⁶⁶⁴ Downs’ interview of Walsh lasted 10 minutes.⁶⁶⁵ It was the only interview IAD conducted in response to Walsh’s complaint. During the interview, Walsh did not disclose that Flaherty was in the sergeants’ office on June 29, 2011, at the moment he (Walsh) discovered the missing Koschman homicide file.⁶⁶⁶ According to Walsh, Downs simply did not ask him during the interview if anyone else was with him (Walsh) when he found the missing Koschman homicide file.⁶⁶⁷ When the OSP asked Walsh why he did not aid Downs’ investigation by informing him (Downs) of Flaherty’s presence (regardless of whether he was asked), Walsh stated that, in his opinion, “you don’t volunteer things” to IAD.⁶⁶⁸ The very next day, Downs submitted his IAD investigative report to his commanding officer for approval.⁶⁶⁹ Downs’ report concluded that “[b]ased on the available evidence gathered in this investigation, and the inability to identify any accused,” the allegation is “Not Sustained.”⁶⁷⁰ IAD conducted no other investigative work on the matter. Its investigation into Walsh’s complaint ended one

⁶⁶¹ Walsh memorandum re Initiation of CL # 1047119 (July 20, 2011) (CPD005770); *see also* Internal Affairs Face Sheet (July 20, 2011) (CPD001791-CPD001792).

⁶⁶² Walsh, Denis, IGO Interview Rep. (Proffer) at 5-6 (Aug. 14, 2013).

⁶⁶³ Internal Affairs Face Sheet at CPD001791 (July 20, 2011) (CPD001791-CPD001792).

⁶⁶⁴ Walsh IAD Interview Tr. at 1797-99 (Aug. 24, 2011) (CPD001784-CPD001810).

⁶⁶⁵ Walsh, Denis, IGO Interview Rep. (Proffer) at 6 (Aug. 14, 2013); Walsh IAD Interview Tr. at 1797-99 (Aug. 24, 2011) (CPD001784-CPD001810).

⁶⁶⁶ Walsh, Denis, IGO Interview Rep. (Proffer) at 6 (Aug. 14, 2013).

⁶⁶⁷ Walsh, Denis, IGO Interview Rep. (Proffer) at 6 (Aug. 14, 2013).

⁶⁶⁸ Walsh, Denis, IGO Interview Rep. (Proffer) at 6 (Aug. 14, 2013).

⁶⁶⁹ Downs memorandum at CPD001800 (Aug. 25, 2011) (CPD001784-CPD001810).

⁶⁷⁰ Summary Rep. Digest CL # 1047119 at CPD001801-CPD001803 (Aug. 25, 2011) (CPD001784-CPD001810).

day after it began.

iii. Det. Yawger's "Working File"

During the course of its investigation, the OSP learned that, besides maintaining one permanent and original homicide file for each Area 3 homicide investigation, Area 3 detectives also typically kept their own personal "working file" for each case they were assigned.⁶⁷¹ The typical "working file" contains copies of reports and GPRs for the detective's use when performing tasks related to an investigation.⁶⁷²

On June 30, 2011 (the day after Walsh "found" the purportedly original Koschman homicide file), Yawger (who retired from CPD in 2007) visited Area 3 and reportedly found his 2004 Koschman "working file."⁶⁷³ According to Yawger, he called Walsh to make arrangements to copy the original Koschman homicide file so he could prepare for his interview with the IGO, which was scheduled to (and did) occur the next day (July 1, 2011).⁶⁷⁴ While Yawger waited to

⁶⁷¹ See, e.g., Chasen, Michael, IGO Interview Rep. at 1-2 (Nov. 27, 2012); Redman, Charles, IGO Interview Rep. (Proffer) at 3 (Oct. 31, 2012).

⁶⁷² See, e.g., Chasen, Michael, IGO Interview Rep. at 1-2 (Nov. 27, 2012); Redman, Charles, IGO Interview Rep. (Proffer) at 3 (Oct. 31, 2012). In theory, according to Rossi, the permanent and original file mirrored the information that was in the working file, and vice versa. Rossi, Nicholas, Kroll Interview Rep. (Proffer) at 3 (Feb. 13, 2013).

⁶⁷³ Furthermore, as discussed above, Nanci Koschman and her attorney (Loretto Kennedy) met with Yawger in July 2004, at Area 3 headquarters to discuss the case. During Kennedy's telephonic interview with the OSP on January 2, 2013, she recalled that Yawger had a manila file folder with him during this meeting that was about an inch and a half thick. Kennedy, Loretto, IGO Interview Rep. at 1 (Jan. 2, 2013). According to Kennedy, neither she nor Mrs. Koschman were permitted to view Yawger's manila file during the meeting, and in fact, when Kennedy requested a copy, Yawger told her that she needed to subpoena the documents or file a FOIA request. Kennedy, Loretto, IGO Interview Rep. at 2 (Jan. 2, 2013).

⁶⁷⁴ Yawger, Ronald, Special Grand Jury Tr. at 98:23-99:2 (July 15, 2013); Yawger, Ronald, IGO Interview Tr. at 54:21-55:2 (July 1, 2011). As previously noted, IGO opened up its own investigation amid the allegations of police misconduct on February 28, 2011, 14 months prior to the appointment of the Special Prosecutor. Furthermore, in a letter dated March 10, 2011, IGO requested from CPD "[c]opies of any and all unredacted documentation" related to the David Koschman investigation, RD# HK-323454. (Grossman letter to Price (Mar. 10, 2011) (CCSAO_014410).) On March 28, 2011, CPD responded via letter, stating the following: "In response to your written request of March 10, 2011 for copies of any and all unredacted documents related to the David Koschman investigation, please find enclosed materials provided to the Office of Legal Affairs by the Record Services Division." (Price letter to Grossman (Mar. 28, 2011) (IG_007571).) CPD's letter to IGO did not mention that the materials

meet with Walsh,⁶⁷⁵ he went into Area 3's detective locker room, where he found his Koschman "working file" in a box labeled with his (Yawger's) name on it.⁶⁷⁶ Walsh submitted a second memorandum to Byrne on June 30, 2011, regarding Yawger's visit to Area 3, which stated in part: "On 30Jun11 at approximately 1420 hours [2:20 p.m.] the R/Lt. [Walsh] met with Retired Detective Ronald Yawger who turned over to the undersigned a file which contained reports relative to the Koschman investigation."⁶⁷⁷

According to Yamashiroya, there were approximately 20 file cabinets in the men's locker room at Area 3 that detectives stored files in (and on top of) in June 2011.⁶⁷⁸ However, it remains unclear why Yawger's "working file" was not discovered in CPD's initial searches in 2011 of Area 3, especially because according to Yamashiroya, the locker room area had

produced to IGO did not include original files, that CPD was aware that the original Koschman homicide file was missing, and/or that CPD personnel had already searched for the original file.

⁶⁷⁵ When Yawger arrived at Area 3, a sergeant informed him that Walsh would be in a meeting for another hour. Yawger, Ronald, Special Grand Jury Tr. at 99:9-14 (July 15, 2013).

⁶⁷⁶ Yawger, Ronald, IGO Interview Rep. at 1 (July 1, 2011); Peterson, Steven, IGO Interview Tr. at 38:21-24 (Jan. 10, 2012). Before the special grand jury, Yawger testified that while employed at Area 3, he used two lockers and "two full drawers of files" in the detectives' locker room. Yawger, Ronald, Special Grand Jury Tr. at 99:16-100:2 (July 15, 2013). When Yawger retired in 2007, he cleaned out the lockers, but not the file drawers. Yawger, Ronald, Special Grand Jury Tr. at 99:20-21 (July 15, 2013). Yawger testified that while in the locker room at Area 3 on June 30, 2011, the file drawers he previously used were occupied by current detectives, but that above those file drawers were two boxes with his name written on them. Yawger, Ronald, Special Grand Jury Tr. at 100:3-7 (July 15, 2013). According to Yawger, he found his working file in one of the two boxes. Yawger, Ronald, Special Grand Jury Tr. at 100:12-16 (July 15, 2013).

According to Yawger, Yamashiroya and Walsh would not permit him to keep his working file, but they did allow him to make copies, which he did. *See* Yawger, Ronald, IGO Interview Tr. at 55:9-11; 60:1-16 (July 1, 2011); *see also* Epach, Thomas, IGO Interview Rep. at 1 (Jan. 31, 2013) (According to Epach, Yawger also sent him copies of certain Koschman CPD reports in 2011); Special Grand Jury Exhibit 149 (police reports Yawger sent to Epach in 2011). Before the special grand jury, Yawger testified that Yamashiroya refused to let Yawger remove his working file from Yamashiroya's office. Yawger, Ronald, Special Grand Jury Tr. at 101:16-18 (July 15, 2013). Yawger testified that he thinks Walsh explained that he could not remove the working file because of an "IAD beef." Yawger, Ronald, Special Grand Jury Tr. at 101:20-102:17 (July 15, 2013). As noted previously, that an IAD complaint with regard to the missing blue binder was first filed on July 20, 2011, nearly three weeks after its discovery. When interviewed by the OSP, Walsh stated he never told Yawger on June 30, 2011, that an IAD investigation was underway. Walsh, Denis, IGO Interview Rep. (Proffer) at 8 (Aug. 14, 2013).

⁶⁷⁷ Walsh memorandum re Yawger file (June 30, 2011) (CPD007131).

⁶⁷⁸ Special Grand Jury Exhibit 148 at 8-9 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)).

previously been searched.⁶⁷⁹ During his interview with the OSP, Yamashiroya stated that it was both “embarrassing” and “shocking” that missing files (both the discovery of the “original” Koschman homicide file as well as Yawger’s “working file”) were turning up with little explanation for their sudden appearance.⁶⁸⁰ During his interview, Walsh told the OSP that he was “surprised” that Yawger gave him a second set of Koschman files only one day after the Koschman blue three-ring binder had been discovered.⁶⁸¹

The OSP obtained phone records indicating Yawger communicated with Walsh (or Area 3) by phone or text message no less than six times from January 2011 through June 2011, including a more than four-minute telephone conversation⁶⁸² with Area 3 (and possibly Walsh himself)⁶⁸³ one day before Walsh reportedly found the missing “original” Koschman homicide file, and two days before Yawger himself “discovered” his Koschman “working file” in Area 3’s locker room.⁶⁸⁴ When the OSP asked Walsh about these phone and text messages between

⁶⁷⁹ Special Grand Jury Exhibit 148 at 8-9 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)). According to Walsh, the locker room at Area 3 had previously been searched, but only for the original Koschman homicide file, not for Yawger’s “working file.” See Walsh, Denis, IGO Interview Rep. (Proffer) at 7 (Aug. 14, 2013).

⁶⁸⁰ Special Grand Jury Exhibit 148 at 8 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)). Yamashiroya also stated it was unusual that Yawger found his file years after his retirement. Special Grand Jury Exhibit 148 at 9 (Yamashiroya, Gary, Kroll Interview Rep. (Feb. 5, 2013)).

⁶⁸¹ Walsh, Denis, IGO Interview Rep. (Proffer) at 7 (Aug. 14, 2013).

⁶⁸² See AT&T Phone Records for Ronald Yawger (June 28, 2011) (ATT003756). Before the special grand jury, Yawger testified that he did not recall speaking with Walsh on June 28, 2011, and had “no idea who I spoke to” that day. Yawger, Ronald, Special Grand Jury Tr. at 96:20-97:13 (July 15, 2013).

⁶⁸³ Yawger, Ronald, Special Grand Jury Tr. at 97:14-98:3 (July 15, 2013).

⁶⁸⁴ Phone records indicate that months earlier, on January 4, 2011, the same day the *Sun-Times* issued a FOIA request to CPD regarding the Koschman case, Yawger called Area 3. See AT&T Phone Records for Ronald Yawger (Jan. 4, 2011) (ATT003683). Then, on January 18, 2011 (a few days after CPD made the decision to re-investigate the Koschman matter), Walsh twice used his Blackberry to call Yawger’s cell phone twice. AT&T Phone Records for Ronald Yawger (Jan. 18, 2011) (ATT003690). Furthermore, a little over a week later, Walsh texted Yawger’s cell phone. AT&T Phone Records for Ronald Yawger (Jan. 26, 2011) (ATT004652). Lastly, on April 20, 2011, five days after IGO sent a written request to CPD for “[a]ny and all original detective interview notes [GPRs] from the David Koschman investigation,” Walsh used his Blackberry to once again call Yawger’s cell phone. AT&T Phone Records for Ronald Yawger (Apr. 20, 2011) (ATT003729); Grossman letter (April 15, 2011) (CCSAO_014412).

Yawger and himself, he could not recall contacting Yawger in 2011, except in January 2011 when, as discussed above, Walsh was instructed by his superiors (shortly after the decision was made by CPD to have Area 5 re-investigate the case) to speak with Yawger regarding his work on the 2004 CPD investigation.⁶⁸⁵

iv. Det. Clemens' Discovery

During the course of its investigation, the OSP learned of yet another version of the Koschman homicide file at Area 3 (which had not been identified or reported previously by CPD, SAO or IGO). Although the OSP has not been able to locate this additional version, Clemens' special grand jury testimony vividly describes a Koschman homicide file he found in 2011 which is different from the "credenza file" Yamashiroya discovered, the "blue three-ring binder" Walsh found, and the "working file" Yawger located.

According to Clemens' testimony before the special grand jury, between late February 2011 and late July 2011,⁶⁸⁶ he found a Koschman homicide file on a table near the photocopier in the detective area at Area 3.⁶⁸⁷ According to Clemens, no other homicide files were on the table where he found the file.⁶⁸⁸ Because personnel at Area 3 frequent the area where Clemens found the Koschman homicide file, he believed that if the file had been on the table for any substantial amount of time, a colleague would have discovered it before he did.⁶⁸⁹

Clemens testified before the special grand jury that the Koschman homicide file he found was contained in a blue hardcover "flip binder" (not a three-ring binder) with what he described

⁶⁸⁵ Walsh, Denis, IGO Interview Rep. (Proffer) at 7 (Aug. 14, 2013).

⁶⁸⁶ According to Clemens' 2013 special grand jury testimony, he likely found the Koschman homicide file at some point between February 28, 2011, when the *Sun-Times* first started publishing articles in 2011 about the Koschman case, but before he read any articles regarding missing files and the Koschman case. Clemens, Robert, Special Grand Jury Tr. 49:10-51:12 (Apr. 24, 2013); see also Clemens, Robert, Kroll Interview Rep. (Proffer) at 11 (Oct. 25, 2012). The *Sun-Times* story "*Who Killed David Koschman? A Watchdog's Investigation*" was first published on February 28, 2011. Special Grand Jury Exhibit 142 (NEWS000022-NEWS000027) (Novak, Fusco, Marin, *Who Killed David Koschman? A Watchdog's Investigation*, *Sun-Times* (Feb. 28, 2011)). The *Sun-Times* first reported missing files related to the Koschman investigation on July 25, 2011. Novak, Fusco, *More Missing Files in David Koschman Case, Cops Still Close It* (July 25, 2011) (NEWS000193).

⁶⁸⁷ Clemens, Robert, Special Grand Jury Tr. at 30:16-20 (Apr. 24, 2013).

⁶⁸⁸ Clemens, Robert, Special Grand Jury Tr. at 49:7-9 (Apr. 24, 2013).

⁶⁸⁹ Clemens, Robert, Special Grand Jury Tr. at 48:7-14 (Apr. 24, 2013).

as a “mailing label” or “Avery label” with the name “Koschman” on it.⁶⁹⁰ Clemens described the dimensions of the spineless folder as 9.5 inches wide, 11-12 inches long, and 2-2.5 inches thick.⁶⁹¹ While Clemens testified that he did not open the binder to review its contents, he noted the documents had two holes in them and were fastened in the flip binder via two metal spindles⁶⁹² (a description other detectives have provided when asked how Area 3 kept permanent homicide files in 2004).⁶⁹³ When shown a color photo of the “original” Koschman homicide file Walsh reportedly found in 2011 (the blue three-ring binder), Clemens testified that the photo depicted something different than the file he found at Area 3 in 2011 (because the Koschman homicide file he found was not a three-ring binder).⁶⁹⁴

According to Clemens, homicide files were not to be left unattended “on the floor” at Area 3.⁶⁹⁵ After finding the Koschman homicide file, he brought it to Walsh.⁶⁹⁶ Clemens testified that he brought the file to Walsh because he was “certainly aware of its importance”⁶⁹⁷ due to the fact that the Koschman case had been the subject of newspaper articles.⁶⁹⁸ Clemens testified that when he gave Walsh the homicide file, he told Walsh, “you don’t want this out on the floor,” to which Walsh responded, “this thing’s got legs.”⁶⁹⁹ Clemens testified he is unsure whether Walsh’s comment was meant to indicate that the Koschman homicide file Clemens had

⁶⁹⁰ Clemens, Robert, Special Grand Jury Tr. at 35:10-38:3, 59:5, 40:12-17 (Apr. 24, 2013).

⁶⁹¹ Clemens, Robert, Special Grand Jury Tr. at 35:10-38:3; 64:14-18 (Apr. 24, 2013).

⁶⁹² Clemens, Robert, Special Grand Jury Tr. at 35:10-38:3, 41:1-5, 58:4-9 (Apr. 24, 2013).

⁶⁹³ See Rossi, Nicholas, Kroll Interview Rep. (Proffer) at 3 (Feb. 13, 2013); Sobolewski, Andrew, IGO Interview Tr. at 44 (Aug. 5, 2011); Redman, Charles, IGO Interview Rep. (Proffer) at 2-3 (Oct. 31, 2012).

⁶⁹⁴ Clemens, Robert, Special Grand Jury Tr. at 60-64 (Apr. 24, 2013).

⁶⁹⁵ Clemens, Robert, Kroll Interview Rep. (Proffer) at 11 (Oct. 25, 2012).

⁶⁹⁶ Clemens, Robert, Special Grand Jury Tr. at 41:7-9 (Apr. 24, 2013).

⁶⁹⁷ Clemens, Robert, Special Grand Jury Tr. at 44:17-22 (Apr. 24, 2013).

⁶⁹⁸ Clemens, Robert, Kroll Interview Rep. (Proffer) at 11 (Oct. 25, 2012).

⁶⁹⁹ Clemens, Robert, Special Grand Jury Tr. at 40:20-22, 42:9-11 (Apr. 24, 2013).

just given him “has legs,” or whether Walsh meant that the entire Koschman case “has legs.”⁷⁰⁰ According to Clemens, Walsh did not express any surprise or shock when he gave him the Koschman homicide file that he had found.⁷⁰¹ When the OSP interviewed Walsh and informed him of Clemens’ grand jury testimony, Walsh stated he had no memory of any of Clemens’ assertions, and further stated he did not recall Clemens ever handing him a Koschman file or any document connected to the Koschman investigation.⁷⁰²

There is no mention of Clemens’ 2011 discovery of the Koschman homicide file in any CPD records. For example, Walsh’s June 2011 internal CPD memoranda regarding the discovery of additional Koschman files do not mention it, nor does Walsh’s July 2011 IAD complaint, nor does IAD’s August 2011 investigative findings report (which included IAD’s interview of Walsh).⁷⁰³

**v. Det. Gilger and Det. Spanos Review the Homicide Files
“Discovered” by Lt. Walsh and Det. Yawger**

On July 20, 2011, the same day that Walsh filed his IAD complaint, he also informed Area 5 detectives Gilger and Spanos (both of whom had conducted the Koschman case re-investigation) of the existence of the Koschman homicide files Yawger and he had discovered approximately three weeks earlier.⁷⁰⁴

Gilger and Spanos, later that same evening (July 20, 2011), and in response to Walsh’s

⁷⁰⁰ Clemens, Robert, Special Grand Jury Tr. at 42-43 (Apr. 24, 2013).

⁷⁰¹ Clemens, Robert, Kroll Interview Rep. (Proffer) at 11 (Oct. 25, 2012). Clemens classified his discovery of the Koschman file as a “non-event.” Clemens, Robert, Special Grand Jury Tr. at 42:21-22 (Apr. 24, 2013). He said he described finding the file as a “non-event” because at the time, he did not know any files related to the Koschman case were missing. Clemens, Robert, Special Grand Jury Tr. at 66:4-19 (Apr. 24, 2013) (testifying that had he read newspaper articles regarding the missing files, and that if he had found the file after reading such articles, it would have been a “significant event” that would have affected to whom he reported his discovery of the file).

⁷⁰² Walsh, Denis, IGO Interview Rep. (Proffer) at 2-3 (Aug. 14, 2013).

⁷⁰³ Clemens was never interviewed by IAD; Clemens, Robert, Special Grand Jury Tr. at 56:16-18 (Apr. 24, 2013).

⁷⁰⁴ Walsh memorandum re Initiation of CL # 1047119 (July 20, 2011) (CPD005770). Special Grand Jury Exhibit 91 at CPD001197-CPD001198 (CPD001187-CPD001198) (Case Supplementary Report HK323454 (approved Sept. 1, 2011)).

notification, went to Area 3's headquarters to review the recently discovered homicide files.⁷⁰⁵ After reviewing the files, Gilger and Spanos determined that neither file changed their conclusions about the case (as had been memorialized in their February 28, 2011 case supp.).⁷⁰⁶ In fact, in a report memorializing their review of the file, Gilger wrote that "none of the new information would have changed the outcome of the investigation," therefore, the Koschman case would remain "CLEARED EXCEPTIONALLY, CLOSED."⁷⁰⁷

D. CPD 2011 Re-investigation and the Mayor's Office

During the course of the OSP's investigation, it discovered evidence demonstrating that the Office of the Mayor ("Mayor's Office") was involved in CPD's response to the *Sun-Times* January 4, 2011 FOIA request, as well as certain CPD press statements regarding the 2011 Koschman case re-investigation. However, there is no evidence gathered by the OSP that demonstrates that then-Mayor Daley directed his staff's actions. Mayor Daley, when interviewed by OSP, stated that he learned about the Koschman incident "sometime" after it occurred, although he was unable to say exactly when.⁷⁰⁸ Mayor Daley also stated that he had

⁷⁰⁵ Special Grand Jury Exhibit 91 at CPD001197-CPD001198 (CPD001187-CPD001198) (Case Supplementary Report HK323454 (approved Sept. 1, 2011)).

⁷⁰⁶ Special Grand Jury Exhibit 15 at CPD001206-CPD001207 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)); Special Grand Jury Ex. 91 at CPD001197-CPD001198 (CPD001187-CPD001198) (Case Supplementary Report HK323454 (approved Sept. 1, 2011)).

⁷⁰⁷ Special Grand Jury Exhibit 91 at CPD001198 (CPD001187-CPD001198) (Case Supplementary Report HK323454 (approved Sept. 1, 2011)) (listing those materials that Gilger and Spanos reported as "discovered" in the blue three-ring binder, as: (1) chronological table of contents; (2) investigative file inventory; (3) crime scene processing reports related to the lineup photos; (4) GPR with Giralamo's PC Login Username and Password, the word "Vanecko" with a phone number and then "V Dailey Sister Son" on the back; (5) copy of Yawger's May 12, 2004 GPR from the Allen interview (with additional legible printing that says "at one point, three guys said fuck it, let's go. Victim says, yeah, you better back down"); (6) morgue photos; *see also* Special Grand Jury Exhibit 151 at 15 (Hehner, Walt, IGO Interview Rep. (Jan. 30, 2013)) (agreeing that the Yawger "working file" did not "shed any light" on the investigation).

⁷⁰⁸ Mayor Daley, Richard M., IGO Interview Rep. at 1 (Apr. 26, 2013). According to Matthew Crowl (Former Mayoral Deputy Chief of Staff for Public Safety), he was informed by someone at CPD of Mayor Daley's nephew's involvement in the incident on Division Street and immediately informed Mayor Daley in person of what he had heard. Crowl, Matthew, IGO Interview Rep. at 2 (April 25, 2013). While Crowl was uncertain of the exact date, he believed he became aware of the Koschman matter shortly after the incident. Crowl, Matthew, IGO Interview Rep. at 2 (Apr. 25, 2013). It was not clear

made it clear to his staff and the public that because he was Vanecko's uncle, he had recused himself from any involvement in the Koschman matter.⁷⁰⁹

On January 4, 2011, an unknown member of CPD's FOIA⁷¹⁰ unit forwarded Novak's January 4, 2011, FOIA request to CPD First Assistant General Counsel Bill Bazarek, CPD General Counsel Debra Kirby, CPD Legal Affairs James McCarthy, CPD Legal Affairs Terrence

whether Mayor Daley was already aware of the incident when Crowl made the disclosure to him. Crowl, Matthew, IGO Interview Rep. at 2 (Apr. 25, 2013). At his interview with the OSP, Mayor Daley did not recall Crowl advising him of the incident. Mayor Daley, Richard M., IGO Interview Rep. at 1 (Apr. 26, 2013).

⁷⁰⁹ Mayor Daley told the OSP he never had substantive discussions with his staff about the law enforcement investigations into Koschman's homicide nor did he ever direct anyone how to handle the matter. The OSP's interviews of his staff confirmed these statements by Mayor Daley. He stated he was not aware of how the *Sun-Times* FOIA request was handled, nor was he aware his staff had any involvement therein. Mayor Daley said that when he was mayor, at any time that he heard news involving his family members, his immediate response, in substance was "no comment, and no interference with City affairs." He further explained, he is "elected with the public's trust" which he stated he would never "jeopardize." He characterized his actions as "recusing" himself from the matter. Mayor Daley, Richard M., IGO Interview Rep. at 1 (Apr. 26, 2013).

Additionally, the OSP interviewed four members of CPD who were assigned to Mayor Daley's security detail in April 2004, including both lower-ranking security specialists and higher-ranking commanders. Each officer interviewed denied having any personal knowledge of the Koschman incident, or of the response to or investigation of the Koschman incident. *See* Weingart, Carol, Kroll Interview Rep. at 4 (Dec. 6, 2012); Roti, Sam, IGO Interview Rep. at 2-3 (Dec. 17, 2012); Thompson, Brian, Kroll Interview Rep. at 5-6 (Feb. 8, 2013); Keating, James, IGO Interview Rep. at 3 (Mar. 11, 2013).

⁷¹⁰ The e-mail "from" line simply said: foia@chicagopolice.org. The function of CPD's FOIA Department is to handle all requests for information, including requests from the media. O'Brien, Rory, Kroll Interview Rep. (Proffer) at 2 (Jan. 15, 2013). Since 2010, the department has accepted FOIA requests through e-mail, which can arrive via links on CPD and city's websites. No matter the source, the e-mail requests are routed to a single inbox that all FOIA officers can access. When requests are received they are printed out, time and date stamped, entered into the department's FOIA log (a database used to track who is working on a request and when a response is sent), and placed in a bin. Individual FOIA officers then pull requests from the bin to process them. An officer typically handles five requests at a time. Sandoval, Matthew, Kroll Interview Rep. (Proffer) at 2-3 (Jan. 11, 2013).

In processing a request, the officer first determines what exactly is being requested, whether a responsive record exists, and whether any records are exempt from release. FOIA officers are also responsible for redacting information as necessary — e.g., any information that would invade someone's privacy or allow a witness to be identified. Sandoval, Matthew, Kroll Interview Rep. (Proffer) at 3 (Jan. 11, 2013); O'Brien, Rory, Kroll Interview Rep. (Proffer) at 5 (Jan. 15, 2013). Redaction decisions are sometimes made by the City Law Department, but it is not the case that they are always approved by the Mayor's Office. *See* O'Brien, Rory, Kroll Interview Rep. (Proffer) at 2, 5 (Jan. 15, 2013). After determining what redactions are needed, the officer prepares a letter summarizing the information being provided, or, alternatively, why the request is being denied. Sandoval, Matthew, Kroll Interview Rep. (Proffer) at 3 (Jan. 11, 2013).

Collins, Commanding Officer Chicago News Affairs Lt. Maureen Biggane, City Law Department attorney Karen Coppa, and City Law Department FOIA Ofc. Jennifer Hoyle.⁷¹¹ On January 11, 2011, Sgt. Melinda Polan e-mailed Bazarek informing him that Ofc. Rory O'Brien would be handling Novak's FOIA request, that the case involved "Vanecko-mayor's nephew," and asking whether Bazarek thought "Chief of Staff or anyone else [should] be notified?"⁷¹²

On January 10, 2011, at 5:02 p.m., Hoyle e-mailed Rosa Escareno and Jodi Kawada (both Deputy Press Secretaries in the Mayor's Office) informing them of the *Sun-Times* FOIA request, as follows:⁷¹³

From: Hoyle, Jennifer
Sent: Monday, January 10, 2011 05:02 PM
To: Escareno, Rosa; Kawada, Jodi
Subject: FOIA issue

Could one of you guys give me a call regarding the following item that was on the agenda for Thursdays' FOIA meeting? The meeting was cancelled so we didn't get a chance to discuss it but I want to give someone a head's up. If you google this guy's name, you'll understand why.

#411: Tim Novak (Sun Times) submitted a request to CPD for all police reports regarding a fight at 35 W. Division at 3:15 am on April 25, 2004 involving David Koschman, 21, who later died of head injuries. The request was submitted on January 4th and the response is due January 11th.

Notes: Novak is interested in one of the bystanders to this fight.

When asked by the OSP, Hoyle stated that she had no concerns about giving the Mayor's Office a "heads up" about a story involving the mayor's nephew, since she wanted them to be

⁷¹¹ E-mail from foia@chicagopolice.org (Jan. 4, 2011) (CPD011991). When requests are submitted by members of the media, the FOIA officers are instructed — pursuant to departmental "practice" — to notify members of specific departments, including CPD News Affairs, City News Affairs, CPD Law, City Law, and the Records Division. Sandoval, Matthew, Kroll Interview Rep. (Proffer) at 4 (Jan. 11, 2013); O'Brien, Rory, Kroll Interview Rep. (Proffer) at 2 (Jan. 15, 2013). At one time, the practice was to notify the different departments only about newsworthy events, but now — and in 2011 — the departments are notified whenever any media request is received. Sandoval, Matthew, Kroll Interview Rep. (Proffer) at 2-4 (Jan. 11, 2013). The FOIA Department maintains an additional list of departments that are notified when a FOIA request is approved, and/or when a draft FOIA response is to be circulated. O'Brien, Rory, Kroll Interview Rep. (Proffer) at 2 (Jan. 15, 2013).

⁷¹² Polan e-mail (Jan. 20, 2011) (CPD000702). According to Bazarek, "Chief of Staff" referred to the Chief of Staff of CPD, who at that time was Mike Masters. Bazarek had no recollection of notifying Masters about the FOIA request. Bazarek, William, Kroll Interview Rep. at 6-7 (Mar. 13, 2013).

⁷¹³ Hoyle e-mail (Jan. 10, 2011) (MAYOR_OFFICE022541).

prepared in case the mayor was asked a question about it.⁷¹⁴ The next morning Escareno e-mailed Hoyle, copying Kawada, asking “who is the bystander??”⁷¹⁵ Kawada thereafter responded to Escareno, copying Hoyle, telling her that “Rosa [I’]ll brief u [sic] on this.”⁷¹⁶

A few minutes later, Hoyle sent Escareno two e-mails: the first attaching the *Chicago Tribune*’s May 22, 2004 article about Vanecko’s presence at the April 25, 2004 incident,⁷¹⁷ and the second stating as follows:⁷¹⁸

From: Hoyle, Jennifer <[REDACTED]@cityofchicago.org>
Sent: Tuesday, January 11, 2011 10:15 AM
To: Escareno, Rosa <[REDACTED]@ex.cityofchicago.org>
Subject: one more thing

Media outlets reported in 2004 that no one would be charged in connection with Dave Koschman’s death. I doubt that Novak realizes he will be getting reports with the witnesses names redacted. I think that he believes that because this case is closed, CPD would not redacted any of the reports and that he would have access to all of the information, including the names of witnesses. That would give the Sun Times the opportunity to write a story with new information.

On January 13, 2011, a discussion of the *Sun-Times* FOIA request took place at the weekly FOIA meeting at the City’s Law Department. Another, more detailed, discussion of the request took place at the January 20, 2011 FOIA meeting. Hoyle recalled that the discussion was more detailed at the second meeting because, by then, the participants were aware of the re-investigation.⁷¹⁹ At the second meeting, it was decided that the *Sun-Times* FOIA request would be denied because the Koschman case was an open investigation.⁷²⁰ The attendees also discussed press strategy, deciding that the official response would be to inform the *Sun-Times* that it would get the requested information “in a little while” if the investigation was to be closed

⁷¹⁴ Hoyle, Jennifer, Kroll Interview Rep. at 3 (Jan. 18, 2013).

⁷¹⁵ Hoyle e-mail (Jan. 10, 2011) (DOIT011671).

⁷¹⁶ Kawada e-mail (Jan. 11, 2011) (DOIT011721).

⁷¹⁷ Hoyle e-mail (Jan. 11, 2011) (MAYOR_OFFICE022542).

⁷¹⁸ Hoyle e-mail (Jan. 11, 2011) (MAYOR_OFFICE022543).

⁷¹⁹ Hoyle, Jennifer, Kroll Interview Rep. at 3 (Jan. 18, 2013).

⁷²⁰ Hoyle, Jennifer, Kroll Interview Rep. at 3 (Jan. 18, 2013).

(which Hoyle believed would occur in a few weeks).⁷²¹

Meanwhile, on January 18, 2011, just five days after Gilger and Spanos were told to reinvestigate the Koschman incident, Biggane sent the following e-mail to members of the Mayor's Office, including Press Secretary Jackie Heard, Kawada, Escareno, and Assistant Press Secretary Lance Lewis:⁷²²

From: Biggane, Maureen C. [mailto: [REDACTED]@chicagopolice.org]
Sent: Tuesday, January 18, 2011 12:19 PM
To: Kawada, Jodi; Lewis, Lance; Escareno, Rosa
Cc: Heard, Jackie
Subject: FOIA Request

FYI: Tim Novak has requested through FOIA reports on an investigation from 2004, where an individual died after late night brawl near downtown bars--- he fell to the pavement and hit his head. Of note: one of the kids involved in the Mayor's nephew (Richard Vanecko). No charges were filed, but the case remains open. His FOIA is being denied based on the status (open investigation), but the case is expected to be closed in the near future.

That same day, Escareno responded to Biggane advising her that "Maureen, we are aware of this request and have been in touch w/Jenny Hoyle on this matter. I believe the names are being redacted from the report."⁷²³

Information about a law enforcement case is not routinely released in response to a FOIA request if the police investigation is "open" or "ongoing," or, if a matter has been indicted and is awaiting trial.⁷²⁴ As discussed above, the Koschman case re-investigation was ordered by Superintendent Weis early in January 2011, and Gilger and Spanos were assigned the matter on or about January 13, 2011. Biggane's January 18, 2011 e-mail was sent five days after the re-investigation began and six weeks prior to its ending; yet its implication is that, though the investigation had just started, CPD knew it would soon end. Further, the e-mail arguably seems to suggest that when the re-investigation ended, the file would be closed, charges would not be returned, and a substantive response to the *Sun-Times* FOIA request would have to be made.⁷²⁵

⁷²¹ Hoyle, Jennifer, Kroll Interview Rep. at 3 (Jan. 18, 2013).

⁷²² Biggane e-mail (Jan. 18, 2011) (CPD030339).

⁷²³ Escareno e-mail (Jan. 18, 2011) (MAYOR_OFFICE000464).

⁷²⁴ See 5 ILCS 140/7(1)(d)(i) and (vii) (West 2011) (exempting from disclosure records that would interfere with an investigation or law enforcement proceeding).

⁷²⁵ Escareno e-mail (Jan. 18, 2011) (MAYOR_OFFICE000464).

When interviewed by the OSP in 2013, Biggane stated she did not remember who told her the Koschman case was “expected to be closed in the near future.”⁷²⁶ Biggane speculated it might have been Chief of Staff Mike Masters or the Chief of Detectives (Byrne).⁷²⁷ In explaining her January 18, 2011 e-mail, Biggane stated that her language should not be read to mean that CPD already knew the conclusion of the Koschman re-investigation.⁷²⁸ Instead, she simply meant that the case would be resolved “one way or the other.”⁷²⁹ Biggane further explained that her use of the phrase in the “near future” meant only that the case was “a priority,” not that it would actually be closed in a matter of days.⁷³⁰ Biggane stated that when she sent this e-mail, she sensed the re-investigation would not take long.⁷³¹ According to Biggane, “everyone recognized it should not have been open all these years.”⁷³²

On February 24, 2011, Biggane e-mailed Andrews a press statement that was to be issued

⁷²⁶ Biggane, Maureen, Kroll Interview Rep. at 5 (Mar. 14, 2013).

⁷²⁷ See Biggane, Maureen, Kroll Interview Rep. at 5 (Mar. 14, 2013).

⁷²⁸ Biggane, Maureen, Kroll Interview Rep. at 6 (Mar. 14, 2013).

⁷²⁹ Biggane, Maureen, Kroll Interview Rep. at 6 (Mar. 14, 2013).

⁷³⁰ Biggane, Maureen, Kroll Interview Rep. at 6 (Mar. 14, 2013).

⁷³¹ Biggane, Maureen, Kroll Interview Rep. at 6 (Mar. 14, 2013).

⁷³² Biggane, Maureen, Kroll Interview Rep. at 6 (Mar. 14, 2013). When the OSP asked Biggane if there was pressure to close the case by a certain date so FOIA materials could be produced, she responded “[t]hat wouldn’t come from my office. I don’t recall being told that.” Biggane, Maureen, Kroll Interview Rep. at 10 (Mar. 14, 2013). In response, the OSP showed Biggane the e-mail in which Escareno references Biggane’s comments that CPD was trying to close the case in consideration of a FOIA deadline, and then the OSP asked Biggane why CPD would want to have a case closed by the FOIA deadline. Biggane, Maureen, Kroll Interview Rep. at 10 (Mar. 14, 2013). Biggane responded that she did not know. Biggane, Maureen, Kroll Interview Rep. at 10 (Mar. 14, 2013).

Additionally, according to Biggane, e-mails like her January 18, 2011, e-mail to Kawada and others (MAYOR_OFFICE000464) were sent to the Mayor’s Office every day. Biggane, Maureen, Kroll Interview Rep. at 4-5 (Mar. 14, 2013). It was the “policy” under Masters to make the Mayor’s Office aware of anything that might lead to questions from the press. Biggane, Maureen, Kroll Interview Rep. at 4-5 (Mar. 14, 2013). It was not unusual for the Mayor’s Office to be involved in FOIA response discussions if the request might result in press attention. Hoyle, Jennifer, Kroll Interview Rep. at 3 (Jan. 18, 2013). In this instance, Biggane did not think it was inappropriate for CPD to be discussing the Koschman reinvestigation with the Mayor’s Office because it was “protocol,” and because she was not giving them “any details.” Biggane, Maureen, Kroll Interview Rep. at 7 (Mar. 14, 2013).

by CPD to the *Sun-Times* relating to the January 4, 2011 FOIA request. In the first line of her e-mail, Biggane advises Andrews that “Below is the final statement as edited and approved by the Mayor’s [sic] Press office. . . .”⁷³³

On March 2, 2011, Escareno contacted Biggane, asking her to call her about CPD’s FOIA response (to Novak’s January 4, 2011 FOIA request) slated to go out later that day.⁷³⁴ As Escareno put it: “This cannot go out until Law and our office [Mayor’s Office] has reviewed.”⁷³⁵ Biggane explained that CPD had to turn over the reports immediately.⁷³⁶ Escareno responded:⁷³⁷

Escarreno, Rosa

From: Escareno, Rosa
Sent: Wednesday, March 02, 2011 3:19 PM
To: Biggane, Maureen C.; Heard, Jackie
Cc: Hoyle, Jennifer; Kawada, Jodi
Subject: RE: CPD FOIA

Importance: High

Maureen,
When we spoke about this case last week, you mentioned a FOIA was due on Friday, which was the reason you indicated CPD was trying to have the case would close by that day. However, I was not aware that either the same or a different FOIA was also being considered this week for the same case. We need to review the information before it is turned over. Please send a copy ASAP:
BTW,
-- Who's requesting the FOIA
-- What's specifically being requested
-- When was it submitted and when is it due

⁷³³ Andrews e-mail (Feb. 24, 2011) (CPD000405). Andrews responded by asking Biggane to call him. Andrews e-mail (Feb. 24, 2011) (CPD000405). About an hour and a half later, Biggane sent, without comment, a revised version of the statement. Biggane e-mail (Feb. 24, 2011) (CPD000403).

⁷³⁴ Escareno e-mail (Mar. 2, 2011) (MAYOR_OFFICE022624).

⁷³⁵ Escareno e-mail (Mar. 2, 2011) (MAYOR_OFFICE022624).

⁷³⁶ Escareno e-mail (Mar. 2, 2011) (MAYOR_OFFICE022624).

⁷³⁷ Escareno e-mail (Mar. 2, 2011) (MAYOR_OFFICE022626).

Biggane then responded:⁷³⁸

From: Biggane, Maureen C. [mailto:[REDACTED]@chicagopolice.org]
Sent: Wednesday, March 02, 2011 03:34 PM
To: Escareno, Rosa
Subject: Re: NOVAK FOIA

Rosa-

The original FOIA was denied, because the case was still opened. We wanted to get the case closed so they could get the FOIA request fulfilled. However, they appealed the denial, and we have been told by PAC to turn it over. The requester is Tim Novak at the ST. The case was closed as of last night.

On March 3, 2011, Biggane sent an e-mail to Escareno informing her that “The Vanecko thing has been pressing. Just FYI--we are meeting with the State’s [Attorney’s] office on this later today.”⁷³⁹ Later that evening, following the meeting at SAO, Biggane sent another e-mail to Escareno, Kawada, Hoyle, and Heard explaining that “We and CCSAO remain in concurrence. Therefore, the file is to be released tomorrow.”⁷⁴⁰

On March 4, 2011, the *Sun-Times* received certain CPD reports (that had been created through that date) related to the Koschman matter (both from the 2004 investigation and the 2011 re-investigation)⁷⁴¹ in response to Novak’s January 4, 2011 FOIA.⁷⁴²

⁷³⁸ Biggane e-mail (Mar. 2, 2011) (CPD009233).

⁷³⁹ Biggane e-mail (Mar. 3, 2011) (MAYOR_OFFICE022632).

⁷⁴⁰ Biggane e-mail (Mar. 3, 2011) (MAYOR_OFFICE022637).

⁷⁴¹ The OSP has found no indication that, in producing these materials to the *Sun-Times*, CPD disclosed that it was not the original investigative file, that CPD was aware that the original Koschman file was missing, and/or that CPD personnel had already searched for the original file.

⁷⁴² Rory O’Brien had previously, on January 18, 2011, sent Novak correspondence stating that, in response to his January 4, 2011 FOIA request, CPD would be producing *only* the redacted General Offense Case Report. O’Brien correspondence (Jan. 18, 2011) (CPD004835). The response would omit “crime scene details, witness and suspect names and statements [that] would interfere with the Department’s ongoing criminal investigation . . . [and] [t]he names, home addresses and telephone numbers, and other identifying information that is unique to the witnesses and any suspect involved in this incident . . .” O’Brien correspondence (Jan. 18, 2011) (CPD004835). The decision by CPD to limit the FOIA response to the General Offense Case Report was appealed by the *Sun-Times* pursuant to the procedures set forth in the Illinois FOIA statute. Ultimately, the decision by CPD to *only* provide the *Sun-Times* the General Offense Case Report was overruled by an Illinois Attorney General Public Access Counselor, and thus, CPD was instructed to provide the *Sun-Times* all reports regarding the Koschman matter. See Biggane e-mail to T. Novak (Mar. 4, 2011) (CPD038485-CPD038487).

E. SAO's Involvement in 2011 and 2012

1. Press Inquiries

Just as *Sun-Times* reporters were pursuing records from CPD, they similarly issued several FOIA requests to SAO seeking records related to the Koschman case. On January 24, 2011, Novak submitted a FOIA request to SAO seeking to “inspect the state’s attorney’s records and files regarding the death of David Koschman . . .”⁷⁴³ Paul Castiglione, SAO’s Executive Assistant State’s Attorney for Policy in 2011, responded to Novak’s request the next day, January 25, 2011, stating “[h]aving searched the State’s Attorney’s files and records, we have no documents that are responsive to your request.”⁷⁴⁴

According to State’s Attorney Alvarez’s Chief of Staff, Dan Kirk, the *Sun-Times* FOIA request prompted SAO to determine who at SAO would be most knowledgeable about the Koschman case.⁷⁴⁵ During his interview with the OSP, Kirk recalled attending a meeting less than one week after the FOIA request where he was briefed on the case and the media’s interest.⁷⁴⁶ State’s Attorney Alvarez explained that between January 24, 2011 (the day the FOIA request was made to SAO), and February 23, 2011 (the day SAO issued a press statement), her staff, including Valentini and Sally Daly (SAO’s Director of Communications), and she were trying to gather all the facts.⁷⁴⁷ She stated that SAO requested the investigative file from CPD

⁷⁴³ Novak FOIA request (Jan. 24, 2011) (CCSAO_024527).

⁷⁴⁴ Castiglione letter to Novak (Jan. 25, 2011) (CCSAO_024528). Following the initial FOIA request in January 2011, on March 16, 2011, the *Sun-Times* issued another FOIA request that asked for specific files related to the Koschman matter, including, among other things, felony review logs, correspondence, or memoranda between State’s Attorney Devine, Milan, State’s Attorney Alvarez, and O’Brien, minutes and records regarding SAO staff meetings about the Koschman case, and telephone records for State’s Attorney Devine, Milan, State’s Attorney Alvarez, and O’Brien for the time period of April 25, 2004 to May 31, 2004. Novak e-mail (Mar. 16, 2011) (CCSAO_024529). On March 29, 2011, SAO denied these requests, in part, on the grounds that production of felony review logs would be unduly burdensome and, in part, on the grounds that no responsive documents were found. Castiglione letter at CCSAO_024532 (Mar. 29, 2011) (CCSAO_024531-024532).

⁷⁴⁵ Kirk, Daniel, IGO Interview Rep. at 3 (Mar. 26, 2013).

⁷⁴⁶ Kirk, Daniel, IGO Interview Rep. at 3 (Mar. 26, 2013).

⁷⁴⁷ Alvarez, Anita, IGO Interview Rep. at 2 (Apr. 29, 2013).

and O'Brien was spoken to, but not by her.⁷⁴⁸ Walt Hehner, Chief Deputy State's Attorney in 2011, attended an O'Brien "de-brief" meeting along with Sally Daly, Kirk, and Boliker in February 2011.⁷⁴⁹ At the time, O'Brien still served as an ASA but was no longer head of the Felony Review unit.⁷⁵⁰

According to Kirk, O'Brien told those present at the meeting that, in 2004, he was called to Area 3 by someone at CPD either directly or through the Felony Review unit dispatcher.⁷⁵¹ Kirk recalled that O'Brien described interviewing witnesses but that he did not formally review the case.⁷⁵² Kirk further recalled that when asked the location of the Felony Review folder, O'Brien stated he did not know if he made one or not and, if he did make one, where it would be.⁷⁵³ At the end of the meeting, Hehner directed O'Brien to scour all of the files, and

⁷⁴⁸ Alvarez, Anita, IGO Interview Rep. at 2 (Apr. 29, 2013).

⁷⁴⁹ Special Grand Jury Exhibit 151 at 6 (Hehner, Walter, IGO Interview Rep. (Mar. 11, 2013)). Kirk recalled that he attended this meeting along with State's Attorney Alvarez, Sally Daly, and "probably Hehner." Kirk, Daniel, IGO Interview Rep. at 4 (Mar. 26, 2013).

⁷⁵⁰ After leaving the Felony Review unit in 2008, O'Brien had a six-month stint as the head of Branch 66 (supervising grand jury proceedings related to homicide and sex crimes) and then became chief of the municipal court division overseeing suburban courts. *See* O'Brien, Darren, IGO Interview Rep. at 2 (Feb. 5, 2013).

⁷⁵¹ Kirk, Daniel, IGO Interview Rep. at 4 (Mar. 26, 2013). Before the special grand jury in 2013, as part of his testimony, O'Brien read a statement which, in part, stated, "[m]y best recollection was that there were two telephone calls. Both calls may have occurred the day of the lineups on May 20, 2004, or one call occurred the day before the lineups and the other call occurred the day of the lineups. I'm not sure if I was paged by the caller directly or received a call through the Felony Review dispatcher." O'Brien, Darren, Special Grand Jury Tr. at 30 (May 8, 2013).

⁷⁵² Kirk, Daniel, IGO Interview Rep. at 4 (Mar. 26, 2013); *see also* Special Grand Jury Exhibit 151 at 6 (Hehner, Walter, IGO Interview Rep. (Mar. 11, 2013)) (According to Hehner, O'Brien stated that the detective was looking for legal advice, and that there was no criminal charge requested to be approved or rejected).

⁷⁵³ Kirk, Daniel, IGO Interview Rep. at 4 (Mar. 26, 2013); Special Grand Jury Exhibit 151 at 6 (Hehner, Walter, IGO Interview Rep. (Mar. 11, 2013)) (recalling O'Brien could not remember if he "did a file or not"). Before the special grand jury in 2013, as part of his testimony, O'Brien read a statement which, in part, stated, "I'm sure I had a Felony Review folder with me when I went out to Area 3 for the Koschman case, and that I started one by writing down the known case information before I interviewed the witnesses. A majority of the folder would have been left blank because the information necessary to complete it did not exist. I probably brought the folder back to the Felony Review office after my interviews to await further contact from CPD regarding any new developments in the case. Due to the number of witnesses I interviewed for the Koschman matter on May 20, 2004, it was possible I used four

warehouses, for the Felony Review folder, and to find the file.⁷⁵⁴ Valentini was also directed to perform an exhaustive search to find the folder.⁷⁵⁵

On February 21, 2011, Novak sent an e-mail to Sally Daly stating, “[w]e’re revisiting this case as is the police department. We would like to sit down and discuss the facts of the case as we understand them with State’s Attorney Alvarez and Darren O’Brien.”⁷⁵⁶ During an interview with the OSP, O’Brien recalled that SAO “powers that be” told O’Brien to do a telephonic interview with the *Sun-Times* — an interview which subsequently occurred on March 3, 2011.⁷⁵⁷

In a statement issued by SAO to the *Sun-Times* on February 23, 2011, apparently based upon what O’Brien told his superiors, SAO stated, “all witnesses who were questioned indicated that Koschman was the aggressor and had initiated the physical confrontation by charging at members of the other group after they were walking away.”⁷⁵⁸ The statement further provided that, “[a]s for the current status of the case, the Cook County State’s Attorney’s Office has not received any information or had any inquiries from the Chicago Police Department or any of the witnesses in connection with this case in the nearly seven years that have elapsed since the

or five Felony Review folders because each folder only had room for biographical information for two witnesses.” O’Brien, Darren, Special Grand Jury Tr. at 32-33 (May 8, 2013).

⁷⁵⁴ Special Grand Jury Exhibit 151 at 6 (Hehner, Walter, IGO Interview Rep. (Mar. 11, 2013)).

⁷⁵⁵ Special Grand Jury Exhibit 151 at 6 (Hehner, Walter, IGO Interview Rep. (Mar. 11, 2013)); Kirk, Daniel, IGO Interview Rep. at 5 (Mar. 26, 2013).

⁷⁵⁶ Novak e-mail to Sally Daly at CCSAO_028227 (Feb. 21, 2011) (CCSAO_028226-CCSAO_028228). Although the exact timing is unclear, Novak followed up his FOIA request with several phone calls. See Daly, Sally, IGO Interview Rep. at 2 (Mar. 28, 2013). Sally Daly subsequently forwarded Novak’s e-mail to Fabio Valentini, SAO’s Chief of the Criminal Prosecutions Bureau in 2011, approximately two hours later, among other things, wondering how reporters obtained O’Brien’s name. Novak e-mail to Sally Daly (Feb. 21, 2011) (CCSAO_028226-CCSAO_028227). Valentini sent an e-mail to Sally Daly in response which, in part, states, “I would bet that they got Darren’s name from the police reports. The reports lay out that we were contacted, we interviewed available witnesses, and gave the advice that the police sought.” Valentini e-mail to Sally Daly (Feb. 21, 2011) (CCSAO_028226). Based upon these e-mails, as of February 21, 2011, at least certain members of State’s Attorney Alvarez’s staff had reviewed police reports from 2004.

⁷⁵⁷ O’Brien, Darren, IGO Interview Rep. (Proffer) at 14 (Feb. 20, 2013).

⁷⁵⁸ Alvarez e-mail to Sally Daly, Boliker, Hehner, and Kirk (Feb. 23, 2011) (CCSAO_028208); Special Grand Jury Exhibit 142 at NEWS000027 (NEWS000022-NEWS000027) (Novak, Fusco, Marin, *Who Killed David Koschman? A Watchdog’s Investigation, Sun-Times* (Feb. 28, 2011)).

incident.”⁷⁵⁹ However, it appears that at least some SAO supervisors knew of the re-investigation shortly after it began in January 2011.⁷⁶⁰

On March 3, 2011, *Sun-Times* reporters Novak, Fusco, and Marin published an article in the series regarding Koschman entitled, “*Witness in Daley Nephew Case Says Koschman Wasn’t the Aggressor.*”⁷⁶¹ The article quoted Connolly as stating, “The state’s attorney said all the witnesses involved said that David was the aggressor. That was a flat-out lie,” and “[w]hat I saw was David definitely being mouthy....I did not see David attempting to attack the other person. He was definitely moving toward the taller guy but not in an aggressive fashion. From what I recall, he was probably moving in to say something else.”⁷⁶² The article also quoted O’Brien’s

⁷⁵⁹ Alvarez e-mail to Sally Daly, Boliker, Hehner, and Kirk (Feb. 23, 2011) (CCSAO_028208). In an e-mail providing the statement to the *Sun-Times* on February 23, 2011, Sally Daly indicated that SAO was declining the *Sun-Times*’ request for an on-camera interview of State’s Attorney Alvarez. Sally Daly explained that while SAO had not been informed by CPD “in any official capacity,” that they had reopened the case, SAO was “not comfortable granting an interview if CPD considers the case open --- with potential new facts or information out there that we are unaware of at this point.” Sally Daly’s e-mail further noted that, “it appears that since the death of Mr. Koschman in 2004, his family has never attempted to contact the CCSAO with any concerns or questions about the case. Nor have any of the witnesses called or reached out to indicate any new facts or different accounts of the events of that evening. Until your inquiry — nearly seven years later — the case has been entirely dormant from our perspective.” Her e-mail further stated, “I realize your level of intrigue is piqued by the fact that we cannot currently locate any paperwork on the case, but we are continuing to search the files in our warehouse to see if anything is available. Regardless, the State’s Attorney’s involvement in this case is memorialized in CPD reports and is consistent with the version of facts and the recollection of the Assistant State’s Attorney who provided the advice to CPD in 2004.” Sally Daly e-mail to Novak (Feb. 23, 2011) (CCSAO_033625-CCSAO_033626).

⁷⁶⁰ Before the special grand jury in 2013, O’Brien testified that he learned about the existence of CPD’s re-investigation when he spoke with Gilger on January 21, 2011. O’Brien, Darren, Special Grand Jury Tr. at 57:7-9 (May 8, 2013). As noted previously, Gilger’s case supp report records their meeting as occurring on January 21, 2011, or roughly one month prior to SAO’s press statement that it had not received any information from CPD. Special Grand Jury Exhibit 15 at CPD001204 (CPD001199-CPD001234) (Case Supplementary Reports 8585610 and 8585620 (approved Feb. 28, 2011)). The “very first thing” Gilger did as part of his re-investigation in January 2011 was visit the head of SAO’s Felony Review unit to inquire about the Felony Review folder for the Koschman case. Gilger, James, Special Grand Jury Tr. at 106:22-107:2, 107:19-107:22 (Jan. 16, 2013).

⁷⁶¹ Tim Novak, et al., *Witness in Daley Nephew Case Says Koschman Wasn’t the Aggressor* (Mar. 3, 2011) (NEWS000036-NEWS000037).

⁷⁶² Tim Novak, et al., *Witness in Daley Nephew Case Says Koschman Wasn’t the Aggressor* at NEWS000036 (Mar. 3, 2011) (NEWS000036-NEWS000037).

statements defending his handling of the matter in 2004 from the interview given to *Sun-Times* reporters via a conference call earlier that day.⁷⁶³

2. March 3, 2011 Meeting with CPD

On the afternoon of March 3, 2011, Denise Perri, CPD Chief of Staff Masters' administrative assistant, sent a calendar invite to Masters, Biggane, Peterson, Byrne, Marya Vidricko (an SAO administrative assistant), and Kirk for a meeting at SAO's offices at 69 West Washington.⁷⁶⁴ The meeting was scheduled for 5 p.m. in the main conference room at SAO. Although State's Attorney Alvarez stopped by the meeting to greet those present, she did not attend.⁷⁶⁵ Peterson, Byrne, Masters, and Biggane attended from CPD, while Kirk and Sally Daly attended from SAO. The subject line for the calendar invite was “[sic] Vaneko.”

According to Sally Daly, the meeting lasted only 15-20 minutes and the purpose was for CPD personnel to bring SAO “the Koschman file.”⁷⁶⁶ During his interview with the OSP, Kirk stated that CPD brought with them recent case supp reports and informed SAO that it intended to release these police reports in response to FOIA requests that CPD had received.⁷⁶⁷

⁷⁶³ O'Brien is quoted in the newspaper article as saying, “‘This was a case that had three major problems, in my opinion, before I could even think about pulling the trigger on charging anybody....There was contrary information given about the contact that was made between somebody in Vanecko’s group and Koschman. Some people said it was a shove. Some people said it was a punch. . . . I couldn’t find anybody that could identify the shover or pusher.’ Koschman’s friends ‘told me that Koschman — even though he was a little guy — when he was drinking, he was an aggressive type of personality...And, in this particular case, he was the aggressor. He would not let it go....If the case was there, and we could have charged it, we would’ve charged it, no matter who it is.’” Tim Novak, et al., *Witness in Daley Nephew Case Says Koschman Wasn’t the Aggressor* at NEWS000037 (Mar. 3, 2011) (NEWS000036-NEWS000037). However, O’Brien admitted under oath that none of the witnesses told him that Koschman took a swing at Vanecko or “something like that.” O’Brien, Darren, Special Grand Jury Tr. at 115:8-18 (May 8, 2013). According to O’Brien, “none of the witnesses told me Koschman threw punches or made physical contact with Vanecko immediately before Koschman was struck.” O’Brien, Darren, Special Grand Jury Tr. at 40:6-9 (May 8, 2013).

⁷⁶⁴ Perri e-mail (Mar. 3, 2011) (CPD037531).

⁷⁶⁵ Daly, Sally, IGO Interview Rep. at 2-3 (Mar. 28, 2013); Alvarez, Anita, IGO Interview Rep. at 3 (Apr. 29, 2013).

⁷⁶⁶ Daly, Sally, IGO Interview Rep. at 2-3 (Mar. 28, 2013).

⁷⁶⁷ Kirk, Daniel, IGO Interview Rep. at 6 (Mar. 26, 2013). As noted earlier, Biggane advised the Mayor’s Office of this meeting and SAO’s concurrence to produce records in response to the *Sun-Times* FOIA request.

3. State's Attorney Alvarez Calls for an Independent Investigation

On March 19, 2011, State's Attorney Alvarez issued a statement dismissing the need for a new investigation into the Koschman death,⁷⁶⁸ but reversed her position five days later. On March 24, 2011, *Sun-Times* reporters Marin and Novak interviewed State's Attorney Alvarez on camera regarding the Koschman case.⁷⁶⁹ During the interview, reporters raised the fact that some witnesses denied statements attributed to them in police reports and that one witness claimed he identified Vanecko in a lineup on May 20, 2004.⁷⁷⁰ According to State's Attorney Alvarez, based on these new allegations, she indicated she would be open to an independent investigation.⁷⁷¹

Also on March 24, 2011, the *Sun-Times* published an article with excerpts from the interview with State's Attorney Alvarez.⁷⁷² During the interview, State's Attorney Alvarez stated, "I think there should be an independent police investigation." State's Attorney Alvarez suggested she would welcome review by an independent agency such as the Illinois State Police ("ISP"); although she indicated that she did not "believe we have a good faith and legal basis to bring charges." State's Attorney Alvarez further explained during the interview, "Before we take something to the grand jury, we have to have a good-faith basis that a crime occurred and that the person we are seeking a true bill of indictment for did it." With regard to using a grand

⁷⁶⁸ On March 19, 2011, in a *Sun-Times* article entitled, "Alvarez: Not Enough Evidence to Charge Daley Nephew," SAO issued a statement which, in part, read, "The contradictory statements made by witnesses seven years after the actual incident do not allow us to discount the statements that those same witnesses made to Chicago police detectives during the course of the initial investigation and within weeks of the incident. At this time, we are unaware of any new evidence that would enable us to bring charges, and therefore we could not bring the case to a grand jury." See Novak, Fusco, Marin, *Alvarez: Not Enough Evidence to Charge Daley Nephew* (Mar. 19, 2011) (NEWS000071).

⁷⁶⁹ Alvarez, Anita, IGO Interview Rep. at 5 (Apr. 29, 2013). Kirk, Boliker, Hehner, and Sally Daly were also present for the interview. Daly, Sally, IGO Interview Rep. at 4 (Mar. 28, 2013); Special Grand Jury Exhibit 151 at 8 (Hehner, Walter, IGO Interview Rep. (Mar. 11, 2013)).

⁷⁷⁰ Alvarez, Anita, IGO Interview Rep. at 5 (Apr. 29, 2013).

⁷⁷¹ Alvarez, Anita, IGO Interview Rep. at 5 (Apr. 29, 2013). According to Kirk, reporters for the *Sun-Times* initially did not hear this remark. According to State's Attorney Alvarez's staff, it was only after they followed up with Novak and Marin as they were near the elevator bank when the reporters became aware and subsequently set up their equipment again to finish the interview. See Kirk, Daniel, IGO Interview Rep. at 8 (Mar. 26, 2013).

⁷⁷² Novak, Marin, Alvarez: *Investigate CPD Handling of Death Involving Daley Nephew* (Mar. 24, 2011) (NEWS000080).

jury, State's Attorney Alvarez stated, "We're not there at this point. It would be unethical for me to go to a grand jury at this point. I don't know if there was a crime committed here based on the facts we have. It could be justifiable."⁷⁷³

According to State's Attorney Alvarez and her staff, she discussed the possibility of referring the matter to an independent investigative agency prior to March 24, 2011.⁷⁷⁴ State's Attorney Alvarez considered referring the matter to an independent agency because she felt CPD could not fairly investigate the alleged police misconduct aspect of the case.⁷⁷⁵ According to Kirk, SAO's initial thought was to send the case to either the FBI or the South Suburban Major Crime Taskforce.⁷⁷⁶ It was determined, however, that both of these organizations lacked the necessary jurisdiction.⁷⁷⁷ The Illinois Attorney General's Office was also considered, but since Yawger worked there, it too presented a potential conflict.⁷⁷⁸

According to Hehner, SAO also evaluated the possibility of appointing someone from its own Special Prosecutions Bureau or petitioning for the appointment of a special prosecutor.⁷⁷⁹ In fact, State's Attorney Alvarez directed one of her top appellate prosecutors, Alan Spellberg, to research the appointment of a special prosecutor.⁷⁸⁰ In a memorandum dated March 10, 2011, Spellberg detailed his research regarding the rules and standards for appointing a special

⁷⁷³ Novak, Marin, Alvarez: *Investigate CPD Handling of Death Involving Daley Nephew* (Mar. 24, 2011) (NEWS000080).

⁷⁷⁴ Boliker, Shauna, IGO Interview Rep. at 3 (Mar. 25, 2013); Alvarez, Anita, IGO Interview Rep. at 5-6 (Apr. 29, 2013); Kirk, Daniel, IGO Interview Rep. at 8 (Mar. 26, 2013); Special Grand Jury Exhibit 151 at 8 (Hehner, Walter, IGO Interview Rep. (Mar. 11, 2013)).

⁷⁷⁵ Alvarez, Anita, IGO Interview Rep. at 5-6 (Apr. 29, 2013).

⁷⁷⁶ Kirk, Daniel, IGO Interview Rep. at 8-10 (Mar. 26, 2013).

⁷⁷⁷ Kirk, Daniel, IGO Interview Rep. at 10 (Mar. 26, 2013); Special Grand Jury Exhibit 151 at 8 (Hehner, Walter, IGO Interview Rep. (Mar. 11, 2013)).

⁷⁷⁸ Kirk, Daniel, IGO Interview Rep. at 8-9 (Mar. 26, 2013); Special Grand Jury Exhibit 151 at 8 (Hehner, Walter, IGO Interview Rep. (Mar. 11, 2013)). This observation raises the question of why SAO did not have a similar conflict based upon O'Brien's continued employment at SAO.

⁷⁷⁹ Kirk, Daniel, IGO Interview Rep. at 10 (Mar. 26, 2013); Special Grand Jury Exhibit 151 at 8 (Hehner, Walter, IGO Interview Rep. (Mar. 11, 2013)).

⁷⁸⁰ Alvarez, Anita, IGO Interview Rep. at 3 (Apr. 29, 2013).

prosecutor, including whether political ties to another person alone were sufficient to warrant the appointment of a special prosecutor.⁷⁸¹ Spellberg's memorandum did not conclude one way or another whether a special prosecutor should be appointed in the case but discussed the application of Section 3-9008 of the Counties Code, which provides that:

Whenever the State's attorney is sick or absent, or unable to attend, or is interested in any cause or proceeding, civil or criminal, which it is or may be his duty to prosecute or defend, the court in which said cause or proceeding is pending may appoint some competent attorney to prosecute or defend such cause or proceeding[.]⁷⁸²

While State's Attorney Alvarez was not involved in the Koschman case in 2004, she was the Chief Deputy State's Attorney at that time. Her current First Assistant and Chief Deputy, Boliker and Hehner, were also supervisors at SAO in 2004.⁷⁸³ Further, O'Brien, who was Felony Review supervisor in 2004, was also a supervisor under State's Attorney Alvarez after she became State's Attorney in 2008. In his April 6, 2012 Order appointing a special prosecutor, Judge Toomin determined that SAO possessed an institutional conflict of interest requiring the appointment of a special prosecutor.⁷⁸⁴

According to Kirk, State's Attorney Alvarez ultimately decided not to seek a special prosecutor but to have her office keep the case. She did decide for investigative purposes only to refer the case to ISP because in her mind it had previously investigated crimes involving CPD personnel, had the necessary resources, had a good working history with SAO, and was known for conducting thorough investigations.⁷⁸⁵ However, State's Attorney Alvarez chose ISP even though she knew that Hiram Grau — who was employed as a CPD Deputy Superintendent in

⁷⁸¹ Spellberg memo re Rules for Appointing a Special State's Attorney or Convening a Grand Jury (Mar. 10, 2011) (CCSAO_019628-CCSAO_019630).

⁷⁸² See 55 ILCS 5/3-9008 (West 2011).

⁷⁸³ In 2004, Boliker was chief of the Sex Crimes Division and Hehner was Deputy Chief of Narcotics. Boliker, Shauna, IGO Interview Rep. at 1 (Mar. 25, 2013); Special Grand Jury Exhibit 151 at 1 (Hehner, Walter, IGO Interview Rep. (Mar. 11, 2013)).

⁷⁸⁴ Order by J. Toomin at 33, Apr. 6, 2012.

⁷⁸⁵ Kirk, Daniel, IGO Interview Rep. at 8-9 (Mar. 26, 2013).

2004⁷⁸⁶ and as Deputy Chief of the Investigations Bureau at SAO in 2011 — would soon become the agency's director.⁷⁸⁷ According to State's Attorney Alvarez, she knew prior to March 22, 2011 that Grau would be taking over at ISP, but she believed the transition would take several months, and if Grau did arrive before the ISP's investigation of the Koschman case was over, ISP could have "walled" Grau off from the case.⁷⁸⁸

During his interview with the OSP, Kirk recalled that he was the first to reach out to ISP.⁷⁸⁹ According to Kirk, on the afternoon of the March 24, 2011, *Sun-Times* interview, he called ISP First Deputy Director Jack Garcia and told him about the proposed referral.⁷⁹⁰ According to Kirk, Garcia told him to send everything SAO had on the Koschman case to ISP Interim Director Patrick Keen.⁷⁹¹ Kirk also recalled that during this call, Kirk flagged the issue of Grau taking over as Director of ISP, but that Garcia assured Kirk it would not be a problem — either ISP would be able to conduct the entire investigation before Grau was confirmed, or Grau

⁷⁸⁶ In 2004, Grau reported to Superintendent Cline and had oversight over CPD's Detective Division. When interviewed by the OSP in 2012, Molloy, Chief of Detectives in 2004 and directly under Grau, recalled that while he did not discuss the case with Grau, he recalled leaving a copy of the detectives' police report "detailing what [went] on the night of the lineup" in a sealed envelope for Grau. Molloy, James, Kroll Interview Rep. at 5 (Dec. 7, 2012). Nevertheless, when asked about Molloy leaving a copy of a police report for him in 2004, Grau stated he did not recall receiving a report from Molloy and indicated he had no involvement in the Koschman case. Grau, Hiram, IGO Interview Rep. at 2-3 (Dec. 19, 2012).

⁷⁸⁷ Boliker, Shauna, IGO Interview Rep. at 4 (Mar. 25, 2013); Kirk, Daniel, IGO Interview Rep. at 9 (Mar. 26, 2013); Special Grand Jury Exhibit 151 at 5 (Hehner, Walter, IGO Interview Rep. (Mar. 11, 2013)); Keen, Patrick, IGO Interview Rep. at 2 (Jan. 10, 2013); Alvarez, Anita, IGO Interview Rep. at 6 (Apr. 29, 2013). Grau told the OSP that he has never spoken with State's Attorney Alvarez about the Koschman case. *Id.* According to State's Attorney Alvarez, she never spoke with Grau about her communications with ISP or Keen. Alvarez, Anita, IGO Interview Rep. at 7 (Apr. 29, 2013).

⁷⁸⁸ Alvarez, Anita, IGO Interview Rep. at 6 (Apr. 29, 2013). According to Grau, he informed State's Attorney Alvarez as soon as he accepted the ISP nomination. Grau, Hiram, IGO Interview Rep. at 3 (Dec. 19, 2012). On April 6, 2011, the *Sun-Times* published an article by Michael Sneed, "*Hot Potato?*," discussing SAO's referral to ISP and quoting Kirk as stating, "Hiram [Grau] still is not in charge of the Illinois State Police — and they certainly had enough time during the past few weeks to re-interview witnesses and finish their probe before he [Grau] got there." Michael Sneed, "*Hot Potato?*" at NEWS000117 (Apr. 6, 2011) (NEWS000116-NEWS000118).

⁷⁸⁹ Kirk, Daniel, IGO Interview Rep. at 9 (Mar. 26, 2013).

⁷⁹⁰ Kirk, Daniel, IGO Interview Rep. at 9 (Mar. 26, 2013).

⁷⁹¹ Kirk, Daniel, IGO Interview Rep. at 9 (Mar. 26, 2013).

would be walled off from the investigation.⁷⁹²

On March 24, 2011, SAO also sent a letter to Keen signed by State's Attorney Alvarez.⁷⁹³ The letter notes that "according to new information brought to my attention, some witnesses now suggest that the versions of events attributed to them in CPD reports from 2004 were not accurate including one witness who now claims that his observations during one of the lineups were not accurately memorialized," and requests that ISP "initiate and conduct an independent investigation of this matter in its entirety."⁷⁹⁴ The letter additionally states, "To be clear, at this point, I have no objective evidence to support the notion that there was any misfeasance or malfeasance on the part of investigators in this case. However, with this new information, it is my belief that an independent investigation from a separate police agency is clearly warranted to ensure that we reach the truth in this case."

On March 25, 2011, State's Attorney Alvarez sent a letter thanking Keen for accepting the referral of the Koschman case pursuant to her March 24, 2011 letter and their conversation "early this afternoon."⁷⁹⁵ Along with that letter, SAO sent copies of what it believed "to be the complete Chicago Police Department investigative file."⁷⁹⁶ According to Keen, although the package was received by Keen's Chief of Staff, Jessica Trame, no one at the agency opened or reviewed it.⁷⁹⁷ According to Keen, ISP awaited further direction from the Governor's Office on

⁷⁹² Kirk, Daniel, IGO Interview Rep. at 9 (Mar. 26, 2013).

⁷⁹³ Alvarez letter to Keen (Mar. 24, 2011) (ISP000013-ISP000014).

⁷⁹⁴ Alvarez letter to Keen (Mar. 24, 2011) (ISP000013-ISP000014).

⁷⁹⁵ Alvarez letter to Keen (Mar. 25, 2011) (CCSAO_033312).

⁷⁹⁶ Alvarez letter to Keen (Mar. 25, 2011) (CCSAO_033312). State's Attorney Alvarez asked Boliker to oversee the logistics of the referral. To that end, Boliker obtained a copy of the Koschman file from Salemme, which she photocopied and had sent to ISP. *See* Alvarez, Anita, IGO Interview Rep. at 6 (Apr. 29, 2013); Boliker, Shauna, IGO Interview Rep. at 6 (Mar. 25, 2013). At this point, CPD did not inform SAO that the Koschman materials it provided SAO did not include original files, that CPD was aware that the original Koschman homicide file was missing, and/or that CPD personnel had already searched for the original file. It was not until July 22, 2011, that CPD provided SAO with the missing Koschman files Walsh and Yawger discovered on June 29 and 30, 2011. Alvarez letter to Ferguson (July 22, 2011) (IG_001737).

⁷⁹⁷ Keen, Patrick, IGO Interview Rep. at 2-3 (Jan. 10, 2013). According to Keen, the file sent by SAO remained unopened in Trame's office.

whether it would actually go through with an independent investigation.⁷⁹⁸

When interviewed by the OSP, Grau stated that sometime around March 25, 2011, the day after State's Attorney Alvarez referred the case to Keen, he called Keen and told him to decline the referral from SAO.⁷⁹⁹ According to Grau, he considered recusing himself but determined that the situation would present a conflict of interest since he was a former SAO and CPD employee.⁸⁰⁰ During his interview with the OSP, Grau stated that on March 28, 2011, he sent a letter to Governor Pat Quinn (which he may have hand-delivered to the Governor's Chicago Office)⁸⁰¹ that "given [his] impending appointment as Director of ISP, ISP must decline to conduct this review."⁸⁰² In his letter, Grau explained that the appearance of a conflict of interest would undermine the effect of ISP's review and recommended "that Cook County State's Attorney Alvarez should request a complete review of this matter by the Federal Bureau of Investigation."⁸⁰³ According to Grau, no one suggested that he write the letter and the

⁷⁹⁸ Keen, Patrick, IGO Interview Rep. at 2-3 (Jan. 10, 2013). On March 25, 2011, at approximately 3:19 p.m., Trame sent an e-mail to others at ISP stating, "The Governor's office has made the decision that we will be re-investigating this death. [Interim] Director Keen has spoken w SA Alvarez and she is fedexing the case file to this office." See Trame e-mail to Mark Piccoli, Rob Haley, and Luis Tigera (Mar. 25, 2011) (ISP000025). Also on March 25, 2011, Novak sent a request to ISP seeking a statement on SAO's letter referring the Koschman case. In response, Isaiah Vega, of ISP's Public Information Office, sent Novak a statement that read, "[a]t the State's Attorney's request, we will review the matter. The primary purpose of the State's Attorney's Office's request and of our review will be investigating the 2004 incident." When Novak subsequently requested an interview with Grau, Vega forwarded the request to an employee of the Governor's Press Office, Grant Klinzman. Klinzman subsequently sent a statement "approved for use" to Vega, which stated, "[w]hile he was not personally involved in CPD's investigation of the 2004 incident, out of an abundance of caution Mr. Grau will be recusing himself from the State Police's review of the matter." This e-mail chain was forwarded on to Keen. Trame e-mail to Keen (Mar. 25, 2011) (ISP000042-ISP000043).

⁷⁹⁹ Grau, Hiram, IGO Interview Rep. at 3-4 (Dec. 19, 2012); Keen, Patrick, IGO Interview Rep. at 4 (Jan. 10, 2013). According to Grau, Keen told him that he had already accepted the referral. Grau, Hiram, IGO Interview Rep. at 3 (Dec. 19, 2012).

⁸⁰⁰ Grau, Hiram, IGO Interview Rep. at 3-4 (Dec. 19, 2012); Keen, Patrick, IGO Interview Rep. at 4 (Jan. 10, 2013).

⁸⁰¹ According to Grau, he probably hand-delivered the letter to the Governor's offices in Chicago. Grau, Hiram, IGO Interview Rep. at 4 (Dec. 19, 2012).

⁸⁰² Grau letter to Quinn (Mar. 28, 2011) (OSP_003196).

⁸⁰³ Grau letter to Quinn (Mar. 28, 2011) (OSP_003196).

decision to write it was his own.⁸⁰⁴

Ultimately, ISP rejected the referral of the Koschman case. According to Keen, ISP waited approximately 7-10 days before the Governor's Office communicated that ISP should send the case back.⁸⁰⁵ According to Kirk, approximately 7-10 days after SAO sent the package of police reports, Garcia called him and, without giving any explanation, hinted that ISP may send the case back to SAO.⁸⁰⁶

On April 4, 2011, Keen sent a letter to State's Attorney Alvarez rejecting the referral.⁸⁰⁷ Keen's letter stated, "I have determined that the Illinois State Police is not the appropriate entity to conduct the requested review of the 2004 investigation. Accordingly, the case file is enclosed and is being returned for further handling as you deem appropriate, whether by naming an independent, special prosecutor who, unlike ISP, if warranted, could convene a grand jury to hear statements made under oath, or by referring the matter to another criminal justice entity with similar powers."⁸⁰⁸ Upon learning of ISP's decision, State's Attorney Alvarez called Keen to express her disappointment; he too provided no explanation for the rejection.⁸⁰⁹

According to Kirk, ISP's rejection of SAO's referral resulted in a "scramble" to find an investigative partner, which led to SAO's decision to partner with IGO and its investigation into the Koschman matter that it began the previous month.⁸¹⁰ By early September 2011, IGO had

⁸⁰⁴ Grau, Hiram, IGO Interview Rep. at 3-4 (Dec. 19, 2012). Grau did not speak with anyone from SAO before writing the letter to Governor Quinn. Grau, Hiram, IGO Interview Rep. at 4 (Dec. 19, 2013).

⁸⁰⁵ Keen, Patrick, IGO Interview Rep. at 4 (Jan. 10, 2013). In response to a subpoena from the special grand jury, ISP asserted attorney-client privilege over approximately 10 documents (including e-mails and handwritten notes) that involved communications with the Governor's Office or personnel in the General Counsel's Office of the Governor's Office.

⁸⁰⁶ Kirk, Daniel, IGO Interview Rep. at 9 (Mar. 26, 2013). According to Keen, he subsequently called Kirk to confirm that ISP was not taking the Koschman case but did not provide a reason for the rejection. Keen, Patrick, IGO Interview Rep. at 5 (Jan. 10, 2013).

⁸⁰⁷ Keen letter to Alvarez (Apr. 4, 2011) (ISP000012).

⁸⁰⁸ Keen letter to Alvarez (Apr. 4, 2011) (ISP000012).

⁸⁰⁹ Alvarez, Anita, IGO Interview Rep. at 6 (Apr. 29, 2013); Kirk, Daniel, IGO Interview Rep. at 9-10 (Mar. 26, 2013); Keen, Patrick, IGO Interview Rep. at 5-6 (Jan. 10, 2013).

⁸¹⁰ Kirk, Daniel, IGO Interview Rep. at 10 (Mar. 26, 2013). As ISP considered whether or not to accept SAO's referral of the Koschman case, Cook County Inspector General Patrick Blanchard

gathered and reviewed certain documents and conducted several witness interviews.

In early September 2011, representatives from both the IGO and SAO met to discuss the use of SAO's grand jury in order to further the IGO's investigation.⁸¹¹ Between September and December 2011, SAO and IGO shared information about the investigation and discussed the order in which witnesses would be called before the grand jury. Prior to any witnesses testifying before SAO's grand jury, on December 14, 2011, Nanci Koschman, Susan Pazderski (Koschman's maternal aunt), and Richard Pazderski (Koschman's uncle) filed a petition for the appointment of a special prosecutor with the Circuit Court of Cook County.⁸¹² SAO first obtained grand jury subpoenas for witnesses to appear on January 18, 2012, after the petition for the appointment of a special prosecutor had been filed, and approximately nine months after SAO had decided to initiate an investigation.⁸¹³

attempted to initiate an investigation of his own into SAO's handling of the Koschman case. On March 30, 2011, Blanchard, accompanied by Steven Cyranoski of the Cook County Inspector General's Office ("CCIGO"), met with Kirk, Boliker, Hehner, and Castiglione from SAO. Kirk told Blanchard that CCIGO did not have jurisdiction to investigate SAO. *See* Blanchard, Patrick, Kroll Interview Rep. at 5-7 (Dec. 19, 2012). At the meeting, Kirk also stated that SAO could not locate a felony review folder for the Koschman case, but that O'Brien went down to Area 3 that day and simply failed to fill one out. Blanchard, Patrick, Kroll Interview Rep. at 5 (Dec. 19, 2012); Blakey, Jack, Kroll Interview Rep. at 2-4 (May 9, 2013); *see also* Kirk, Daniel, IGO Interview Rep. at 4 (Mar. 26, 2013).

⁸¹¹ Mahoney, John, Kroll Interview Rep. at 4-5 (Mar. 7, 2013). By September 2011, IGO had issued document requests to CPD and formally subpoenaed SAO seeking records related to the Koschman case. IGO had also interviewed witnesses, including Koschman's friends: Allen, Copeland, Francis, and Hageline.

⁸¹² *In re Appointment of Special Prosecutor*, No. 2011 Misc. 46, Petition to Appoint a Special Prosecutor in the Matter of the Death of David Koschman (Dec. 22, 2011) (Locke E. Bowman and Alexa Van Brunt of the Roderick MacArthur Justice Center at Northwestern University School of Law and G. Flint Taylor of the People's Law Office represented Mrs. Koschman, Mrs. Pazderski, and Mr. Pazderski). The petition for the appointment of a special prosecutor argued, in part, that State's Attorney Alvarez maintained a "clear political — and personal — interest in the case" based upon her public statements defending "the work of the Chicago Police and the Cook County State's Attorney's Felony Review unit, insisting to *Sun-Times* reporters that there was insufficient evidence to charge Vanecko." *In re Appointment of Special Prosecutor*, No. 2011 Misc. 46, Petition to Appoint a Special Prosecutor in the Matter of the Death of David Koschman at 19-20 (Dec. 22, 2011).

⁸¹³ SAO issued its first grand jury subpoenas on Jan. 18, 2012 to Lt. Walsh, Det. Rita O'Leary, Ofc. Tremore, Det. Clemens, Craig Denham, Kevin McCarthy, and Bridget McCarthy. Mahoney, John, Kroll Interview Rep. at 11 (Mar. 7, 2013); *see also* SAO Grand Jury Subpoenas (Jan. 18, 2011) (CCSAO_013735 (Walsh); CCSAO_013743 (Rita O'Leary); CCSAO_013742 (Tremore); CCSAO_013744 (Clemens); CCSAO_013746 (Denham); CCSAO_013749 (Kevin McCarthy); CCSAO_013750 (Bridget McCarthy)). While SAO interviewed several witnesses, only two witnesses

4. State's Attorney's Office's Response to the Petition for the Appointment of a Special Prosecutor

When interviewed by the OSP in 2013, Boliker indicated that in the days following the filing of the petition for the appointment of a special prosecutor, State's Attorney Alvarez's staff met and decided to file an opposition to the petition.⁸¹⁴ On January 6, 2012, WLS-890 radio talk show host Bill Cameron interviewed State's Attorney Alvarez. Part of the interview included several questions regarding the Koschman matter. During the interview, State's Attorney Alvarez indicated it was still unclear whether SAO would be opposing the petition. State's Attorney Alvarez commented on the strength of the case, stating:

Mayor Daley didn't have a good relationship with the rank-and-file CPD and that's the truth, there are you know, but you have to look at what occurred in this case in the simple fact, you know, people looked at lineups and did not identify [sic] any prosecutor knows that's a fatal flaw in your case if you don't have identification and any defense attorney would be doing backflips if his client did not get identified in a case, so there are flaws — there are serious flaws...You know, we're not even sure who threw the punch and that's the conflicting evidence that we have looked at. At the time this happened no one identified him as being the one, and we don't even know if it was [sic] punch or push.

State's Attorney Alvarez's comments regarding a lack of certainty that Koschman was punched contrasted with CPD's conclusions in 2011 that Vanecko alone punched Koschman and Scott Allen and James Copeland's statements in 2004 and 2011, as the only two witnesses who saw the moment of impact, that Koschman was punched. Judge Toomin noted that comments such as these by State's Attorney Alvarez arguably call into question whether SAO could have independently reviewed the matter.⁸¹⁵

testified before a grand jury. *See* Blakey, Jack, Kroll Interview Rep. at 3 (May 9, 2013). On February 15, 2012, SAO had Rita O'Leary read a prepared statement before the grand jury. O'Leary, Rita, SAO Grand Jury Tr. (Feb. 15, 2012) (CCSAO_018589). On Feb. 21, 2012, Megan McDonald also testified before a grand jury. McDonald, Megan, SAO Grand Jury Tr. (Feb. 21, 2012) (CCSAO_017540).

⁸¹⁴ *See* Boliker, Shauna, IGO Interview Rep. at 4 (Mar. 25, 2013).

⁸¹⁵ *See* Order by J. Toomin at 29, Apr. 6, 2012. Former State's Attorney Devine recalled commenting to State's Attorney Alvarez (sometime after SAO's involvement became public in 2011) that

On January 31, 2012, SAO filed its brief opposing the appointment of a special prosecutor, relying heavily on witness statements given by Koschman's friends in arguing a lack of an evidentiary basis for the appointment.⁸¹⁶ On April 6, 2012, Judge Toomin granted Nanci Koschman's petition for a Special Prosecutor and on April 23, 2012, appointed Dan Webb as Special Prosecutor. As a result of the Court's rulings, SAO ceased its investigation and cooperated in transitioning the case to the OSP. However, SAO continued to comment on the case.

Indeed, on April 24, 2012, one day after the appointment of the Special Prosecutor, in a *Chicago Tribune* article entitled, “*Investigator Has Many Targets Koschman Case Involves Cops, Prosecutors, Daley Clout*,” reporters noted that, “According to Kirk, Alvarez’s chief of staff at that time [in 2004], there was no admissible evidence that could have been used to file charges.”⁸¹⁷ However, when interviewed by the OSP in 2013, Kirk acknowledged that there was in fact some evidence that would be admissible at trial and that he had based his statements to the *Chicago Tribune* on what he learned from O’Brien and Hehner — and without conducting an extensive review of the police reports or speaking with any witnesses or detectives.⁸¹⁸

On December 3, 2012, the special grand jury indicted Vanecko for involuntary manslaughter in connection with Koschman’s death. State’s Attorney Alvarez made a statement that same day that SAO’s grand jury investigation had been looking into the case for “months, almost close to a year.”⁸¹⁹ When interviewed by the OSP, State’s Attorney Alvarez explained

“This [the Koschman case] was on my watch, you don’t need to wear the jacket on this.” Devine, Richard, IGO Interview Rep. at 6 (Apr. 9, 2013).

⁸¹⁶ See *In re Appointment of Special Prosecutor*, No. 2011 Misc. 46, People’s Resp. to the Pet. To Appoint a Special Pros. at 15-37 (Jan. 31, 2012). Additionally, in response to petitioner’s motion to compel witness statements recorded by IGO’s investigators, on February 21, 2012, SAO filed a brief with Judge Toomin warning, “The wholesale disclosure of the information that Petitioners request would disrupt the ongoing criminal investigation and further undermine an already dim prospect of any future criminal prosecution.” *In re Appointment of Special Prosecutor*, No. 2011 Misc. 46, People’s Response to Petitioners’ Motion to Compel at 8 (Feb. 21, 2012); Fusco, Novak, *State’s Attorney: Releasing Koschman Transcripts Would ‘Undermine’ Case* (Feb. 22, 2012) (NEWS000310).

⁸¹⁷ Jason Meisner and Steve Mills, *Investigator Has Many Targets Koschman Case Involves Cops, Prosecutors, Daley Clout* at NEWS000408 (Apr. 24, 2012) (NEWS000406-NEWS000411).

⁸¹⁸ Kirk, Daniel, IGO Interview Rep. at 7-8 (Mar. 26, 2013).

⁸¹⁹ Dan Mihalopoulos, *Alvarez: State’s Attorney Office Did Nothing Wrong* at NEWS000522 (Dec.

that she meant IGO's investigation had lasted a year, even if her office had not utilized the grand jury for the whole period.⁸²⁰ While IGO conducted over 30 interviews in 2011 and early 2012, SAO did not use the grand jury at all in 2011 and conducted six interviews in 2011 and early 2012. Between January and April 2012, SAO presented one witness and one statement of a witness before a grand jury.

V. LEGAL ANALYSIS

A. Three Levels of Scienter (State of Mind): Recklessness, Knowledge, and Intent

There are three relevant levels of scienter (state of mind), relating to the criminal statutes at issue, which are defined in the Illinois Criminal Code: recklessness,⁸²¹ knowledge,⁸²² and intent.⁸²³

1. Recklessness

"Recklessness" is a mental state involving a degree of criminal liability below that of knowledge or intent,⁸²⁴ and is defined by the Illinois Criminal Code as follows:

A person is reckless or acts recklessly when that person consciously disregards a substantial and unjustifiable risk that circumstances exist or that a result will follow, described by the statute defining the offense, and that disregard constitutes a gross deviation from the standard of care that a reasonable person would exercise in the situation. . . .⁸²⁵

3, 2012) (NEWS000522-NEWS000523).

⁸²⁰ Alvarez, Anita, IGO Interview Rep. at 8 (Apr. 29, 2013).

⁸²¹ 720 ILCS 5/4-6 (West 2013).

⁸²² 720 ILCS 5/4-5 (West 2013).

⁸²³ 720 ILCS 5/4-4 (West 2013).

⁸²⁴ *People v. Higgins*, 229 N.E.2d 161, 163-64 (Ill. App. Ct. 5th Dist. 1967).

⁸²⁵ 720 ILCS 5/4-6 (West 2013); *see also* Illinois Pattern Jury Instruction 5.01 ("A person acts recklessly when he consciously disregards a substantial and unjustifiable risk that circumstances exist or that a result will follow, and such disregard constitutes a gross deviation from the standard of care which a reasonable person would exercise in the situation.") (*citing People v. Baier*, 203 N.E.2d 633 (Ill. App. Ct. 1st Dist. 1964)).

2. Knowledge

The Illinois Criminal Code defines the mental state of “knowledge” as follows:

A person knows, or acts knowingly or with knowledge of:

- (a) The nature or attendant circumstances of his or her conduct, described by the statute defining the offense, when he or she is consciously aware that his or her conduct is of that nature or that those circumstances exist. Knowledge of a material fact includes awareness of the substantial probability that the fact exists.
- (b) The result of his or her conduct, described by the statute defining the offense, when he or she is consciously aware that that result is practically certain to be caused by his conduct. . . .

When the law provides that acting knowingly suffices to establish an element of an offense, that element also is established if a person acts intentionally.⁸²⁶

3. Intent

The Illinois Criminal Code defines “intent” as follows:

A person intends, or acts intentionally or with intent, to accomplish a result or engage in conduct described by the statute defining the offense, when his conscious objective or purpose is to accomplish that result or engage in that conduct.⁸²⁷

Under Illinois law, every sane person is presumed to intend all the natural and probable results of his or her own deliberate act.⁸²⁸

B. Scienter (State of Mind) Requirements of Relevant Criminal Statutes

As noted above, the four Illinois criminal statutes primarily evaluated by the Special Prosecutor were: (1) official misconduct; (2) obstructing justice; (3) conspiracy; and (4) tampering with public records. The definitions of each of these crimes, including their criminal intent (scienter) requirements, follows:

⁸²⁶ 720 ILCS 5/4-5 (West 2013); *see also* Illinois Pattern Jury Instruction 5.01.

⁸²⁷ 720 ILCS 5/4-4 (West 2013); *see also* Illinois Pattern Jury Instruction 5.01A.

⁸²⁸ *People v. Shields*, 127 N.E.2d 440, 443 (Ill. 1955); *People v. Varnell*, 370 N.E.2d 145, 146 (Ill. App. Ct. 2d Dist. 1977); *People v. Smith*, 219 N.E.2d 82, 86-87 (Ill. App. Ct. 1st Dist. 1966).

Official Misconduct: A public officer or employee violates Illinois' official misconduct statute when he does any of the following in his official capacity: (a) *[i]ntentionally or recklessly* fails to perform any mandatory duty as required by law; (b) *[k]nowingly* performs an act which he knows he is forbidden by law to perform; (c) *[w]ith intent* to obtain a personal advantage for himself or another, he performs an act in excess of his lawful authority; or (d) [s]olicits or *knowingly* accepts for the performance of any act a fee or reward which he knows is not authorized by law⁸²⁹

Obstructing Justice: A person obstructs justice when, *with intent* to prevent the apprehension or obstruct the prosecution or defense of any person, he *knowingly* commits any of the following acts: (a) destroys, alters, conceals or disguises physical evidence, plants false evidence or furnishes false information; (b) induces a witness having knowledge material to the subject at issue to leave the State or conceal himself; (c) possesses knowledge material to the subject at issue, leaves the State or conceals himself or herself.⁸³⁰

Conspiracy: A person commits the offense of conspiracy when, *with intent* that an offense be committed, he or she agrees with another to the commission of that offense. No person may be convicted of conspiracy to commit an offense unless an act in furtherance of that agreement is alleged and proved to have been committed by him or her or by a co-conspirator. . . .⁸³¹

Tampering with Public Records: A person commits tampering with public records when he or she *knowingly*, without lawful authority, and *with the intent* to defraud any party, public officer or entity, alters, destroys, defaces, removes or conceals any public record. . . .⁸³²

⁸²⁹ See 720 ILCS 5/33-3(a)-(d) (West 2013) (emphasis added).

⁸³⁰ 720 ILCS 5/31-4 (West 2013) (emphasis added).

⁸³¹ 720 ILCS 5/8-2(a) (West 2013) (emphasis added)

⁸³² 720 ILCS 5/32-8(a) (West 2013) (emphasis added).

C. Prosecution of Conduct Committed in 2004 is Barred by the Statute of Limitations

As of the Special Prosecutor's appointment on April 23, 2012, approximately eight years had passed since the incident on Division Street. As a result, in evaluating⁸³³ whether criminal charges should be brought against any CPD or SAO employees for conduct occurring during the initial investigation into Koschman's death in 2004, the Special Prosecutor was required to contend with the reality that many potential criminal charges were likely barred by Illinois' statute of limitations, 720 ILCS 5/3-5.⁸³⁴ The Special Prosecutor was also required to consider his burden of proof. Under Illinois law, where an indictment on its face shows that an offense was not committed within the applicable limitation period, the prosecutor must allege those facts that invoke an exception to the statute of limitations and ultimately must prove that exception beyond a reasonable doubt at trial.⁸³⁵

Aside from specifically enumerated offenses such as murder or involuntary manslaughter, 720 ILCS 5/3-5(b) requires that any prosecution for an offense not so enumerated "must be commenced within 3 years after the commission of the offense if it is a felony, or within one year and 6 months after its commission if it is a misdemeanor." Thus, a prosecution for a felony violation of state law official misconduct, obstructing justice, conspiracy, or tampering with public records statutes is time-barred if not brought within three years — with only limited circumstances in which the three-year limitations period set forth in 720 ILCS 5/3-5(b) may be extended or tolled (temporarily halted). As detailed below, the Special Prosecutor evaluated whether such circumstances might apply in this matter, including the following

⁸³³ The Special Prosecutor's evaluation was limited to state (and not federal) criminal law violations.

⁸³⁴ A statute of limitations is a "statute establishing a time limit for prosecuting a crime, based on the date when the offense occurred." Black's Law Dictionary (9th ed. 2009); *see also Toussie v. United States*, 397 U.S. 112, 114 (1970) ("The purpose of a statute of limitations is to limit exposure to criminal prosecution to a certain fixed period of time following the occurrence of those acts the legislature had decided to punish by criminal sanctions. Such a limitation is designed to protect individuals from having to defend themselves against charges when the basic facts have become obscured by the passage of time and to minimize the danger of official punishment because of acts in the far-distant past. Such a time limit may also have the salutary effect of encouraging law enforcement officials promptly to investigate suspected criminal activity.").

⁸³⁵ See Illinois Pattern Jury Instructions (Criminal) § 24-25.23; *People v. Morris*, 135 Ill. 2d 540, 546 (1990); *People v. Pacheco*, 338 Ill. App. 3d 616, 617-18 (Ill. App. Ct. 2d Dist. 2003); *People v. Gwinn*, 255 Ill. App. 3d 628, 631 (Ill. App. Ct. 2d Dist. 1994).

exceptions or tolling provisions applicable to the three-year limitations period, but ultimately concluded that none applied.

1. Public Misconduct

First, Illinois law provides for an extension to the three-year limitations period in cases involving an “offense based upon misconduct in office by a public officer or employee.”⁸³⁶ Specifically, 720 ILCS 5/3-6(b) provides that “[a] prosecution for any offense based upon misconduct in office by a public officer or employee may be commenced within one year after discovery of the offense by a person having a legal duty to report such offense, or in the absence of such discovery, within one year after the proper prosecuting officer becomes aware of the offense.” However, 720 ILCS 5/3-6(b) further states that “in no such case is the period of limitation so extended more than 3 years beyond the expiration of the period otherwise applicable.” Thus, even assuming the three-year statute of limitations period for an offense such as official misconduct could be extended based upon delayed discovery of the crime, the limitations period for any such offense committed in 2004 expired six years later, in 2010, prior to the Special Prosecutor’s appointment.⁸³⁷

2. Out-of-State Residency

Second, Illinois law provides that the “period within which a prosecution must be commenced does not include any period in which . . . [t]he defendant is not usually and publicly resident within this State.”⁸³⁸ As to individuals who were putative targets of the Special Prosecutor’s investigation into acts stemming from conduct that occurred in 2004, this tolling provision did not apply.

3. Continuous Conduct

Third, under Illinois law, where a defendant is charged with an offense comprised of a

⁸³⁶ 720 ILCS 5/3-6(b) (West 2013).

⁸³⁷ *See People v. Grever*, 353 Ill. App. 3d 736, 769 (Ill. App. Ct. 2d Dist. 2004) (“the longest period of limitations for the offense of official misconduct is six years (three years for the Class 3 felony (720 ILCS 5/3-5(b) (West 1998)) plus a three-year extension under section 3-6(b) because the offense is based upon misconduct in office by a public officer or employee (720 ILCS 5/3-6(b) (West 1998)).”), overruled in part on other grounds by *People v. Grever*, 222 Ill.2d 321 (Ill. 2006); see also *People v. Stevens*, 66 Ill. App. 3d 138, 139 (1978).

⁸³⁸ 720 ILCS 5/3-7(a) (West 2013).

series of individual acts or continuous conduct, the three-year limitations period does not commence until such time as the last act is committed. 720 ILCS 5/3-8 provides that, “[w]hen an offense is based on a series of acts performed at different times, the period of limitation prescribed by this Article starts at the time when the last such act is committed.”⁸³⁹ An offense such as obstructing justice⁸⁴⁰ is not a continuing offense for purposes of tolling the limitations period where the defendant simply fails to reveal his or her prior criminal conduct.⁸⁴¹ Thus, the failure of any CPD or SAO employees to later reveal to authorities criminal conduct occurring in 2004, or the concealment of such prior criminal conduct in 2004, would not convert any obstruction of justice committed in 2004 into a continuing offense such that it would not be time-barred by the statute of limitations.

4. Conspiracy

The Special Prosecutor also evaluated whether conduct committed in 2004 could potentially be charged as part of a continuing conspiracy. Under Illinois law, the limitations period for the offense of conspiracy begins to run from the date of the commission of the last

⁸³⁹ The term “act” is defined as including “a failure or omission to take action.” 720 ILCS 5/2-2 (West 2013). By way of example, courts have considered offenses such as failing to make and keep records of controlled substances administered, *People v. Griffiths*, 67 Ill. App. 3d 16 (Ill. App. Ct. 4th Dist. 1978), escape, *People v. Miller*, 157 Ill. App. 3d 43 (Ill. App. Ct. 1st Dist. 1987), concealing and failing to disclose the death of a social security beneficiary, *United States v. Morrison*, 43 F.R.D. 516 (N.D. Ill. 1967), and failing to register as an illegal alien, *United States v. Franklin*, 188 F.2d 182 (7th Cir. 1951), to constitute continuing offenses for purposes of determining whether a crime is barred by the statute of limitations.

⁸⁴⁰ 720 ILCS 5/31-4 (West 2013).

⁸⁴¹ See *People v. Criswell*, 12 Ill. App. 3d 102, 105 (Ill. App. Ct. 1st Dist. 1973). In *Criswell*, the defendant, after losing consciousness, found his step father’s body on the kitchen floor of their home with a knife stuck in his chest. *Id.* at 103. The defendant, afraid police would suspect he was culpable, disposed of the knife and buried the stepfather’s body in the home’s backyard. *Id.* After more than three years had passed, the defendant was charged with murder and misdemeanor obstructing justice (which was governed by a limitations period of one year and six months). *Id.* at 103-04. Prosecutors contended that the defendant’s obstruction of justice was a continuing offense under Illinois law because he had failed or omitted to dig up the step father’s body and indicate to law enforcement authorities that evidence had been concealed. *Id.* at 104. After the defendant was acquitted of murder at trial but convicted of obstructing justice, the appellate court reversed the conviction on the grounds that the offense was not a continuing offense and thus was barred by the statute of limitations. *Id.* at 105.

overt act in furtherance of that conspiracy.⁸⁴² As a result, the Special Prosecutor evaluated both: (a) whether there was evidence of a conspiracy in 2004 with a limitations period tolled by subsequent overt acts in furtherance of that conspiracy, and (b) whether there was evidence of a continuing conspiracy that spanned both 2004 and 2011 (and thus the limitations period would have commenced in 2011).

a. Evidence of a Conspiracy in 2004 with a Limitations Period Tolled by Subsequent Overt Acts

As noted above, the limitations period for a conspiracy offense commences at the time of the last overt act in furtherance of that conspiracy. Nevertheless, where the criminal purpose of a conspiracy has been attained, a subsequent overt act or conspiracy to conceal the initial conspiracy “may not be implied from circumstantial evidence showing merely that the conspiracy was kept a secret and that the conspirators took care to cover up their crime in order to escape detection and punishment.”⁸⁴³ Thus, assuming (for purposes of determining whether the statute of limitations would bar such a claim) the existence of a conspiracy in 2004, the Special Prosecutor would be barred from charging that conspiracy absent additional subsequent overt acts in furtherance of that conspiracy, aside from mere silence. In other words, if police and/or prosecutors conspired to obstruct justice in 2004, the Special Prosecutor could not charge that conspiracy without an additional subsequent overt act.

While the Special Prosecutor and the OSP reviewed records (such as access logs recording when police personnel accessed police reports) and interviewed witnesses which might have provided evidence of an intervening overt act (occurring after 2004 and within three years prior to the Special Prosecutor’s appointment in 2012), the Special Prosecutor’s investigation did not reveal any evidence of activity on behalf of police or prosecutors that might have served to toll the limitations period for any conspiracy that occurred in 2004.

⁸⁴² See *People v. Isaacs*, 37 Ill. 2d 205, 218 (1967); *People v. Drury*, 250 Ill. App. 547, 574-75 (Ill. App. Ct. 3d Dist. 1928).

⁸⁴³ *People v. Criswell*, 12 Ill. App. 3d 102, 105 (Ill. App. Ct. 1st Dist. 1973) (“allowing such a conspiracy to conceal to be inferred or implied from mere acts of concealment would result in a great widening of the scope of conspiracy prosecutions, since it would extend the life of a conspiracy indefinitely”).

b. Evidence of a Conspiracy Spanning Both 2004 and 2011

The Special Prosecutor's investigation also did not uncover evidence to prove beyond a reasonable doubt the existence of a conspiracy that spanned from the initial investigation into Koschman's death in 2004 through the re-investigation in 2011. In order for there to be a conspiracy, there must be an agreement of some kind.⁸⁴⁴ Additionally, in order to prove the offense of conspiracy, while unnecessary to demonstrate all co-conspirators were acquaintances or took part in all overt acts in furtherance of the conspiracy,⁸⁴⁵ a prosecutor must still demonstrate the existence of a conspiracy and each co-conspirator's specific intent to join that conspiracy.⁸⁴⁶ The Special Prosecutor's investigation did not uncover sufficient evidence to prove beyond a reasonable doubt that the same conspiracy existed in both 2004 and 2011 in connection with Koschman's death.

As detailed herein, the Special Prosecutor's investigation revealed that the same individuals involved with the investigation into Koschman's death in 2004 were not involved in CPD's re-investigation or SAO's involvement with the case in 2011. While the Special Prosecutor's investigation revealed some contact between certain of those individuals (for example, communications between Yawger and Walsh in 2011 concerning the missing Koschman homicide file), there was insufficient evidence to prove the existence of an agreement or the specific intent of any individual to join such an agreement. While the destruction or

⁸⁴⁴ *People v. Foster*, 457 N.E.2d 405, 408-09 (Ill. 1983); *People v. Ambrose*, 329 N.E.2d 11, 14 (Ill. App. Ct. 3d Dist. 1975); *People v. Cohn*, 193 N.E. 150, 153 (Ill. 1934); *see also People v. Lattimore*, 955 N.E.2d 1244 (Ill. App. Ct. 1st Dist. 2011); *People v. Chambers*, 303 N.E.2d 24, 27 (Ill. App. Ct. 3d Dist. 1973); *People v. Rudd*, 970 N.E. 2d 580, 583-84 (Ill. App. Ct. 5th Dist. 2012).

⁸⁴⁵ *People v. Cohn*, 193 N.E. 150, 153 (Ill. 1934) ("It [is] not necessary that [a co-conspirator] should be acquainted with all the others engaged in the conspiracy. The doing of some act or the making of some agreement showing [his or her] intent to be a participant [is] sufficient."); *People v. Buffman*, 636 N.E.2d 783, 790 (Ill. App. Ct. 1st Dist. 1994) ("Conspirators need not have entered the conspiracy at the same time or have taken part in all its actions to be criminally accountable for acts in furtherance of conspiracy.")

⁸⁴⁶ *People v. Foster*, 457 N.E.2d 405, 408-09 (Ill. 1983); *People v. Ambrose*, 329 N.E.2d 11, 14 (Ill. App. Ct. 3d Dist. 1975) ("definition of agreement implies an intent to agree between a minimum of two people"); *People v. Cohn*, 193 N.E. 150, 153 (Ill. 1934); *see also People v. Lattimore*, 955 N.E.2d 1244 (Ill. App. Ct. 1st Dist. 2011) (Intent may be inferred (1) from the defendant's conduct surrounding the act and (2) from the act itself); *People v. Chambers*, 303 N.E.2d 24, 27 (Ill. App. Ct. 3d Dist. 1973); *People v. Rudd*, 970 N.E. 2d 580, 583-84 (Ill. App. Ct. 5th Dist. 2012).

concealment of evidence or case files related to the Koschman case could constitute an overt act in furtherance of a theoretical prior conspiracy in 2004 to obstruct justice,⁸⁴⁷ the Special Prosecutor's investigation did not uncover evidence sufficient to prove such a conspiracy beyond a reasonable doubt.

D. The Events of 2011-2012: Evaluating Whether Employees of CPD and SAO Violated Illinois Criminal Law

1. Prosecution is Not Barred by the Applicable Statute of Limitations

As noted previously, unlike the events which occurred in 2004, any state law violations (e.g., for official misconduct, obstructing justice, conspiracy, or tampering with public records), by employees of CPD and SAO relating to acts that occurred in 2011-2012 are not barred by the applicable three-year statute of limitations as of the date of this report.

2. Summary of the Evidence from 2011-2012 Which Was Thoroughly Reviewed for Potential Criminal Charges

Generally, there are two types of evidence available to a prosecutor to prove criminal intent beyond a reasonable doubt: documentary evidence and testimonial evidence. Furthermore, criminal intent can be proven either directly or indirectly (i.e., inferred from circumstantial evidence). The Special Prosecutor and his office have analyzed all available documentary and testimonial evidence in this case — whether direct or circumstantial — for anything tending to show that any individual recklessly, knowingly, or intentionally violated Illinois law by suppressing and concealing evidence, furnishing false evidence, or generally impeding the investigation into Koschman's death. Having reviewed over 300,000 pages of documents obtained pursuant to special grand jury subpoenas, including e-mails, phone records, internal memoranda, and CPD report access logs, the Special Prosecutor has found no documentary evidence proving beyond a reasonable doubt that any employees of CPD or SAO recklessly, knowingly, or intentionally violated Illinois law during their participation in the Koschman matter in 2011 and 2012. Likewise, after questioning nearly 150 witnesses, the Special Prosecutor has identified no testimonial evidence proving beyond a reasonable doubt that any employees of CPD or SAO recklessly, knowingly, or intentionally violated Illinois law during their participation in the Koschman matter in 2011 and 2012.

⁸⁴⁷

See People v. Peebles, 457 N.E.2d 1318, 1322 (Ill. App. 1st Dist. 1983).

Therefore, based upon all the evidence gathered by the Special Prosecutor and the OSP (e.g., witness interviews, sworn witness testimony before the special grand jury, documents subpoenaed and reviewed), and after having evaluated the elements of the potentially applicable state criminal laws with regard to the acts of certain individuals, the Special Prosecutor does not believe he could prove beyond a reasonable doubt by legally sufficient evidence at trial that any employees of CPD or SAO recklessly, knowingly, or intentionally violated Illinois law during their participation in the Koschman matter in 2011 and 2012.

The Special Prosecutor, before making this determination, and based upon a thorough review of the entirety of the evidence from 2011-2012, ultimately focused on two primary issues for potential criminal charges: (1) whether CPD's 2011 determination that Vanecko acted in self-defense was criminal misconduct, and (2) whether the facts and circumstances surrounding Walsh's 2011 discovery of the missing CPD original Koschman homicide file amount to criminal misconduct. Both issues are discussed in turn below.

a. Whether CPD's 2011 Determination that Vanecko Acted In Self-Defense Was Criminal Misconduct

As discussed above in Section IV., C., CPD's 2011 re-investigation ultimately concluded that Vanecko punched Koschman, but that Vanecko had acted in self-defense. Vanecko never provided a statement to CPD about the April 2004 Division Street incident, including anything relating to his actual and subjective belief that such force was necessary to prevent imminent death or great bodily harm to himself or another. However, to be clear, Vanecko was not legally or constitutionally obligated to make any statement to CPD. The self-defense conclusion was significant because it was CPD's primary basis for not seeking charges in 2011.

The Special Prosecutor's investigation identified certain evidence that is arguably consistent with the theory that CPD's 2011 determination that Vanecko acted in self-defense was criminal misconduct. That evidence is discussed below.

i. Det. Gilger and Det. Spanos

The Special Prosecutor's investigation identified limited evidence that is arguably consistent with a theory that Gilger and Spanos manufactured CPD's 2011 self-defense determination. To begin with, three witness statements recorded by the two detectives have been called into question by these witnesses. In each instance, the inaccuracies identified by the witnesses in these statements tended to support CPD's 2011 determination that Vanecko acted in

self-defense. First, according to Gilger and Spanos' concluding case supp, which is based upon the witness statements they memorialized in their 2011 GPRs, "Copeland stated that they were trying to pull KOSCHMAN away from starting anymore [sic] trouble" before he was struck. But during his testimony before the special grand jury in 2012, Copeland testified this statement was not an accurate reflection of what happened the night of the incident, stating, "No. Again, I mean, I do remember, you know, gesturing and nudging him to kind of move away, but physically pulling him back, I don't remember doing that." Second, Gilger's GPR of the 2011 Allen interview stated that Koschman "was in the thick of the argument and was also yelling." But, when Allen appeared before the special grand jury in 2012, he testified that the statement was inaccurate "[b]ecause it's not like [Koschman] was in the thick of the argument. It was one giant argument and we were all yelling, so no, I would not—I did not say that." Finally, according to the GPR of the 2011 Kohler interview, Kohler stated "pushing and shoving happened between the two groups." Third, in 2012 before the special grand jury, Kohler testified that he did not believe that statement was accurate: "I believe I stated that they were arguing, but I don't think I said anything about pushing or shoving at that point."

Additionally, although Gilger and Spanos' concluding case supp in 2011 states that Koschman yelled "Fuck you! I'll kick your ass," this precise language is not supported by any of the interviews in either 2004 or 2011. Indeed, Gilger and Spanos incorporated this misstated and unattributed quote into their 2011 concluding case supp, without making it clear who provided it or when. The closest source for this language appears to be a statement recorded in Yawger's interview of Kevin McCarthy on May 19, 2004, during which Kevin McCarthy stated "at this time the primary kid (Koschman) and another kid were still swearing, calling himself [McCarthy], Craig [Denham], and Richard [Vanecko] names, and saying things like 'I'll kick your ass,' etc." Kevin McCarthy never provided a statement to Gilger and Spanos, and to the extent Gilger and Spanos were relying on a paraphrased statement from Kevin McCarthy made not to them, but rather to the 2004 CPD detectives, the trustworthiness of that statement is undermined by the fact that Kevin McCarthy lied to CPD in 2004 on at least two occasions.

Finally, Gilger and Spanos' concluding case supp did not relate the fact that in his 2011 interview, Allen, one of only two people at the scene of the incident who saw the physical contact between Vanecko and Koschman, stated that Vanecko and his group "were the aggressors." Allen's statement undermines CPD's 2011 determination that Vanecko acted in

self-defense. Even Gilger himself acknowledged during his special grand jury testimony in 2013 that the failure to include this particular statement from Allen in the concluding case supp was a fairly important omission that was contrary to CPD's 2011 determination that Vanecko acted in self-defense.

ii. Dept. Chief Andrews, Cmdr. Salemme and Sgt. Cirone

The Special Prosecutor's investigation identified limited evidence that was arguably consistent with a theory that certain CPD commanding officers engaged in criminal activity, with requisite criminal intent, to manufacture a phony self-defense determination. As detailed above in Section IV., C., the Special Prosecutor obtained two versions of Gilger and Spanos' concluding case supp—an initial draft from on or about February 11, 2011, and the final draft from on or about February 28, 2011. The earlier draft made no mention of self-defense, while the later draft concluded that Vanecko had acted in self-defense. Furthermore, the Special Prosecutor obtained e-mails sent during the time in between these two drafts (February 27, 2011) in which Andrews and Cirone discussed "corrections" related to the subject matter of self-defense. Salemme was copied on one of these e-mails.

iii. The Special Prosecutor's Decision Not to Seek Charges Against Det. Gilger, Det. Spanos, Dept. Chief Andrews, Cmdr. Salemme, and Sgt. Cirone

Because of their direct involvement in handling CPD's 2011 re-investigation of the Koschman case, the OSP focused on the acts of Gilger, Spanos, Andrews, Salemme and Cirone in evaluating whether any state law criminal wrongdoing occurred. Andrews and Salemme voluntarily cooperated with the OSP's investigation, Cirone was interviewed by the OSP pursuant to a proffer agreement and Gilger and Spanos were compelled to testify pursuant to court-ordered "use immunity."

During the course of his investigation, it became apparent to the Special Prosecutor that in order to understand what happened during CPD's 2011 re-investigation of the Koschman case, the special grand jury would have to hear testimony from the detectives who handled the 2011 re-investigation. Because those detectives, Gilger and Spanos, refused to testify voluntarily before the special grand jury based upon their Fifth Amendment privilege, the OSP thought it

was necessary, in order to fulfill Judge Toomin's mandate, to seek court-ordered "use immunity" to compel their testimony.⁸⁴⁸

Concerning the evidence against Gilger and Spanos, all the issues identified by the Special Prosecutor are, *at most*, slight circumstantial evidence of wrongdoing—that is, none directly proves that either detective broke the law. During their testimony before the Special Grand Jury, both Gilger and Spanos characterized their February 11, 2011 draft case supp as "just a draft." Gilger further explained to the special grand jury that he "do[es not] always put everything in there that I ultimately want to have in the report. . . . There were things I was going to add, and there was [sic] probably things I was going to take out, you know. But at that point when I typed it in, that's what I had so far." Gilger also explained to the special grand jury that although he had not yet included anything about self-defense, he was planning on doing so. Overall, both Gilger's and Spanos' special grand jury testimony indicates that the inclusion in the February 28, 2011 concluding case supp that Vanecko had acted in self-defense was their own (and not influenced by their commanding officers).

As for the evidence against Andrews, Salemme, and Cirone, none directly proves that any of these individuals violated Illinois law. In addition, these officers provided plausible non-criminal explanations for why they sent the "corrections" e-mails. During his interview with the OSP, Cirone stated he sent the e-mails because supervisor approval is a routine requirement for exceptionally clear/closing a case, stating that in such instances it must be reviewed by a commander "up the food chain". Additionally, Cirone could not identify who actually crafted the language contained in the "corrections" e-mails. Further, Cirone told the OSP that Gilger was with him in his office when Cirone sent the "corrections" e-mails, and that he used his personal e-mail account because "it was probably the account [he] had open" – the OSP discovered nothing to contradict these assertions. Andrews also corroborated Cirone's story when interviewed by the OSP, explaining that the e-mail exchange would have been part of the review process for the report. With regard to the substance of the changes, Andrews told the OSP he "probably asked for some minor changes," including that the case supp narrative be more specific and document the exchange between Koschman and Vanecko. Furthermore, when interviewed by the OSP, Salemme could not recall the single "corrections" e-mail that he

⁸⁴⁸ See footnote 25, *supra*, regarding grants of immunity.

received, nor did he know why those specific corrections were being suggested, but he did say his editing of the report was limited to only minor issues – such as spelling and typos.

Significantly, the Special Prosecutor's investigation was unable to locate any drafts of Gilger's report between the February 11, 2011 draft narrative and the February 27, 2011 e-mail with "corrections," sent 16 days later. As a result, it is unclear which version Andrews and Salemme may have edited. As stated above, the February 11, 2011 draft lacked any mention of self-defense — the subject of one of the "corrections" in the February 27, 2011 e-mail. Thus, the precise extent of Andrews' or Salemme's edits are unknown and could not be proved.

Therefore, it is the Special Prosecutor's opinion that he cannot prove beyond a reasonable doubt that Gilger, Spanos, Andrews, Salemme or Cirone engaged in criminal activity, with requisite criminal intent, to manufacture a phony self-defense determination.⁸⁴⁹

b. Whether the Facts and Circumstances Surrounding Lt. Walsh's 2011 Discovery of the Missing CPD Original Koschman Homicide File Amount to Criminal Misconduct

As discussed above in Section IV, C. 7., at CPD, every homicide case is supposed to have a corresponding permanent master homicide case file, and at Area 3, homicide files were primarily stored on a bookcase and in file cabinets located in the sergeants' office where they were indefinitely retained until the case was closed. But, that was not the case for the original Koschman homicide file.

As we now know, after CPD received the January 4, 2011 *Sun-Times* FOIA request surrounding the Koschman case, Andrews ordered Area 3 to gather the original Koschman homicide file so it could be provided to those at Area 5 who would be handling the 2011 CPD re-investigation. In response, Yamashiroya and Walsh searched for, but could not find, the original Koschman homicide file. In fact, it was not until June 29, 2011, four months after Gilger and Spanos finished Area 5's re-investigation, that Walsh reportedly found the original Koschman homicide file.

The Special Prosecutor's investigation identified certain evidence that is arguably consistent with the theory that the facts and circumstances surrounding Walsh's 2011 discovery

⁸⁴⁹ The OSP has concluded that the facts and testimony do not objectively establish self-defense, which issue will be addressed at Vanecko's trial. This conclusion, however, does not mean that the OSP can prove beyond a reasonable doubt that CPD personnel's incorrect interpretation of facts and testimony as it relates to self-defense constitutes criminal obstruction of justice.

of the missing CPD original Koschman homicide file amount to criminal misconduct. That evidence is discussed below.

i. Lt. Walsh's Discovery of the Original Koschman Homicide File (Blue Three-Ring Binder)

To begin, and as discussed in detail above, through events which all occurred in 2011, Walsh was tied to three other files at issue in this case besides his June 29, 2011 discovery of the original CPD Koschman homicide file, specifically: (1) Yamashiroya told the OSP that Walsh was present in January 2011, when Yamashiroya discovered the Koschman “credenza file” (*see* Section IV., C., 7., b., i.); (2) Yawger was visiting Walsh at Area 3 on June 30, 2011, when he (Yawger) discovered his Koschman “working file” in the detective locker room (*see* Section IV., C., 7., b., iii.); and (3) Clemens, sometime between late February 2011 and late July 2011, allegedly found and immediately turned over to Walsh another version of the Koschman homicide file he found at Area 3 (*see* Section IV., C., 7., b., iv.).

In following up on Walsh’s connection to the four files at issue, the Special Prosecutor and his office further discovered that Walsh reportedly found the original Koschman homicide file conspicuously displayed (a blue binder surrounded by only white binders) on a wooden shelf in Area 3’s sergeants’ office (an area that had been searched numerous times previously). While certainly possible, it is somewhat improbable that Walsh would ultimately find the original Koschman homicide file in Area 3’s sergeants’ office – a small room that is frequently occupied by CPD sergeants, often 24 hours a day.

In addition, it seemed counterintuitive to the Special Prosecutor and his office that Walsh would not have wanted to memorialize in writing (thus providing him an avenue in which his story could independently be corroborated) that he was not alone when he discovered the missing Koschman homicide file (the most critical and sought-after police file from a “heater case” which had already received scrutiny both inside and outside of CPD). Be that as it may, it was not until the OSP’s questioning of Walsh in August 2013 that, likely for the first time,⁸⁵⁰ Walsh

⁸⁵⁰ During his interview with the OSP, Walsh stated that when he first reported the discovery of the blue binder to Yamashiroya he informed Yamashiroya that Flaherty was in the sergeants’ office when he found the blue binder. However, Yamashiroya told the OSP that he does not remember Walsh ever telling him that anyone else was present in the sergeants’ office when he discovered the missing Koschman homicide file. Indeed, according to Yamashiroya, had he known someone else besides Walsh was present in the sergeants’ office at the exact moment Walsh found the binder, he would have suggested that fact be included in the Walsh to Byrne June 30, 2011 memorandum.

mentioned he was not alone at the moment he found the Koschman homicide file, but rather was with Flaherty (his former CPD partner and close friend). Indeed, Walsh's June 30, 2011, memorandum to Byrne in which he memorialized his June 29, 2011 finding of the Koschman homicide file neglected to mention Flaherty's presence. Instead, Walsh told the OSP that, in his opinion, there was no reason to mention that Flaherty was with him.

Furthermore, even though Walsh was instructed by a superior to file the July 20, 2011, IAD complaint (which alleged that the original Koschman homicide file that was "believed to have been lost was obviously not lost" and instead had been "removed and returned in violation of department rules and regulations" by an "Unknown Chicago Police Officer"), he himself demonstrated an apparent lack of forthrightness during IAD's investigation – behavior more likely expected by a person who sees himself as a target of the investigation, as opposed to that of a person who filed the complaint initiating the investigation. For example, during Walsh's August 24, 2011 IAD interview regarding the disappearance and ultimate discovery of the Koschman homicide file, he once again did not disclose that Flaherty was in the sergeants' office on June 29, 2011 at the moment he (Walsh) discovered the file. Walsh told the OSP that in his opinion, unless specifically asked, "you don't volunteer things" to IAD.

ii. The Special Prosecutor's Decision Not to Seek Charges Against Lt. Walsh

For several reasons, the Special Prosecutor determined he would not be able to prove beyond a reasonable doubt at trial that Walsh recklessly, knowingly, or intentionally violated Illinois law during his participation in the Koschman matter in 2011. Because Walsh refused to voluntarily be interviewed by the OSP, the OSP thought it was necessary, in order to fulfill Judge Toomin's mandate, to conduct his interview pursuant to a proffer agreement.

During the course of the Special Prosecutor's investigation, their was not a single witness or document discovered by the OSP that directly contradicted Walsh's statement that he actually and honestly found (i.e., without any nefarious orchestration of events) the missing original Koschman homicide file on June 29, 2011. While the 2013 special grand jury testimony of Det. Clemens, as detailed above in Section IV., C., 7., b., iv., arguably undermines the truthfulness of Walsh's statements regarding his June 29, 2011 discovery of the original Koschman homicide file, Clemens' testimony has not been substantiated by others, was denied by Walsh, and the binder Clemens allegedly found (which Clemens described to the special grand jury as a blue

hardcover “flip binder”, as opposed to the blue three-ring binder Walsh found) has never been discovered by CPD, SAO, IGO, or the OSP. Furthermore, even though Walsh told the OSP that after finding the original Koschman homicide file that he took it to his house for some period of time to store for safekeeping in his personal safe, there is no way for the OSP to determine what documents in the binder (e.g., GPRs), if any, may have been altered, added, or removed by Walsh.

Additionally, the OSP interviewed Flaherty in order to see whether he would corroborate Walsh’s statement that Flaherty was with Walsh when he (Walsh) found the original Koschman homicide file. During his interview with the OSP, Flaherty substantiated Walsh’s statement, and explained that he was indeed in the sergeants’ office when Walsh retrieved a blue binder from the bookshelf, which Walsh immediately told him was the missing Koschman homicide file. In an attempt to independently verify Flaherty’s statement, the OSP reviewed CPD records and determined that Flaherty, a sergeant, was in fact assigned to Area 3 and working the third watch on June 29, 2011. Moreover, the OSP, in yet a further attempt to corroborate or potentially disprove both Walsh’s and Flaherty’s statements made to the OSP that they were together in Area 3’s sergeants’ room on June 29, 2011 at the precise moment Walsh found the missing homicide file,⁸⁵¹ sought cell phone records and cell phone tower information via special grand jury subpoenas and court orders. The available responsive records the OSP received and reviewed in response to these efforts did not contradict the statements Walsh or Flaherty made to the OSP when interviewed in 2013.

The Special Prosecutor and his office agree with what former Deputy Superintendent Peterson explained during his interview with the OSP—that common sense dictates that someone had to have placed the blue binder Koschman homicide file on the shelf (next to all the white binders) knowing it would be found. However, without any actual testimonial or documentary evidence demonstrating that Walsh played some nefarious role in arranging his discovery of the original Koschman homicide file (or perhaps that he earlier prevented its discovery, or perhaps altered the file in some fashion after its discovery), there is nothing close to proof beyond a reasonable doubt that would support charges against Walsh. Therefore charges are not warranted.

⁸⁵¹ According to Walsh’s June 30, 2011 memorandum, he found the missing original Koschman homicide file at exactly 9:39 p.m., on June 29, 2011.

c. The Special Prosecutor's Decision Not to Seek Charges Against Any Employee of SAO

Lastly, the Special Prosecutor identified no evidence of any kind suggesting that any employee of SAO recklessly, knowingly, or intentionally violated Illinois law during their participation in the Koschman matter in 2011 and 2012. As such, charges were not sought.

VI. CONCLUSION

The evidence discussed in this report supports the findings by Judge Toomin in his April 6, 2012, Memorandum of Opinion and Order in which he decided to appoint a special prosecutor, wherein he stated:

Section 7-1 of the Illinois Criminal Code provides:

'A person is justified in the use of force against another when and to the extent that he reasonably believes that such conduct is necessary to defend himself or another against such other's imminent use of unlawful force. However, he is justified in the use of force which is intended or likely to cause death or great bodily harm only if he reasonably believes that such force is necessary to prevent imminent death or great bodily harm to himself or another, or the commission of a forcible felony.' 720 ILCS 5/7-1 (West 2002).

Inherent in the ability to raise a legitimate claim of justifiable force is the requirement that a person seeking to avail himself of the defense be able to present some evidence of six salient factors, to wit: (1) force was threatened against a person; (2) the person threatened was not the aggressor; (3) the danger of harm was imminent; (4) the threatened force was unlawful; (5) the person actually and subjectively believed a danger existed that required the use of force applied; and (6) the person's beliefs were objectively reasonable. *People v. Jeffries*, 164 Ill. 2d 104, 127-28, 646 N.E.2d 587, 598 (1995); *People v. Lee*, 311 Ill. App. 3d 363, 367, 724 N.E.2d 557, 561 (2000).

Here, the viability of the self-defense claim imputed to Vanecko by the police and [SAO] rests solely upon the oft-repeated conclusion that Koschman was the aggressor. Yet, that determination derives from conflicting statements provided by Koschman's companions as well as independent witnesses suggesting that Koschman was verbally rather than physically aggressive. Vanecko's friends provided no meaningful insight, claiming their backs were turned

when Koschman was struck. However, even assuming Koschman was the aggressor, that determination should only be the start of the inquiry. Adherence to the salient factors noted would have been far more telling. First, there is no credible evidence that Koschman employed any physical force against Vanecko. On the contrary, the quoted materials from the [IGO] investigation incorporated in petitioners' reply clearly undermine that claim. Second, there is only conflicting evidence that Koschman was the aggressor, albeit verbally. Third, there is no indication that there was any danger of imminent harm to Vanecko, particularly given the disparity in size between himself (6'3", 230 pounds) and Koschman (5'5", 140 pounds). Fourth, the submissions before this court are barren of any suggestion, much less evidence, that Vanecko actually and subjectively believed that a danger existed that required the use of force he applied. If nothing else, one aspect of the police investigation is uncontested, no police officer or [SAO] prosecutor ever interviewed or spoke to Vanecko. In fact, Detective Yawger, in an interview with the *Sun-Times*, lamented how Vanecko's attorney frustrated his efforts to speak with his client after initially promising Yawger that Vanecko would talk to investigators.

Yet, it is the existence of a person's subjective belief that the evidence must show. *People v. Malvin Washington*, Ill. Sup. Ct., No. 110283, January 20, 2012 ¶ 48. In the absence of such evidence, an objective observer might well express amazement as to how the police or [SAO] could so blithely divine the subjective feelings of Vanecko. Clearly, they could not. Under these circumstances, the public could well conclude that the entire claim of self-defense came not from Vanecko, but, rather, was conjured up in the minds of law enforcement. A discerning citizen could well surmise that it simply is an argument made of whole cloth. Whether Vanecko may, in fact, have a valid claim of self-defense should properly be for him to raise, not the police.

[SAO's] concurrence in what one might charitably characterize as a rather creative exercise of the police investigative processes offers little confidence in [SAO's] ability to conduct the kind of objective 'fresh look' that this matter requires. This is not to suggest that there is merit to petitioners' claim of political or personal interest. Nonetheless, [SAO's] efforts to denigrate the evidence against Vanecko, coupled with [SAO's] recurring calls for an independent investigation evokes a decided interest in the matter sufficient to warrant appointment of a special prosecutor.⁸⁵²

⁸⁵² Order by J. Toomin at 30-32, Apr. 6, 2012.

VII. WINSTON & STRAWN INVESTIGATIVE PERSONNEL

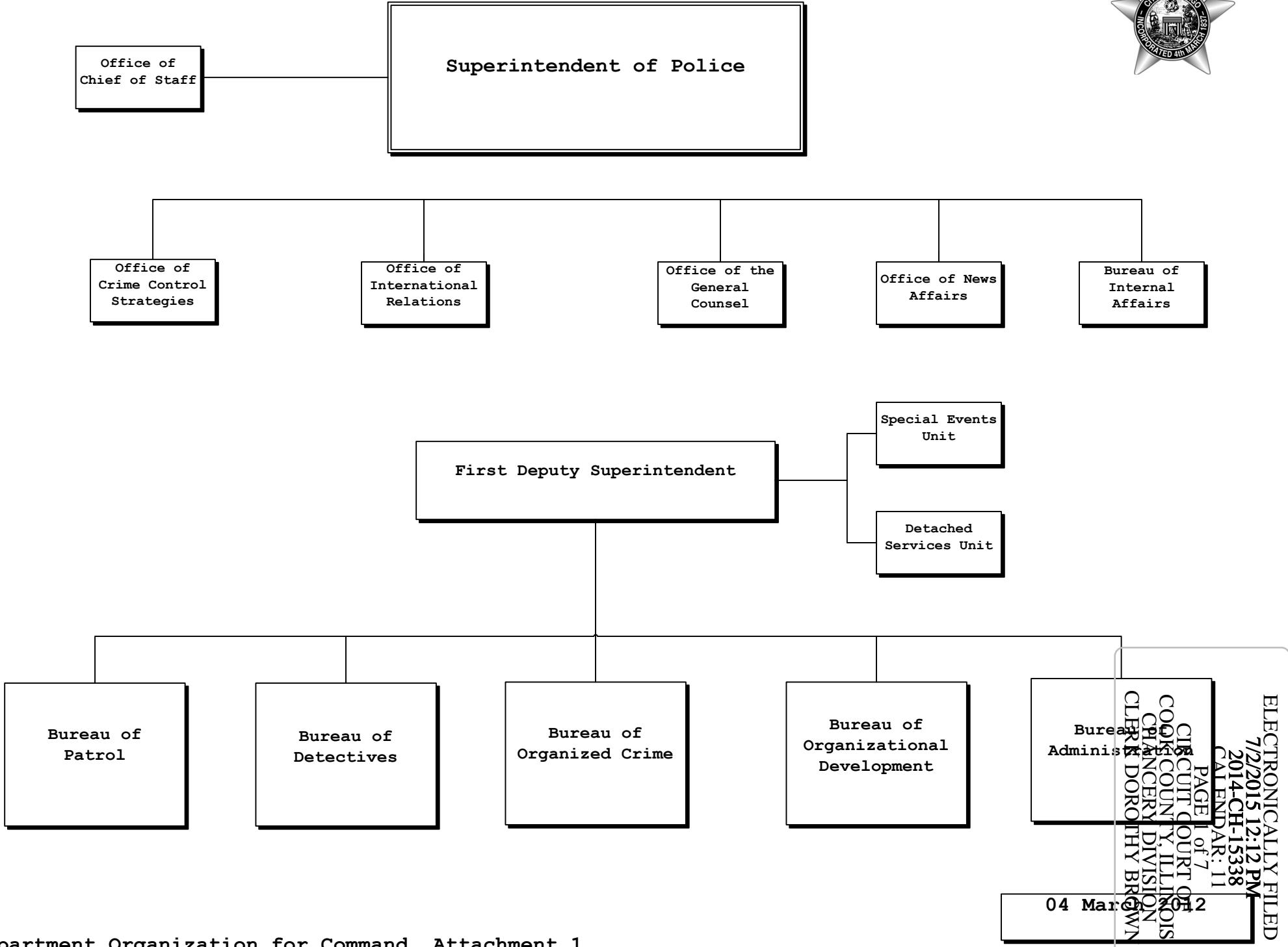
Special Prosecutor Dan K. Webb is the Chairman of Winston & Strawn LLP, and the former United States Attorney for the Northern District of Illinois. This matter is the fourth time Mr. Webb has served as a special prosecutor.

Mr. Webb was principally assisted in the investigation by Winston & Strawn attorneys and Deputy Special Prosecutors Stephen J. Senderowitz, Daniel D. Rubinstein, Derek J. Sarafa, Matthew J. Hernandez, and Sean G. Wieber. Mr. Senderowitz is a former Assistant United States Attorney and has previously served as a deputy special prosecutor on another matter. Mr. Rubinstein is a former Assistant United States Attorney.

In addition, valuable assistance was provided by other Winston & Strawn attorneys, including: Jennifer L. Bekkerman, Andrew C. Erskine, Matthew R. Carter, Thomas G. Weber, Shannon T. Murphy, Jared L. Hasten, Solana P. Flora, and Katherine V. Boyle.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 169 of 169

CHICAGO POLICE DEPARTMENT - ORGANIZATIONAL OVERVIEW

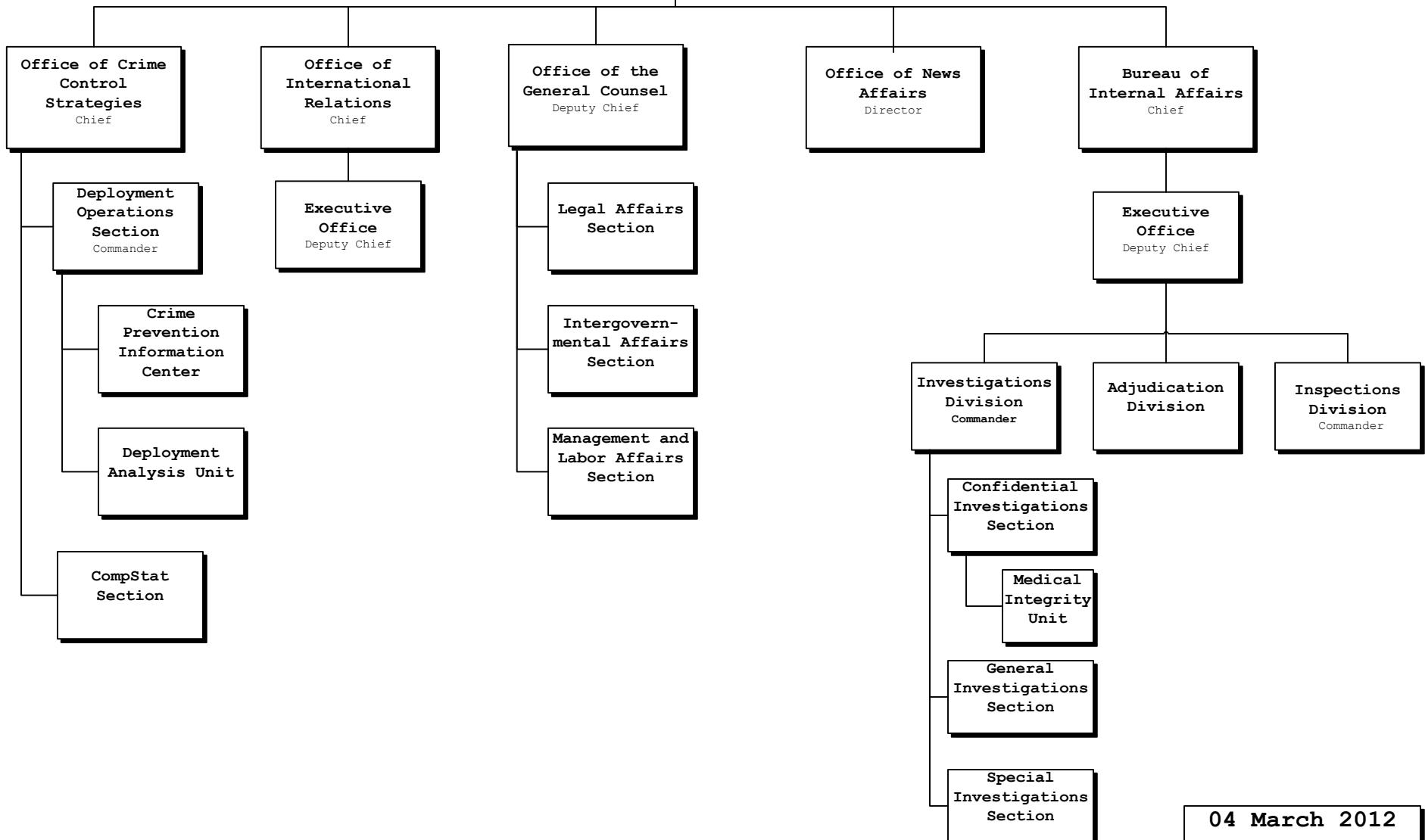


OFFICE OF THE SUPERINTENDENT

ELECTRONICALLY FILED

7/2/2015 12:12 PM

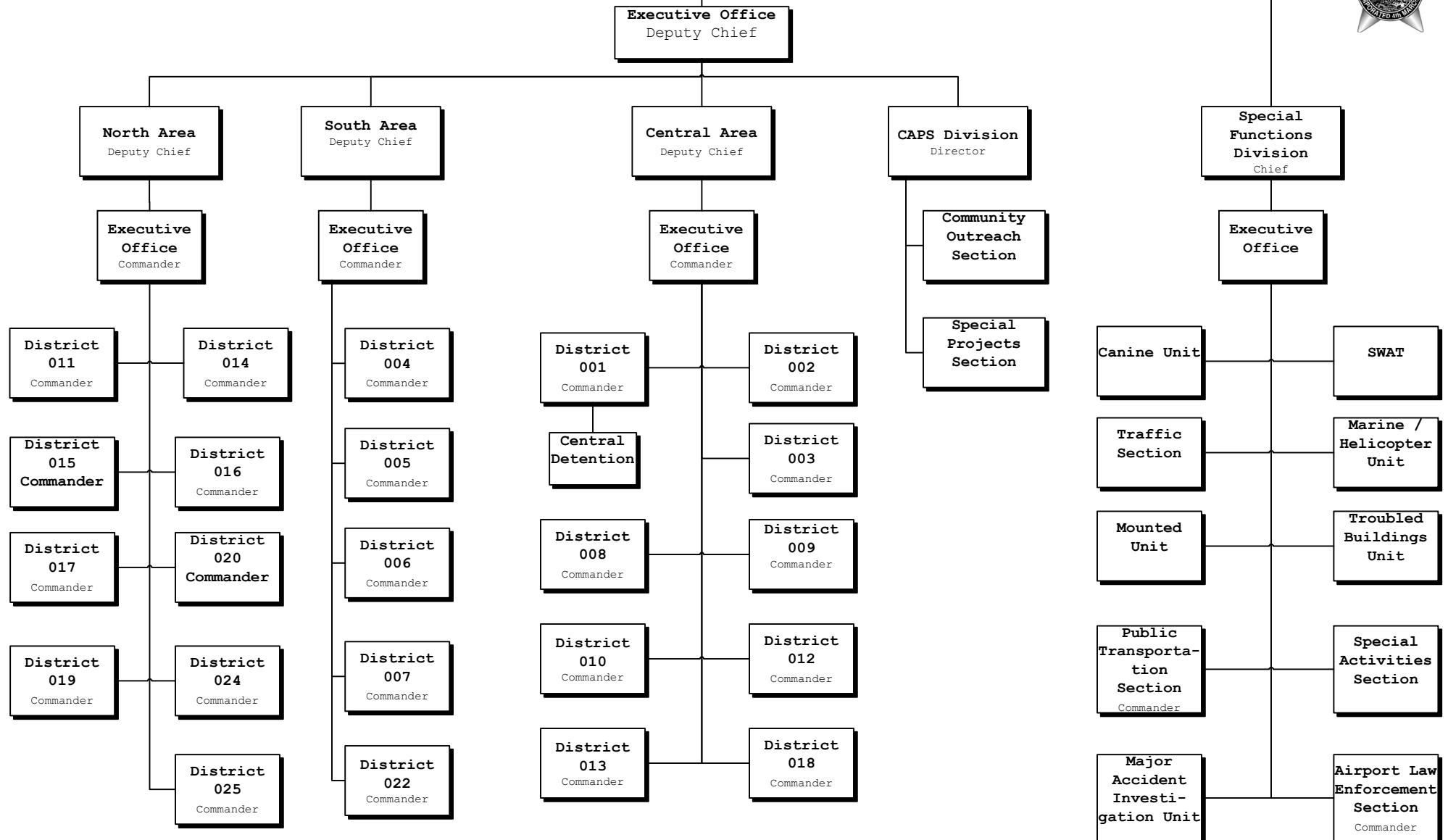
2014-CH-15338
PAGE 2 of 7
**Superintendent of
Police**



04 March 2012

BUREAU OF PATROL

ELECTRONICALLY FILED
7/2/2015 12:12 PM
Bureau of Patrol
2014-CH-15338
Chief
PAGE 3 of 7



Department Organization for Command,
Attachment 3

04 March 2012
(v.b)

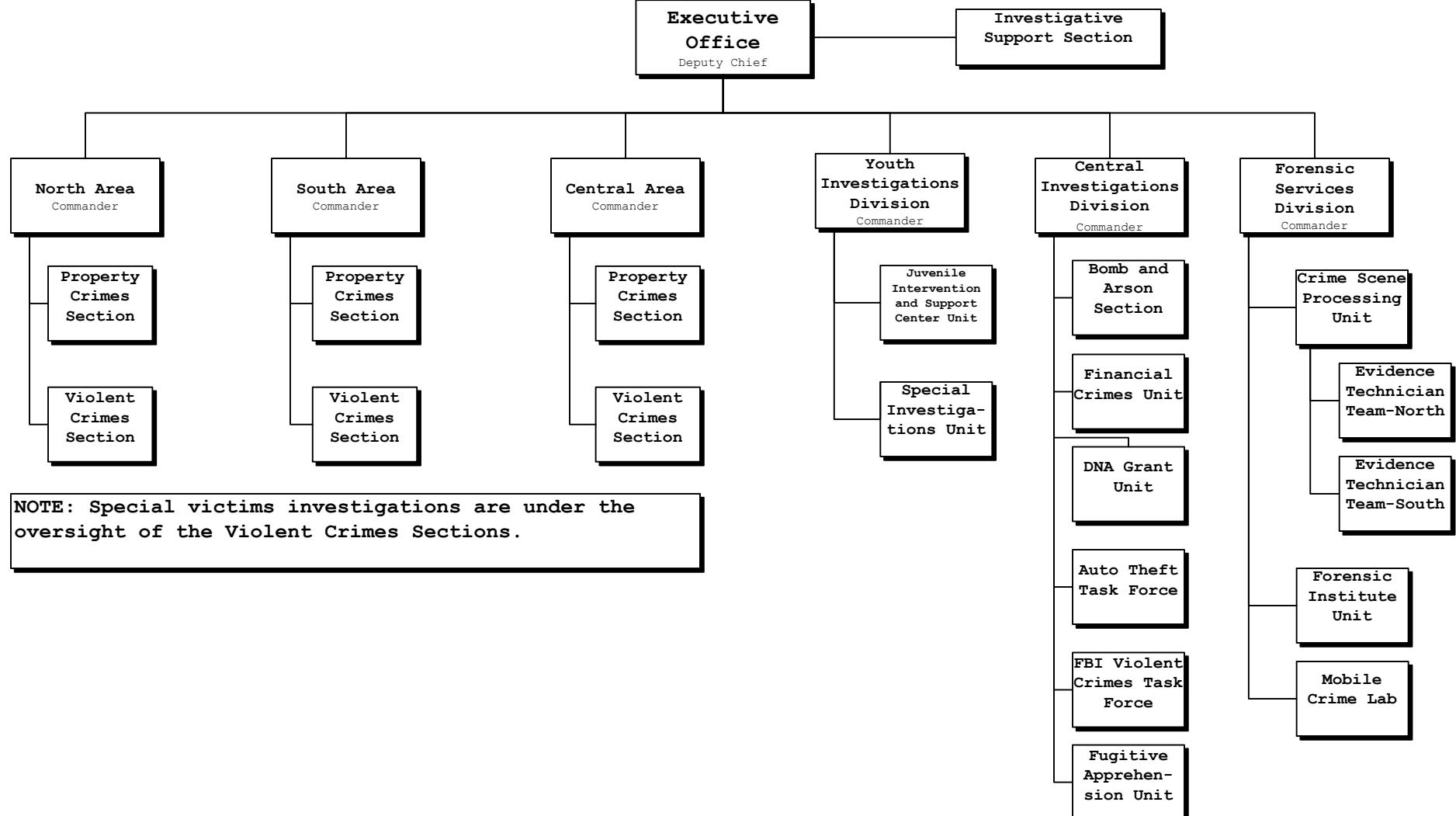
BUREAU OF DETECTIVES

ELECTRONICALLY FILED

7/2/2015 12:12 PM

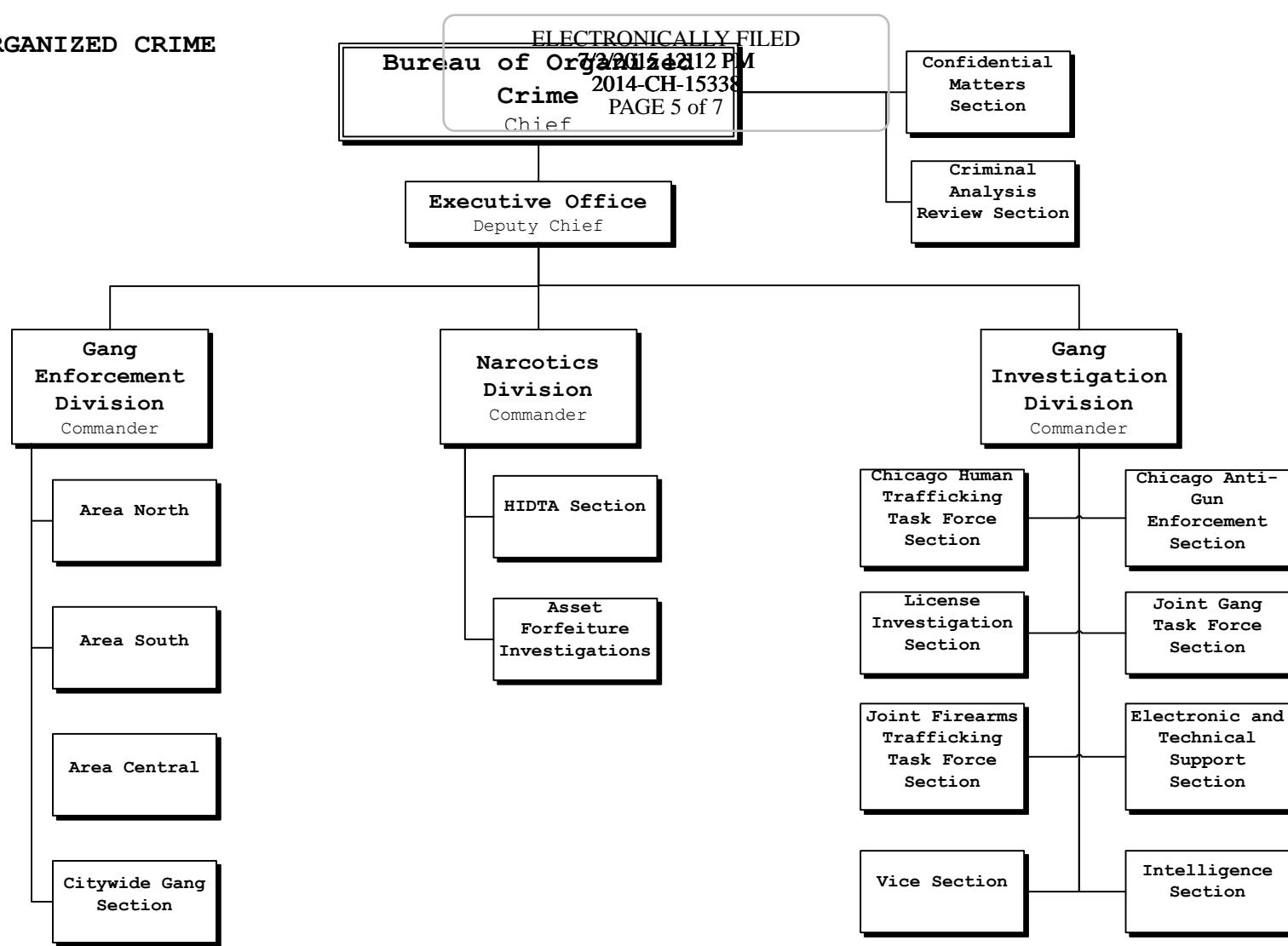
Bureau of Detectives

PAGE 4 of 7



NOTE: Special victims investigations are under the oversight of the Violent Crimes Sections.

ELECTRONICALLY FILED
 Bureau of Organized Crime Chief
 04/04/2012 12 PM
 2014-CH-15338
 PAGE 5 of 7



04 March 2012

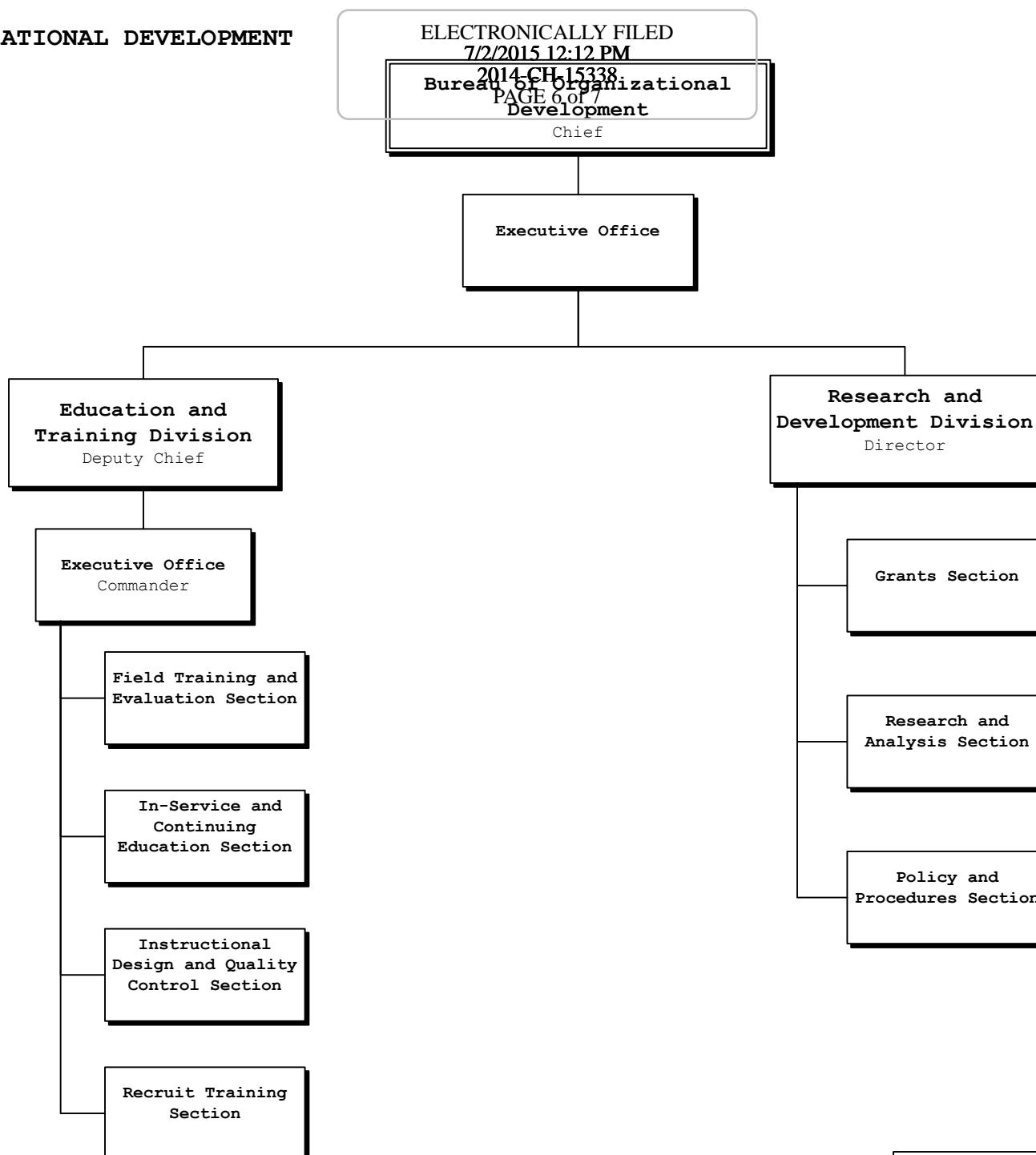
BUREAU OF ORGANIZATIONAL DEVELOPMENT

ELECTRONICALLY FILED

7/2/2015 12:12 PM

2014-CH-15338
Bureau of Organizational
Development

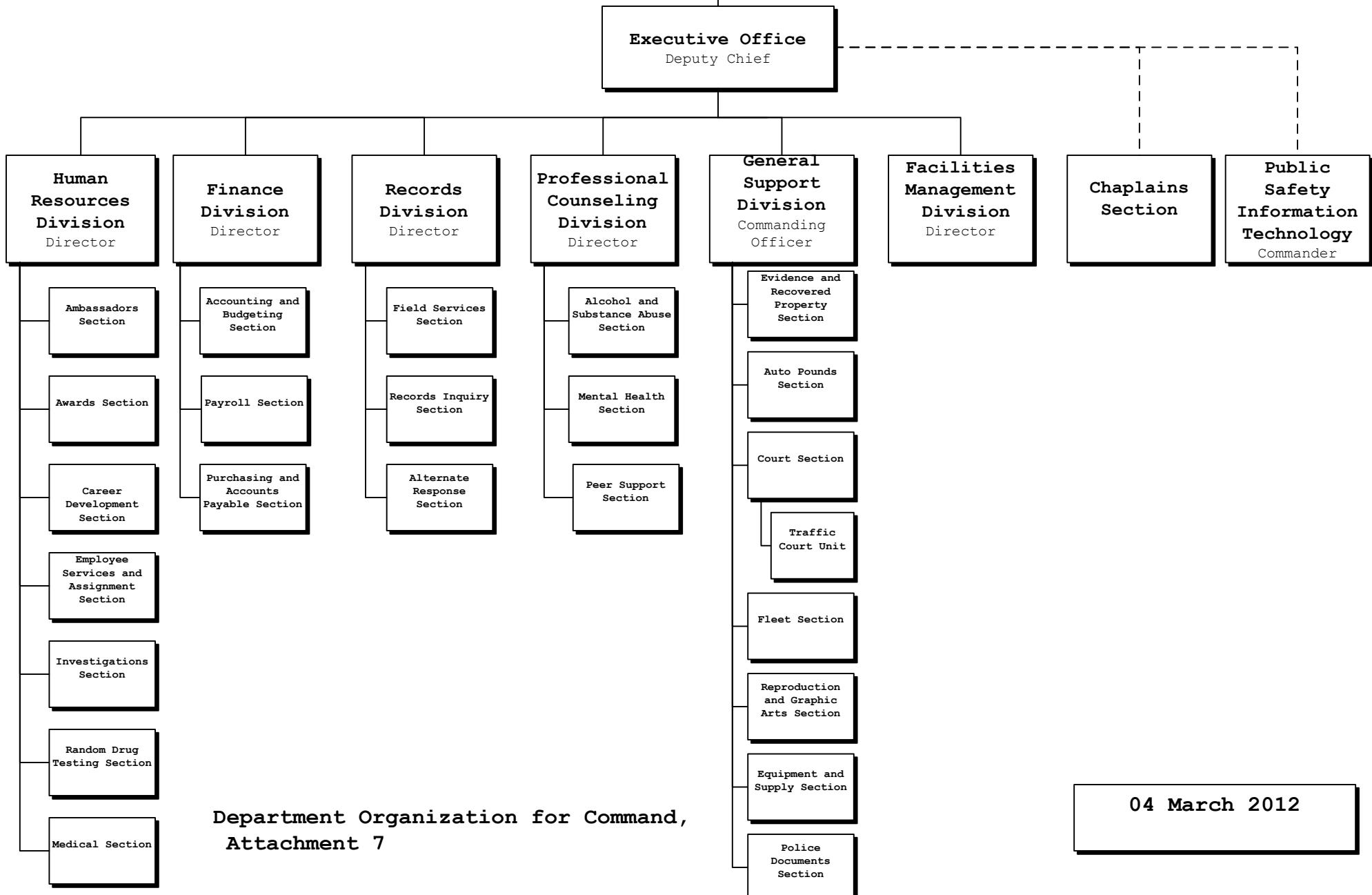
Chief



04 March 2012

BUREAU OF ADMINISTRATION

ELECTRONICALLY FILED
7/2/2015 12:12 PM
Bureau of Administration
PAGE 7 of 7



[Home](#)
[About DDTC](#)
[Getting Started](#)
[Registration](#)
[DTAS-Online](#)
[DTrade](#)
[Licensing](#)
[Compliance](#)
[Export Control Reform](#)
[Commodity Jurisdiction](#)
[Response Team](#)
[Regulations and Laws](#)

[Laws](#)
[Proposed Rules](#)
[Country Policies and Embargoes](#)
[Treaties](#)
[FAQs](#)
[Outreach](#)
[Metrics](#)
[Reports](#)
[Federal Register Notices](#)
[Links to Other Web Sites](#)
[DTAG](#)
[Miscellany](#)

[DDTC Homepage](#) / [Regulations and Laws](#) / The International Traffic in Arms Regulations (ITAR)

The International Traffic in Arms Regulations (ITAR)

The Department of State is responsible for the export and temporary import of defense articles and services governed by 22 U.S.C. 2778 of the Arms Export Control Act ("AECA"; see the [AECA Web page](#)) and Executive Order 13637. The International Traffic in Arms Regulations ("ITAR," 22 CFR 120-130) implements the AECA. The ITAR is available from the Government Printing Office (GPO) as an annual hardcopy or e-document publication as part of the Code of Federal Regulations (CFR) and as an updated e-document.

UPDATED ITAR:

The Electronic Code of Federal Regulations (e-CFR) is a regularly updated, unofficial editorial compilation of CFR material and amendments published in the Federal Register. The updated, but unofficial, version of the ITAR provided by e-CFR is linked below.

[ITAR Part 120 - Purpose and Definitions](#)
[ITAR Part 121 - The United States Munitions List](#)
[ITAR Part 122 - Registration of Manufacturers and Exporters](#)
[ITAR Part 123 - Licenses for the Export of Defense Articles](#)
[ITAR Part 124 - Agreements, Off-Shore Procurement and Other Defense Services](#)
[ITAR Part 125 - Licenses for the Export of Technical Data and Classified Defense Articles](#)
[ITAR Part 126 - General Policies and Provisions](#)
[ITAR Part 127 - Violations and Penalties](#)
[ITAR Part 128 - Administrative Procedures](#)
[ITAR Part 129 - Registration and Licensing of Brokers](#)
[ITAR Part 130 - Political Contributions, Fees and Commissions](#)

OFFICIAL ITAR: ANNUAL EDITION

The annual edition of the ITAR (directly below) is published every April 1. It does not contain amendments to the ITAR that take effect between annual publications. Those [amendments](#) are published in the *Federal Register* (see further below).

[ITAR Part 120 - Purpose and Definitions](#) (PDF, 223KB)
[ITAR Part 121 - The United States Munitions List](#) (PDF, 407KB)
[ITAR Part 122 - Registration of Manufacturers and Exporters](#) (PDF, 192KB)
[ITAR Part 123 - Licenses for the Export of Defense Articles](#) (PDF, 245KB)
[ITAR Part 124 - Agreements, Off-Shore Procurement and Other Defense Services](#) (PDF, 218KB)
[ITAR Part 125 - Licenses for the Export of Technical Data and Classified Defense Articles](#) (PDF, 200KB)
[ITAR Part 126 - General Policies and Provisions](#) (PDF, 358KB)
[ITAR Part 127 - Violations and Penalties](#) (PDF, 216KB)
[ITAR Part 128 - Administrative Procedures](#) (PDF, 200KB)
[ITAR Part 129 - Registration and Licensing of Brokers](#) (PDF, 203KB)
[ITAR Part 130 - Political Contributions, Fees and Commissions](#) (PDF, 197KB)

AMENDMENTS TO THE ITAR:

Amendments to the ITAR are published in the *Federal Register*. While every effort is made by DDTC to keep the listing of ITAR amendments current on this page, please consult the *Federal Register* for the official record of amendments.

[80 FR 30614 - Final Rule: Amendment to the International Traffic in Arms Regulations: Policy on Exports to the Republic of Fiji](#) (PDF, 217KB)
[79 FR 45089 - Final Rule: Amendment to the International Traffic in Arms Regulations: Central African Republic and UNSCR 2149](#) (PDF, 201KB)
[79 FR 37536 - Final Rule: Amendment to the International Traffic in Arms Regulations: United States Munitions List Category XI \(Military Electronics\), and Other Changes](#) (PDF, 389KB)
[79 FR 36393 - Final Rule, Correction: Amendment to the International Traffic in Arms Regulations: Third Rule Implementing Export Control Reform; Correction](#) (PDF, 273KB)
[79 FR 27180 - Interim Final Rule: Amendment to the International Traffic in Arms Regulations: Revision of U.S. Munitions List Category XV](#) (PDF, 288KB)

[79 FR 21616 - Final Rule: Amendment to the International Traffic in Arms Regulations: Central African Republic \(PDF, 201KB\)](#)[79 FR 21616 - Final Rule: Amendment to the International Traffic in Arms Regulations: Changes to Authorized Officials and the UK Defense Trade Treaty Exemption; Correction of Errors in Lebanon Policy and Violations; and Adoption of Recent Amendments as Final; Correction \(PDF, 201KB\)](#)[79 FR 8082 - Final Rule: Amendment to the International Traffic in Arms Regulations: Changes to Authorized officials and the UK Defense Trade Treaty Exemption; Correction of Errors in Lebanon Policy and Violations; and Adoption of Recent Amendments as Final \(PDF, 225KB\)](#)[79 FR 34 - Final Rule: Amendment to the International Traffic in Arms Regulations: Third Rule Implementing Export Control Reform \(PDF, 304KB\)](#)[79 FR 26 - Final Rule; Correction: Amendment to the International Traffic in Arms Regulations: Continued Implementation of Export Control Reform; Correction \(PDF, 301KB\)](#)[78 FR 61750 - Final Rule; Correction: Amendment to the International Traffic in Arms Regulations: Initial Implementation of Export Control Reform; Correction \(PDF, 416KB\)](#)[78 FR 52680 - Interim Final Rule: Amendment to the International Traffic in Arms Regulations: Registration and Licensing of Brokers, Brokering Activities, and Related Provisions \(PDF, 280KB\)](#)[78 FR 47179 - Final Rule: Amendment to the International Traffic in Arms Regulations: Libya and UNSCR 2095 \(PDF, 221KB\)](#)[78 FR 40922 - Final Rule: Amendment to the International Traffic in Arms Regulations: Continued Implementation of Export Control Reform \(PDF, 418KB\)](#)[78 FR 40630 - Final Rule: Amendment to the International Traffic in Arms Regulations: Canadian Firearms Components Exemption \(PDF, 207KB\)](#)[78 FR 32362 - Final Rule: Implementation of the Defense Trade Cooperation Treaty Between the United States and Australia; Announcement of Effective Date for Regulations \(PDF, 196KB\)](#)[78 FR 22740 - Final Rule: Amendment to the International Traffic in Arms Regulations: Initial Implementation of Export Control Reform \(PDF, 291KB\)](#)[78 FR 21523 - Final Rule: Implementation of the Defense Trade Cooperation Treaty Between the United States and Australia \(PDF, 306KB\)](#)

[Directorate of Defense Trade Controls](#) | [Office of Defense Trade Controls Compliance](#) | [Office of Defense Trade Controls Licensing](#) | [Office of Defense Trade Controls Policy](#) | [Office of Defense Trade Controls Management](#)

The Office of the Executive Director, Technology Division, Bureau of International Security and Nonproliferation (ISN/EX/TD), manages this site as a source of information from the Directorate of Defense Trade Controls, Bureau of Political-Military Affairs, U.S. Department of State. External links to other Internet sites should not be construed as an endorsement of the views or privacy policies contained therein.

[Contact Information](#) | [Site Map](#) | [Privacy Notice](#) | [Copyright Information](#)

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 2 of 2

STATE OF NEW YORK
SUPREME COURT : COUNTY OF ERIE

In the Matter of

NEW YORK CIVIL LIBERTIES UNION,

Petitioner,

Index No. I2014-000206

-v-

ERIE COUNTY SHERIFF'S OFFICE,

Respondent.

Bradley S. Morrison, being duly sworn, deposes and states:

1. I am a Supervisory Special Agent (“SSA”) with the Federal Bureau of Investigation (“FBI”), currently assigned as the Chief, Tracking Technology Unit, Operational Technology Division (“OTD”) in Quantico, Virginia. I am over the age of 18 years and without legal disability, and if called as a witness could competently testify to the facts set forth below.

2. I have been employed as a FBI Special Agent since 1996. As Unit Chief, I am responsible for the development, procurement, deployment, and management of technical assets and capabilities to surreptitiously locate, tag, and track targets of interest in support of all FBI investigative, intelligence collection, and operational programs. I am responsible for establishing and advising on policy guidance for the FBI, including whether a particular tool or technique my program manages meets the criteria for protection as law enforcement sensitive, while ensuring that state-of-the-art technical investigative assets remain available to field technical programs to *BSM*

enable them to assist in a wide range of technical investigative missions. This includes the use and deployment of electronic surveillance devices such as cell site simulators.

2. Title 5, United States Code, Section 301 empowers the head of an executive department to set regulations that govern the dissemination of information belonging to that department. With respect to the FBI, as a component of the Department of Justice ("DOJ"), the Attorney General has promulgated 28 C.F.R. § 16.21, in which the Attorney General set forth procedures to follow upon receiving a request for information relating to material contained in the files of the department, or acquired from the department as part of one's official duties. DOJ officials are required to consider several factors in deciding whether to allow privileged information to be released, including whether disclosure of the information sought would "reveal investigatory records compiled for law enforcement purposes, and would . . . disclose investigative techniques and procedures" whose effectiveness would be impaired by disclosure. 28 C.F.R. § 16.26(b)(5).

3. The FBI protects information about the use of this technology in response to requests under the federal Freedom of Information Act ("FOIA"), 5 U.S.C. § 552. Law enforcement techniques and procedures enjoy categorical protection under FOIA Exemption 7(E), in order to preserve the utility of those techniques and procedures and mitigate the risk that they will be circumvented. 5 U.S.C. § 552(b)(7)(E). Under FOIA Exemption 7(E), the FBI protects a range of information about cell site simulators, including operational details such as how, when, where, and under what circumstances the FBI uses cell site simulators, and technical details, such as the particular technology and equipment that the FBI uses. Likewise, the FBI OTD always has asserted that cell site simulators are exempt from disclosure pursuant to the

BSM

“law enforcement sensitive” qualified evidentiary privilege, as information concerning this equipment, if made public, could easily impair the use of this investigative method.

4. Similarly, the FBI has an interest in the protection of information about the use of this technology in response to requests to local law enforcement authorities under state disclosure statutes.

5. I make this Affidavit in opposition to this action brought pursuant to Article 78 of the New York Civil Practice Laws and Rules whereby petitioner, New York Civil Liberties Union (“NYCLU”) seeks production of information about the use of this technology pursuant to New York Freedom of Information Law (“FOIL”) found in New York Public Officers Law Article 6.

6. Disclosure of even minor details about the use of cell site simulators may reveal more information than their apparent insignificance suggests because, much like a jigsaw puzzle, each detail may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself. Thus, disclosure of what appears to be innocuous information about cell site simulators would provide adversaries with critical information about the capabilities, limitations, and circumstances of their use, and would allow those adversaries to accumulate information and draw conclusions about the use and technical capabilities of this technology. In turn, this would provide them the information necessary to develop defensive technology, modify their behaviors, and otherwise take countermeasures designed to thwart the use of this technology. Disclosure would thus allow them to evade detection by law enforcement and circumvent the law.

7. In recognition of this vulnerability, the FBI has, as a matter of policy, for over 10 years, protected this electronic surveillance equipment and techniques from disclosure, directing

its agents that while the product of the identification or location operation can be disclosed, neither details on the equipment's operation nor the tradecraft involved in use of the equipment may be disclosed. The FBI routinely protects information from disclosure under FOIA and asserts the law enforcement sensitive privilege in discovery over cell site simulator equipment because discussion of the capabilities and use of the equipment in court would allow criminal defendants, criminal enterprises, or foreign powers, should they gain access to the items, to determine law enforcement's techniques, procedures, limitations, and capabilities in this area. This knowledge could easily lead to the development and employment of countermeasures to FBI tools and investigative techniques by subjects of investigations and completely disarm law enforcement's ability to obtain technology-based surveillance data in criminal investigations. This, in turn, could completely prevent the successful prosecution of a wide variety of criminal cases involving kidnappings, murder, terrorism and criminal conspiracies where cellular location is frequently used. *See United States v. Rigmaiden*, 845 F.Supp. 982 (D. Ariz. 2012); *United States v. Garey*, 2004 WL 2663023 (M.D. Ga. Nov. 15, 2004).

8. Further, the FBI has entered into a non-disclosure agreement ("NDA") with our state and local law enforcement partners, including the Erie County Sheriff's Office, which is a respondent in this action. The NDA is specific to state and local law enforcement use of cell site simulator technology, and was entered into in an effort to protect law enforcement sensitive details about the technology. The NDA acknowledges that "[d]isclosing the existence of and the capabilities provided by [cell site simulator equipment] to the public would reveal sensitive technological capabilities possessed by the law enforcement community and may allow individuals who are the subject of investigation to employ countermeasures to avoid detection by law enforcement. This would not only potentially endanger the lives and physical safety of law

BSM

enforcement officers and other individuals, but also adversely impact criminal and national security investigations. That is, disclosure of this information could result in the FBI's inability to protect the public from terrorism and other criminal activity because, through public disclosures, this technology has been rendered essentially useless for future investigations. In order to ensure that [cell site simulator equipment] continues to be available for use by the law enforcement community, the equipment/technology and any information related to its functions, operation, and use shall be protected from potential compromise by precluding disclosure of this information to the public."

9. Adding to the sensitive nature of the FBI's cell site simulator equipment, the same techniques and tools used in criminal cases are often used in counterterrorism and counterintelligence investigations. Thus, compromise of the law enforcement community's investigational tools and methods in a criminal case or public records disclosure could have a significant detrimental impact on the national security of the United States.

10. Additionally, cell site simulator technology is a regulated defense article on the United States Munitions List ("USML") (*see* 22 C.F.R. § 121.1 – the US Munitions List, Category XI – Military Electronics, subpart (b) – electronic equipment specifically designed for intelligence, security or military use in surveillance, direction-finding of devices which operate on the electromagnetic spectrum). As such, technical details concerning this technology are subject to the non-disclosure provisions of the International Traffic in Arms Regulations ("ITAR"), 22 C.F.R. Parts 120-130. The ITAR implements the Arms Export Control Act, 22 U.S.C. § 2778, and Executive Order 13637, which control the export and import of defense-related articles and services listed on the USML. Because this equipment is explicitly governed by the ITAR, 22 C.F.R. § 123.1 requires anyone, prior to making an export, to obtain a license

BBM

from the Department of State. Notably, technical information does not have to leave the borders of the United States to be deemed an export subject to the regulation. (*See* 22 C.F.R. § 120.17, which defines an export as the disclosure of technical data about a defense article to a foreign national, even while located in the United States.)

11. Accordingly, if a local government disseminates any part of the technical information knowing that a media organization intends to release the information to the public through the media or via a website, due to the accessibility of the information to non-US citizens, or the requesting media organization employs or has any non-US citizens present at its offices, this may constitute a violation of the Arms Control Export Act. Any unauthorized disclosure of ITAR-controlled information is a felony punishable by up to 20 years imprisonment and up to \$1 million per occurrence. *See* 22 C.F.R. Part 127.

12. Given the media attention to this case and the inability to control the unauthorized release of information in the internet age, once information about the simulator is publicly confirmed, the FBI, as well as the larger law enforcement community, will not be able to employ the equipment again in the future with the same degree of success. Although there is information about cell site simulators and their operation on the Internet, the specific capabilities, settings, limitation and tradecraft used in their deployment were not authoritatively disclosed or confirmed by the FBI. Therefore, should this type of information be authoritatively disclosed or endorsed, criminal defendants will gain valuable intelligence on the specific capabilities of the



law enforcement community to effect surveillance of and locate individuals.

I declare under penalty of perjury that the foregoing facts are true and correct.

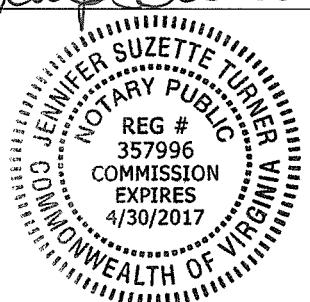
FURTHER AFFIANT SAYETH NOT.

Bradley S Morrison

Bradley S. Morrison
Supervisory Special Agent (SSA)
Chief, Tracking Technology Unit
Federal Bureau of Investigation

Signed and sworn to before me
this 31st day of December 2014

Jennifer Suzette Turner



ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 7 of 11

Bradley S. Morrison, being duly sworn, deposes and states:

I am a Supervisory Special Agent (SSA) with the Federal Bureau of Investigation (FBI), currently assigned as the Chief, Tracking Technology Unit, Operational Technology Division (OTD) in Quantico, Virginia. I have been employed as a FBI Special Agent since 1996. As Unit Chief, I am responsible for the development, procurement, deployment, and management of technical assets and capabilities to surreptitiously locate, tag, and track targets of interest in support of all FBI investigative, intelligence collection, and operational programs. I am responsible for establishing and advising on policy guidance for the FBI, including whether a particular tool or technique my program manages meets the criteria for protection as law enforcement sensitive, while ensuring that state-of-the-art technical investigative assets remain available to field technical programs to enable them to assist in a wide range of technical investigative missions. This includes the use and deployment of electronic surveillance devices such as the cell site simulator at issue in this case.

Title 5, United State Code, Section 301 empowers the head of an executive department to set regulations that govern the dissemination of information belonging to that department. With respect to the FBI, as a component of the Department of Justice (DOJ), the Attorney General has promulgated 28 C.F.R. §16.21, in which the Attorney General set forth procedures to follow upon receiving a request for information relating to material contained in the files of the department, or acquired from the department as part of one's official duties. DOJ officials are required to consider several factors in deciding whether to allow privileged information to be released, including whether disclosure of the information sought would "reveal investigatory records compiled for law enforcement purposes, and would... disclose investigative techniques and procedures" whose effectiveness would be impaired by disclosure. 28 C.F.R. §16.26(b)(5).

The FBI OTD has always asserted that the cell site simulators are exempt from discovery pursuant to the "law enforcement sensitive" qualified evidentiary privilege, as information concerning this equipment, if made public, could easily impair use of this investigative method. Likewise, the FBI protects information about its use of this technology in response to requests under the federal Freedom of Information Act ("FOIA"), 5 U.S.C. § 552. Law enforcement techniques and procedures enjoy categorical protection under FOIA Exemption 7(E), 5 U.S.C. § 552(b)(7)(E), in order to preserve the utility of those techniques and procedures, and mitigate the risk that they will be circumvented. Under FOIA Exemption 7(E), the FBI protects a range of information about cell site simulators, including operational details such as how, when, where, and under what circumstances the FBI uses cell site simulators, and technical details, such as the particular technology and equipment that the FBI uses. Disclosure of even minor details about the use of cell site simulators may reveal more information than their apparent insignificance suggests because, much like a jigsaw puzzle, each detail may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself. Thus, disclosure of what appears to be innocuous information about the use of cell site simulators would provide adversaries with critical information about the capabilities, limitations, and circumstances of their use, and would allow those adversaries to accumulate information and draw conclusions about the

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 8 of 11

use and technical capabilities of this technology. In turn, this would provide them the information necessary to develop defensive technology, modify their behaviors, and otherwise take countermeasures designed to thwart the use of this technology. Doing so would thus allow them to evade detection by law enforcement and circumvent the law.

In recognition of this vulnerability, the FBI has, as a matter of policy, for over 10 years, protected this specific electronic surveillance equipment and techniques from disclosure, directing its agents that while the product of the identification or location operation can be disclosed, neither details on the equipment's operation nor the tradecraft involved in use of the equipment may be disclosed. The FBI routinely asserts the law enforcement sensitive privilege over cell site simulator equipment because discussion of the capabilities and use of the equipment in court would allow criminal defendants, criminal enterprises, or foreign powers, should they gain access to the items, to determine the FBI's techniques, procedures, limitations, and capabilities in this area. This knowledge could easily lead to the development and employment of countermeasures to FBI tools and investigative techniques by subjects of investigations and completely disarm law enforcement's ability to obtain technology-based surveillance data in criminal investigations. This, in turn, could completely prevent the successful prosecution of a wide variety of criminal cases involving terrorism, kidnappings, murder, and other conspiracies where cellular location is frequently used. See United States v. Rigmaiden, 845 F.Supp. 982 (D.Ariz. 2012); United States v. Garey, 2004 WL 2663023 (M.D.Ga. Nov. 15, 2004); see also generally FBI's Technical Personnel and Technical Equipment and Use Policy Implementation Guide (0631DPG), sections 1.2.1, 1.2.3, and 1.3, and the FBI's Manual of Investigative Operations and Guidelines, §§ 6-2.1, 6-5.3, 10-10.13, 16-4.8.6 and 16-4.8.14.

Further, the FBI has entered into a non-disclosure agreement (NDA) with our state and local law enforcement partners. The NDA is specific to state and local law enforcement use of cell site simulator technology, and was entered into in an effort to protect law enforcement sensitive details about the technology. The NDA acknowledges that "[d]isclosing the existence of and the capabilities provided by [cell site simulator equipment] to the public would reveal sensitive technological capabilities possessed by the law enforcement community and may allow individuals who are the subject of investigation...to employ countermeasures to avoid detection by law enforcement. This would not only potentially endanger the lives and physical safety of law enforcement officers and other individuals, but also adversely impact criminal and national security investigations. That is, disclosure of this information could result in the FBI's inability to protect the public from terrorism and other criminal activity because, through public disclosures, this technology has been rendered essentially useless for future investigations. In order to ensure that such [cell site simulator] equipment continues to be available for use by the law enforcement community, the equipment/technology and any information related to its functions, operation, and use shall be protected from potential compromise by precluding disclosure...to the public..."

Adding to the sensitive nature of the FBI's cell site simulator equipment, the same techniques and tools used in criminal cases are often used in counterterrorism and counterintelligence investigation. Thus, the compromise of the law enforcement community's investigational tools and

methods in a criminal case or public records disclosure could have a significant detrimental impact on the national security of the United States.

Specifically, any information shared by the federal government with a state concerning cell site simulator technology is considered homeland security information under the Homeland Security Act. The Act defines homeland security information as information that relates to the ability to prevent, interdict, or disrupt terrorist activity; information that would improve the identification or investigation of a suspected terrorist or terrorist organization; or information that would improve the response to a terrorist act. See 6 U.S.C. §§ 482(f)(1)(B)-(D). Cell site simulator technology meets all three criteria. Accordingly, under 6 U.S.C. §482(e), homeland security information "obtained by a State or local government from a Federal agency under this section shall remain under the control of the Federal agency, and a State or local law authorizing or requiring such a government to disclose information shall not apply to such information." The FBI does not consent to release of the information, including technical specifications, technique limitations and vulnerabilities, and training and operational materials.

Additionally, cell site simulator technology is a regulated defense article on the United States Munitions List (USML) (see 22 C.F.R. §121.1 – the US Munitions List, Category XI – Military Electronics, subpart (b) – electronic equipment specifically designed for intelligence, security or military use in surveillance, direction-finding of devices which operate on the electromagnetic spectrum). As such, technical details concerning this technology are subject to the non-disclosure provisions of the International Traffic in Arms Regulations ("ITAR"), 22 C.F.R. Parts 120-130. The ITAR implements the Arms Export Control Act, 22 U.S.C. §2778, and Executive Order 13637, which control the export and import of defense-related articles and services listed on the United States Munitions List (USML). Because this equipment is explicitly governed by the ITAR, 22 C.F.R. §123.1 requires anyone, prior to making an export, to obtain a license from the Department of State. Notably, technical information does not have to leave the borders of the United States to be deemed an export subject to the regulation. (see 22 C.F.R. §120.17, which defines an export as the disclosure of technical data about a defense article to a foreign national, even while located in the United States).

Accordingly, if a state disseminates any part of the technical information knowing that a media organization intends to release the information to the public through the media or via a website, due to the accessibility of the information to non-US citizens, or the requesting media organization employs or has any non-US citizens present at its offices, this may constitute a violation of the Arms Control Export Act. Any unauthorized disclosure of ITAR-controlled information is a felony punishable by up to 20 years imprisonment and up to \$1 million per occurrence. See 22 C.F.R. Part 127.

Specifically, with respect to the cell site simulator used in this case, given the media attention to this case and the inability to control the unauthorized release of information in the internet age, once information about the simulator is publicly confirmed, the FBI, as well as the larger law enforcement community, will not be able to employ the equipment again in the future with the same degree of success. Although there is information about cell site simulators and their operation on the Internet, the specific capabilities, settings, limitation and tradecraft used in their deployment were not authoritatively disclosed or confirmed by the FBI. Therefore, should this type of information be

authoritatively disclosed or endorsed, criminal defendants will gain valuable intelligence on the specific capabilities of the law enforcement community to effect surveillance of and locate individuals.

I declare under penalty of perjury that the foregoing facts are true and correct.

4/11/14

Bradley S. Morrison

Date

Bradley S. Morrison
Supervisory Special Agent (SSA)
Chief, Tracking Technology Unit
Federal Bureau of Investigation



Kelly A. Haden
NOTARY PUBLIC
Commonwealth of Virginia
Reg. #353472
My Commission Expires
March 31, 2016

City/County of Stafford
Commonwealth of Virginia
The foregoing instrument was acknowledged before me
this 11 day of April 2014,
by Bradley S. Morrison
Kelly A. Haden Notary Public
My commission expires 3-31-2016

BSM

STINGRAYS

The Most Common Surveillance Tool
the Government Won't Tell You About

A Guide for Criminal Defense Attorneys

FROM THE ACLU OF NORTHERN CALIFORNIA

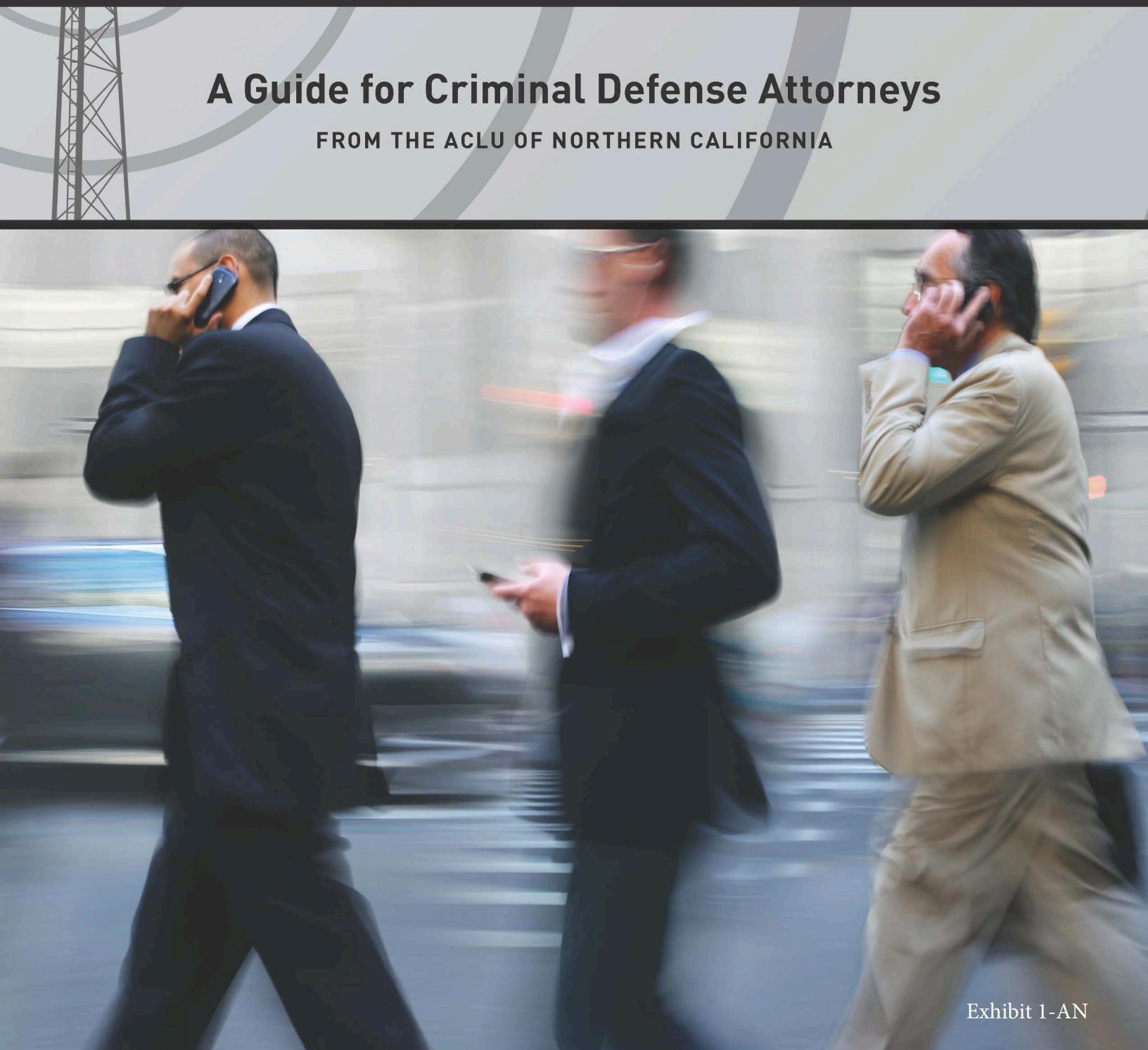




Photo credit: US Patent & Trademark Office

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 2 of 46

Author: Linda Lye, Senior Staff Attorney, ACLU of Northern California
Cover: Gigi Pandian, ACLU of Northern California
Design: Carey Lamprecht

Published by the ACLU of Northern California, June 27, 2014

The author wishes to thank Nanci Clarence, Josh Cohen, Catherine Crump, Hanni Fakhoury, Carey Lamprecht, Robin Packel, Mindy Phillips, and Nate Wessler for reviewing and commenting on drafts of this paper, and Christopher Soghoian for providing an eye-opening education on IMSI catchers. Special thanks go to Daniel Rigmaiden for his keen insights on legal and technological issues and for shedding light on this important issue.



TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	StingRays: What do they do and how do they work?	2
III.	What kind of court authorization, if any, does the government currently obtain to use the device?	4
A.	No court authorization?.....	4
B.	Pen register/trap and trace order?	5
C.	Hybrid Order?	6
D.	Warrant?.....	7
IV.	What guidance have courts offered on StingRays?	7
V.	How can you tell if the government used a StingRay in your case?.....	9
A.	Terminology	9
B.	How did the government find out your client's cell phone number?	10
C.	How did the government locate your client?	10
VI.	Key legal arguments to raise if an IMSI catcher was used	10
A.	IMSI catchers trigger Fourth Amendment scrutiny	11
1.	Use in connection with residences	11
2.	Use in public	12
B.	IMSI catchers engage in the electronic equivalent of a "general search" and their use therefore violates the Fourth Amendment	13
C.	Statutory orders do not suffice to authorize IMSI catcher use.....	14
D.	Even if the government obtained a warrant, use of an IMSI catcher is still invalid	15
1.	The government's omission of information about new surveillance technology from a warrant application prevents courts from exercising their constitutional oversight function and would render a warrant invalid	15
a.	A warrant that fails to disclose the government's intended use of an IMSI catcher is predicated on a material omission	16

b.	A defendant is entitled to a <i>Franks</i> hearing	18
2.	A warrant that accurately describes an IMSI catcher's capabilities would be facially invalid.....	19
VII.	CONCLUSION.....	22
APPENDIX: Issues to Pursue in Discovery		23
ENDNOTES		28

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 4 of 46

I. Introduction

Federal and state law enforcement entities across the country are using a powerful cell phone surveillance tool commonly referred to as a “StingRay.” These devices are capable of locating a cell phone with extraordinary precision, but to do so they operate in dragnet fashion, scooping up information from a target device, as well as other wireless devices in the vicinity. In addition, these devices can be configured to capture the content of voice and data communications. Although the federal government has been using these devices since at least 1995, and use by state and local governments is quite widespread, there are only a handful of opinions addressing their use.

At this juncture, few criminal defense attorneys are aware of these highly intrusive but extremely common surveillance tools. This is entirely understandable because the federal government has a policy of not disclosing information about this device. The government appears to be withholding information from criminal defendants. It even appears to be providing misleading information and making material omissions to judicial officers when it seeks purported court authorization to use this device – inaccurately referring to it as a “confidential source” or calling it a different kind of device (like a pen register), and failing to alert courts to constitutionally material facts about the technology, such as the full breadth of information it obtains from a suspect and its impact on third parties. As a result, courts are probably not aware that they are authorizing use of this device and have not had an opportunity to rule on its legality, except in very rare instances.

The secrecy surrounding these devices is deeply troubling because this technology raises grave constitutional questions. There is a compelling argument that StingRays should never be used. Because they operate in dragnet fashion, they engage in the electronic equivalent of the “general searches” prohibited by the Fourth Amendment. But at a minimum, law enforcement should obtain a warrant. Even in those instances when law enforcement obtains a warrant, however, there are likely strong arguments that the warrant is invalid.

The purpose of this paper is to provide criminal defense attorneys with a basic introduction to StingRays, allowing them to assess whether the devices may have been used in their cases and to outline potential arguments for a motion to suppress.

Part II of this paper provides a brief overview of salient aspects of the technology and uses for the device. Part III describes the types of court authorization, if any, the government likely obtains to use the device. Part IV discusses the guidance courts have offered on the technology. Part V suggests indicia for determining whether the device was used in a particular case. Part VI outlines key constitutional arguments for a motion to suppress, focusing on Ninth Circuit caselaw. Potential issues to pursue in discovery are set forth in an appendix to this paper. Detailed footnotes are intended to assist attorneys preparing briefs.

II. **StingRays: What do they do and how do they work?**

“StingRay” is the name for a line of “cell site simulator” technology sold by the Harris Corporation.¹ Other Harris cell site simulator models include the “TriggerFish,” “KingFish,” and “Hailstorm.”² The more generic term for the technology is “IMSI catcher,” in reference to the unique identifier – or international mobile subscriber identity – of a wireless device. Although IMSI catchers may be the most under-litigated surveillance tool in widespread use, there is a fair amount of publicly available information about them.

The government has been using IMSI catchers for approximately two decades. According to documents obtained by the Electronic Privacy Information Center (“EPIC”) in a Freedom of Information Act (“FOIA”) lawsuit, the Federal Bureau of Investigation (“FBI”) has been using the technology since 1995, agents have undergone extensive training on these devices, and usage is dramatically increasing.³ A number of federal law enforcement agencies, including the FBI, Drug Enforcement Administration, Bureau of Alcohol, Tobacco, Firearms and Explosives, Secret Service, Marshals Service, and Immigration and Customs Enforcement, are known to own and use cell site simulators.⁴ Use is not limited to the federal government. At least 34 law enforcement agencies in 15 states have purchased IMSI catchers.⁵

Wireless carriers provide coverage through a network of base stations, also called cell sites, that connect wireless devices to the regular telephone network. Cell phones periodically identify themselves to the base station that has the strongest radio signal, which is often, but not always, the nearest base station.⁶ A cell phone automatically transmits to the base station “signaling data,” which includes the phone’s unique numeric identifier, as well as its cell site code, which identifies its location.⁷ An IMSI catcher masquerades as a wireless carrier’s base station, thereby prompting cell phones to communicate with it as though it were actually the carrier’s base station.⁸ The equipment consists of “an antenna, an electronic device that processes the signals transmitted on cell phone frequencies, and a laptop computer that analyzes the signals and allows the agent to configure the collection of information.”⁹ It “can be carried by hand or mounted on vehicles or even drones.”¹⁰

StingRays are capable of capturing the following types of information:

First, if the government knows a suspect’s location, it can use the device to determine the unique numeric identifier associated with her cell phone. To do this, law enforcement agents “position a StingRay in the vicinity of the target[’s phone],” which will then transmit to the IMSI catcher the signaling information (including unique numeric identifier) it would normally transmit to the carrier’s base station.¹¹ There are a variety of unique numeric identifiers, including International Mobile Subscriber Identity (“IMSI”),¹² Electronic Serial Number (“ESN”),¹³ and Mobile Identification Number (“MIN”).¹⁴ Obtaining a cell phone’s unique numeric identifier facilitates the government’s efforts to obtain a wiretap or call records on a target of an investigation.

Second, if the government knows a cell phone’s unique numeric identifier, it can use an IMSI catcher to determine the phone’s location.¹⁵ The numeric identifier is programmed into the

IMSI catcher, which then sorts through the signaling data (including location) of cell phones in the area until it finds a match.¹⁶ While law enforcement can also obtain location information through requests to carriers for cell site location information,¹⁷ IMSI catchers vary from carrier requests in at least two regards. IMSI catchers can typically be used without carrier assistance.¹⁸ In addition, IMSI catchers produce extremely precise location information, in some cases “within an accuracy of 2 m[eters].”¹⁹ In one federal case, the government conceded that the IMSI catcher located the defendant’s wireless device precisely within a specific apartment in an apartment complex.²⁰ In Florida, Tallahassee police testified that by “using portable equipment” and going to “every door and every window” in a large apartment complex, they were able to identify the “particular area of the apartment that that handset was emanating from.”²¹ While carrier-provided cell site location information may under certain circumstances achieve similar precision, it is entirely variable, and depends on a number of factors, including the density of cell towers.²²

Third, IMSI catchers are capable of capturing the content of communications, such as voice calls and text messages.²³ The devices used by the federal government are likely configured to disable the content intercept function; as the United States Department of Justice (“DOJ”) acknowledges, a wiretap order under the heightened Title III standard (18 U.S.C. § 2518) would otherwise be necessary.²⁴ While some devices can be configured to intercept content, we are not aware of instances in which law enforcement has deployed an IMSI catcher in this fashion and the primary governmental uses appear to be identifying a phone’s unique numeric identifier or location.

Several aspects of the technology are salient.

First, an IMSI catcher scoops up information from third parties, not just the target of an investigation. The type of IMSI catcher currently used by law enforcement mimics a wireless company’s network equipment, sending signals to and triggering an automatic response from third parties’ mobile devices.²⁵ DOJ concedes as much, as one of its template applications pertaining to IMSI catchers builds in the contingency that “any cellular phone that is within close proximity to the government device . . . may autonomously register with the device.”²⁶ The devices also may disrupt third parties’ network connectivity,²⁷ although DOJ contends that its policy is to take steps to “minimize any potential temporary disruption of service” to “non-target telephones,” “by operating the device for limited duration and only when the cellsite information acquired from the provider indicates that the Subject Telephone is operating nearby.”²⁸

Second, the device broadcasts electronic signals that penetrate the walls of private spaces not visible to the naked eye, including homes and offices.²⁹ Depending on the device’s signal strength, the broadcast radius can reach up to “several kilometers,”³⁰ allowing the IMSI catcher to scoop up information from any and all private locations in the area.

Third, an IMSI catcher *forces* cell phones to transmit signaling information.³¹ As one law enforcement officer has described it, the government’s device “actually captures the phone” and “direct[s] the signal from the [carrier’s] tower to [the government’s] equipment.”³²

Fourth, an IMSI catcher operates in the same basic manner – mimicking a base station and forcing an automatic response from devices in the immediate vicinity – regardless of the type of signaling information captured (unique numeric identifier or location). As DOJ explains:

A cell site simulator, digital analyzer, or a triggerfish can electronically force a cellular telephone to register its mobile identification number (“MIN,” *i.e.*, telephone number) and electronic serial number (“ESN,” *i.e.*, the number assigned by the manufacturer of the cellular telephone and programmed into the telephone) when the cellular telephone is turned on. Cell site data (the MIN, the ESN, and the channel and cell site codes identify the cell location and geographical sub-sector for which the telephone is transmitting) are being transmitted continuously as a necessary aspect of cellular telephone call direction and processing. The necessary signaling data (ESN/MIN, channel/cell site codes) are not dialed or otherwise controlled by the cellular telephone user. Rather, the transmission of the cellular telephone’s ESN/MIN to the nearest cell site occurs automatically when the cellular telephone is turned on....If the cellular telephone is used to make or receive a call, the screen of the digital analyzer/cell site simulator/triggerfish would include the cellular telephone number (MIN), the call’s incoming or outgoing status, the telephone number dialed, the cellular telephone’s ESN, the date, time, and duration of the call, and the cell site number/sector (location of the cellular telephone when the call was connected).³³

Thus, an IMSI catcher operates in the same fashion, engaging in the same dragnet for information, regardless of whether the government ultimately filters the information obtained for a phone’s unique numeric identifier or its location.

III. What kind of court authorization, if any, does the government currently obtain to use the device?

Although the full extent of government use of IMSI catchers remains to be revealed, even less is known about the legal process used by the government when deploying this technology. With respect to federal use, there are a handful of public DOJ documents that reference this technology.³⁴ The guidance and best practices set forth in these documents are somewhat internally inconsistent. DOJ has resisted disclosing further information about its policies, practices, and procedures for using this device.³⁵

A. No court authorization?

In some instances, law enforcement entities, at least at the state and local level, are not obtaining any court authorization to use the device. The police department in Tucson, Arizona, has admitted in court-filed pleadings that while it has used IMSI catchers on at least five occasions, it has never obtained a warrant to do so and has no records of having obtained any other kind of court order authorizing use of the device; similar revelations have been made in Sacramento, California where the Sheriff almost certainly has a IMSI catcher, but the District Attorney’s Office and superior court judges state they have no knowledge of the device being used.³⁶

B. Pen register/trap and trace order?

It appears that DOJ recommends that the government obtain an order under the Pen Register/Trap and Trace Statute (“Pen/Trap Statute”) when using an IMSI catcher to identify a target phone’s unique numeric identifier or location. The DOJ documents are somewhat inconsistent and it is unclear if DOJ’s position is that a Pen/Trap order is necessary or merely a “best practice.”

Under the Pen/Trap Statute, the government may obtain an order authorizing installation of a pen register or trap and trace device upon an application certifying that “the information likely to be obtained is relevant to an ongoing criminal investigation.” 18 U.S.C. § 3122(b)(2). A pen register is typically understood to be a device that records the numbers dialed by a particular telephone; a trap and trace device records the incoming numbers to a telephone.³⁷ The Pen/Trap Statute was amended in 2001 to expand the definition of pen/trap devices to include not only devices that capture incoming and outgoing numbers, but also those that capture “signaling information.”³⁸

DOJ has taken the following positions:

- *Pen/Trap order necessary and sufficient to obtain numeric identifier and location information.* DOJ’s 2005 Electronic Surveillance Manual states that a Pen/Trap order “must be obtained by the government before it can use its own device to capture the [unique numeric identifier] of a cellular telephone” and that a Pen/Trap order would also suffice to obtain location information.³⁹
- *Pen/Trap order merely considered a “best practice” to obtain numeric identifier and location information.* Elsewhere, however, the same manual states: DOJ “[does] not concede that a device used to receive[s] radio signals, emitted from a wireless cellular telephone” and that “identif[ies] that telephone to the network,” in other words, an IMSI catcher, constitutes a ‘pen register’ or ‘trap and trace’ device,” but recommends an application for court authorization “out of an abundance of caution.”⁴⁰ A 2008 PowerPoint training on “Cellular Tracking and Other Legal Issues” produced by the FBI in a FOIA lawsuit describes use of a Pen/Trap order as a “best practice” when using “Cellsight Simulators” to “[i]dentify a target phone or . . . [l]ocate a phone.”⁴¹
- *Pen/Trap order necessary to obtain numeric identifier; position as to location information unclear.* A 2013 DOJ document asserts that a Pen Trap Order is necessary (*i.e.*, not merely a “best practice” or sought “out of an abundance of caution”), at least when the government seeks to identify the unique numeric identifier of a target phone using an IMSI catcher.⁴² The publicly available portion of the 2013 document does not address DOJ’s position with respect to using a Pen/Trap order to obtain a target phone’s location with an IMSI catcher.

Any argument that a Pen/Trap order suffices to obtain location information is noteworthy in light of the Communications Assistance for Law Enforcement Act (“CALEA”). Congress enacted CALEA in 1994 for the purpose of requiring telecommunications carriers to adopt the technology necessary to provide, upon appropriate court order, content and “call-identifying information” to law enforcement.⁴³ The statute, however, expressly prohibits use of a Pen/Trap order to obtain location information: “with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices . . . such call-identifying information shall not include any information that may disclose the physical location of the subscriber . . . ”⁴⁴ DOJ’s 2005 Electronic Surveillance Manual states that the government can, notwithstanding CALEA, use an IMSI catcher to obtain location information because CALEA’s “prohibition applies only to information collected by a provider and not to information collected directly by law enforcement authorities.”⁴⁵

C. Hybrid Order?

Although some DOJ materials state that a Pen/Trap order suffices when the government uses an IMSI catcher to obtain location information, other materials appear to recommend use of a so-called “hybrid order” for this purpose.

A hybrid order is the same type of order that DOJ contends is sufficient to obtain prospective, or real-time, cell site location information from a wireless carrier.⁴⁶ As noted above, CALEA prohibits the government from relying “solely” on a Pen/Trap order to obtain location information from a carrier.⁴⁷ Under the hybrid theory, the government justifies acquisition of location information from wireless carriers by combining the Pen/Trap Statute with the Stored Communications Act (“SCA”), 18 U.S.C. § 2703(d), which authorizes the government to obtain records from a provider pertaining to certain kinds of records or information pertaining to customers or subscribers. The relevant provision of the SCA requires the government to set forth “specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought, are relevant and material to an ongoing criminal investigation.”⁴⁸ Notably, a significant majority of courts have held that a hybrid order does *not* suffice to obtain prospective cell site location information, and that a warrant is instead required.⁴⁹

An IMSI catcher, like an order for prospective cell site information, obtains location information in real time. DOJ’s 2005 Electronic Surveillance Manual includes a template application for a hybrid order that authorizes use of a device that appears to be an IMSI catcher.⁵⁰ Although the template application refers to the device as a “pen register,” the template’s brief allusions to the manner in which the device operates strongly suggests that the device at issue is actually an IMSI catcher.⁵¹

Note that although DOJ’s template application for a hybrid order provides some description of how the device functions, actual IMSI catcher applications filed in court provide no such information. In *United States v. Rigmaiden*, 844 F. Supp. 2d 982 (D. Ariz. 2012), for example, the government ultimately acknowledged it used an IMSI catcher, but its affidavit in support of the relevant court order nowhere referred to an IMSI catcher or explained how the

device functions. The affidavit instead made fleeting references to an unspecified “mobile tracking device,” and the only description of how the device works stated that “[t]he mobile tracking equipment ultimately generate[s] a signal that fixes the geographic position of the Target [Device].”⁵²

In short, DOJ appears to take the position that a hybrid order suffices to authorize use of an IMSI catcher to identify a target phone’s location in real time, even though most courts have rejected the related argument that a hybrid order suffices when the government seeks to obtain real-time location information from a carrier. In addition, DOJ’s template application for an order authorizing use of an IMSI catcher to obtain location information nowhere uses the term “IMSI catcher” or any other related term, and instead is styled as an application to install a “pen register.” Finally, even though DOJ’s template application for an IMSI catcher contains some description (albeit minimal) of how the technology functions, actual IMSI catcher applications filed in court do not.

D. Warrant?

In at least some instances, the federal government has sought warrants to use a StingRay to obtain location information.⁵³ Warrants, of course, require, among other things, the government to establish probable cause and to state with particularity the place to be searched, and the persons or things to be seized.⁵⁴

IV. What guidance have courts offered on StingRays?

Only a handful of published decisions have addressed IMSI catchers.

The earliest reported decision involved an early-generation IMSI catcher called a “digital analyzer.” *See In re Application for an Order Authorizing Use of a Cellular Telephone Digital Analyzer*, 885 F. Supp. 197 (C.D. Cal. 1995) (hereinafter “*In re Digital Analyzer*”). The government submitted an application for a Pen/Trap order to use the device to detect the unique numeric identifier of the cell phones used by five subjects of a criminal investigation. *See id.* at 199. The opinion contains two main holdings, each somewhat difficult to reconcile with the other. The government contended, and the court agreed, that no court order was required because the device – which is not physically attached to a telephone – did not fall under the statutory definition of a pen register or trap and trace device then in effect. *See id.* at 199-200 (citing 18 U.S.C. § 3127(3) & (4)). The court went on to hold, however, that to the extent some procedure was required, the government’s proposed procedure lacked sufficient safeguards. *See id.* at 201. The court then denied the application for an order authorizing use of the device, without prejudice to a renewed application proposing greater safeguards. *See id.* at 202.

More recently, the court in *In re Application for an Order Authorizing Installation and Use of a Pen Register and Trap and Trace Device*, 890 F. Supp. 2d 747 (S.D. Tex. 2012) (hereinafter “*In re StingRay*”), also denied the government’s application for a Pen/Trap order to use an IMSI catcher to ascertain a suspect’s telephone number. Although the statute had been expanded in 2001, after *In re Digital Analyzer*, to set forth a broader definition of “pen

register,”⁵⁵ the court still concluded that the statute was inapplicable. *See id.* It held that a Pen/Trap order is only available for known telephone numbers, and not to ascertain unknown numbers. *See id.* But, unlike the Central District of California, the Southern District of Texas did not hold that, given the inapplicability of the Pen/Trap Statute, no court order was required. Instead, it strongly suggested that a warrant would instead be necessary. *See id.* at 752. It also criticized the government’s application for failing to “explain the technology, or the process by which the technology will be used to engage in electronic surveillance” or to address key facts about the government’s proposed operation of the device and handling of third-party data. *Id.* at 749.

This case suggests that even technology savvy magistrates, such as those in the Southern District of Texas, are not familiar with the device and have many unanswered questions about how it works. As discussed above, the template application to use an IMSI catcher in DOJ’s Electronic Surveillance Manual nowhere explicitly mentions an IMSI catcher and instead refers only to “pen register” devices, and actual applications and orders to use IMSI catchers filed in court similarly make no explicit reference to IMSI catchers, let alone how they work.⁵⁶ It is thus very likely that judicial officers across the country are unaware that they are being presented with requests and granting authorization to use IMSI catchers.

In *Rigmaiden*, a *pro se* defendant accused of electronic tax fraud succeeded through creative discovery in forcing the government to concede what the government had not acknowledged in any other criminal prosecution until that point, in particular, that:

- the government used a “cell site simulator” to locate the defendant’s wireless device;
- the cell site simulator “mimicked a Verizon Wireless cell tower and sent signals to, and received signals from,” the defendant’s device; and
- the cell site simulator “located [the defendant’s device] precisely within Defendant’s apartment – Unit 1122 of the Domicilio Apartments.”

Id. at 995-96. In addition to these highly noteworthy factual concessions, the government also conceded that the use of the cell site simulator was sufficiently intrusive to constitute a search within the meaning of the Fourth Amendment. *Id.* This was highly significant, in light of the position set forth in DOJ’s Electronic Surveillance Manual, that a Pen/Trap or hybrid order suffices. *See supra* Section III.

Thereafter, Rigmaiden brought a motion to suppress on numerous grounds, including a challenge to the use of the IMSI catcher. The government contended that it had obtained a warrant to use the device. Rigmaiden, joined by *amici* ACLU and the Electronic Frontier Foundation, contended, among other things, that the government had withheld constitutionally material information from the issuing magistrate, rendering the order on which the government relied an invalid general warrant. The application failed to alert the issuing magistrate that the government intended to use an IMSI catcher and omitted constitutionally material information about how the technology works, such as its impact on third parties.⁵⁷ Emails obtained by the ACLU of Northern California in a FOIA lawsuit suggest that the government’s failure to disclose to the court information about IMSI catchers in its applications for authorization to use the

device was not isolated to the *Rigmaiden* case.⁵⁸

Unfortunately, the court denied the motion to suppress. *See United States v. Rigmaiden*, 2013 WL 1932800 (D. Ariz. May 8, 2013). It held that information about how the IMSI catcher operates was a mere “detail of execution which need not be specified.” *Id.* at *20. The court also dismissed the significance of the government’s capturing of third-party information because the government expunged the data. *Id.* at *22. Finally, although the court found that the government did not violate the Fourth Amendment, it also found that the government acted in good faith because the “agents were using a relatively new technology” and lacked legal precedent on the type of warrant to be sought. *Id.* at *31.

In *United States v. Espudo*, 954 F. Supp. 2d 1029 (C.D. Cal. 2013), an IMSI catcher was also used. But the court denied the motion to suppress, based on a government affidavit stating that evidence from the IMSI catcher was not used to further the investigation. *See id.* at 1045. In *Thomas v. State*, 127 So. 3d 658 (Fla. Dist. Ct. App. 2013), the police used unspecified technology to track a cell phone to the defendant’s home. *Id.* at 659-60 & n.2. The ACLU unsealed a transcript from a hearing in the court below and it confirms that the technology at issue was an IMSI catcher.⁵⁹ The appellate court in *Thomas* did not address the legality of the use of the technology and resolved the case on other grounds. An IMSI catcher also was used in *Wisconsin v. Tate*, No. 2012AP336 (Wis. Ct. App. June 5, 2011), a case now pending before the Wisconsin Supreme Court.⁶⁰ It is not clear if the court will reach the IMSI catcher issue, which was not addressed by the court below.

V. How can you tell if the government used a StingRay in your case?

There are very few cases addressing IMSI catchers, leaving the area ripe for litigation. The challenge lies in determining whether an IMSI catcher was even used. Even in those instances where the government obtains some kind of court authorization to use the device, the application and order will very likely *not* refer to IMSI catcher technology. The FBI has publicly acknowledged that it “has, as a matter of policy, for over 10 years, protected this specific electronic surveillance equipment and techniques from disclosure, directing its agents that while the product of the identification or location operation can be disclosed, neither details on the equipment’s operation nor the tradecraft involved in use of the equipment may be disclosed.”⁶¹ There are, however, several indications that the government may have used an IMSI catcher in any particular case.

A. Terminology

While technologists use the term “IMSI catcher,” DOJ does not and instead uses widely varying, inconsistent terms, including, but not limited to, digital analyzer, cell site simulator, cell site emulator, cell site monitor, triggerfish, StingRay, kingfish, amberjack, hailstorm, and WITT, in reference to the FBI’s Wireless Intercept Tracking Team. Be on the lookout for any of the foregoing terms. But the government may also conceal use of an IMSI catcher by instead referring to a “mobile tracking device” or “pen register,” even though the former term typically refers to GPS devices (or so-called “bumper beepers”), and the latter to requests for information

from telephone service providers.⁶² In some instances, the government is even referring to an unspecified “confidential source.”⁶³ An indicator of potential IMSI catcher use, more reliable than terminology, is how the government’s investigation actually unfolded.

B. How did the government find out your client’s cell phone number?

IMSI catchers can be used to capture the unique numeric identifier, such as an Electronic Serial Number or Mobile Identity Number, of a wireless device, and public DOJ documents clearly contemplate use of this device for this purpose.⁶⁴ The fact that applications and court orders refer only to pen register devices does not rule out the possibility that an IMSI catcher was used.

Obtaining the ESN, IMSI, MIN, or other identification number of a suspect’s phone is a necessary predicate for a wiretap order or an order to a carrier for call records. If the government obtained such orders in your case, but it is unclear how it obtained your client’s cell phone number, or the only explanation is a highly cryptic reference to an unspecified “confidential source” or “source of information” with no details as to the source, consider pursuing the issue of an IMSI catcher in discovery. (An alternative possibility is that the government obtained the number through another surveillance program known as the “Hemisphere project.”⁶⁵)

C. How did the government locate your client?

IMSI catchers are also used to locate targets of an investigation. The government is very likely to offer alternative explanations for how it located a suspect to avoid disclosing that a StingRay was used. One email from an FBI Special Agent in *Rigmaiden* read: “The tech guys were able to narrow the signal to 3 apartments. Today, we will be doing as much follow up research as we can. *We need to develop independent probable cause of the search warrant... FBI does not want to disclose the [redacted] (understandably so).*” (Ellipsis in original).⁶⁶ If there was any point in the investigation when the government was able to identify the location of your client, and even if the government offered non-StingRay related explanations for how it did so, consider pursuing this issue in discovery.

VI. Key legal arguments to raise if an IMSI catcher was used

There are several broad categories of constitutional concerns that arise from IMSI catcher use. First, use of an IMSI catcher triggers Fourth Amendment scrutiny because it constitutes both a search and a seizure within the meaning of the Fourth Amendment. Second, there is a strong argument that IMSI catchers can never be used consistent with the Fourth Amendment because they engage in the electronic equivalent of a “general search.” Third, law enforcement must at least obtain a warrant; a statutory order does not suffice. Fourth, even if law enforcement obtained a warrant, it is likely invalid. While precise legal arguments would vary depending on the actual language of the warrant, one of two scenarios is likely. Any warrant was likely based on an *inaccurate* affidavit that contained materially misleading statements or omissions about the government’s intended use of an IMSI catcher; those material statements and omissions render a warrant invalid. Alternatively, if the warrant is *accurate* in describing

the government's intended and actual use of the IMSI catcher, then it almost certainly does not satisfy particularity and breadth requirements and is facially invalid. Additional and more specific legal arguments are almost certainly available, depending on the particular facts and circumstance of each case.

A. IMSI catchers trigger Fourth Amendment scrutiny

IMSI catchers are so intrusive that they violate both reasonable expectations of privacy and property interests. Their use therefore constitutes a search within the meaning of the Fourth Amendment. They also give rise to Fourth Amendment seizures.

1. Use in connection with residences

IMSI catchers invade reasonable expectations of privacy because they can be used to ascertain the location or unique numeric identifier of a suspect's cell phone, while the suspect is located inside her private residence or other private space.⁶⁷ The use of an electronic device to determine information about the interior of private residences and other constitutionally protected spaces clearly constitutes a Fourth Amendment search. *See United States v. Karo*, 468 U.S. 705, 715 (1984) (placing beeper into can of ether that was taken into a residence constituted a search because it "reveal[ed] a critical fact about the interior of the premises"); *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (thermal imaging to detect heat from home constituted search).

An IMSI catcher allows the government to ascertain whether a suspect is located inside a residence or the number of the cell phone she chooses to use while inside. This is all information "about the interior of the premises that the Government is extremely interested in knowing and that it could not otherwise have obtained without a warrant." *Karo*, 468 U.S. at 716.

To be sure, the Supreme Court has held that individuals lack a reasonable expectation of privacy for incoming and outgoing telephone numbers because the information is "voluntarily" conveyed to the third party telephone company. *See Smith v. Maryland*, 442 U.S. 735, 745-46 (1979) (use of pen register does not constitute search). Relying on this rationale, a number of courts have held, in the context of government requests for cell site location information from wireless carriers, that individuals lack a reasonable expectation of privacy in the location of their phone because the information was voluntarily conveyed to the carrier. *See, e.g., In re Application for Historical Cell Site Data*, 724 F.3d 600, 614-15 (5th Cir. 2013) (hereinafter "Fifth Circuit Decision"); *United States v. Skinner*, 690 F.3d 772, 778-79 (6th Cir. 2012); *but see In re Application for an Order Directing a Provider of Electronic Comm. Serv. to Disclose Records*, 620 F.3d 304, 317 (3d Cir. 2010) (rejecting government's argument that subscribers lack reasonable expectation of privacy in cell site location information because they have shared their information with third party communications provider).

But these cases are distinguishable. First, when the government uses an IMSI catcher, it obtains the information directly, not from a third party. *Cf. Smith*, 442 U.S. at 744 (telephone subscriber "assume[s] the risk that the company would reveal to police the numbers he dialed"); *Fifth Circuit Decision*, 724 F.3d at 610 ("the Government . . . draws a line based on whether it is

the Government collecting the information . . . or whether it is a third party, of its own accord and for its own purposes, recording the information"). Second, there is nothing "voluntary" about the information obtained by an IMSI catcher, which "force[s]" cell phones to transmit signaling data.⁶⁸ Third, an individual has a reasonable expectation of privacy about her information when she is inside a residence or other private location, even if she would have no such expectation for the same type of information when in a public place. *Compare United States v. Knotts*, 460 U.S. 276, 281 (1983) (use of bumper beeper to track suspect's location did not constitute search because "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."), with *Karo*, 468 U.S. at 715 (use of beeper to determine suspect "was actually in the house" constituted search: "[t]he case is thus not like *Knotts*, for there the beeper told the authorities nothing about the interior of Knotts' cabin"). When using an IMSI catcher to locate someone or to identify the number of the phone she chooses to use while inside a private location, the government is obtaining "a critical fact about the interior of the premises," *Karo*, 468 U.S. at 715, rather than information emitted from a phone while the suspect is "traveling on public thoroughfares." *Skinner*, 690 F.3d at 781. The Supreme Court has warned that even if a rudimentary form of surveillance technology appears not to effect a "'significant' compromise of the homeowner's privacy," "we must take the long view" when "the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion." *Kyllo*, 533 U.S. at 40.

Relatedly, use of an IMSI catcher in connection with residences may constitute a Fourth Amendment search under a property rationale. To the extent investigators use portable IMSI catchers while walking within the curtilage of a home,⁶⁹ the use constitutes a search because it entails a physical intrusion on constitutionally protected areas. *See Florida v. Jardines*, 133 S. Ct. 1409, 1417 (2013) (use of drug-sniffing dog on front porch of home constituted search under trespass theory); *United States v. Broadhurst*, 2012 WL 5985615 at *6 (D. Or. Nov. 28, 2012) (use of "Shadow," a handheld device that scans wireless networks to determine devices connected to it, while on front lawn constituted search under trespass theory). Even without a physical intrusion into the curtilage by the operator of an IMSI catcher, the IMSI catcher itself broadcasts electronic signals that penetrate the walls of private locations. *See supra* Section II & n.29. This "unauthorized physical penetration into the premises" constitutes a search. *Silverman v. United States*, 365 U.S. 505, 509 (1961) (finding search where government used "spike mike," a microphone attached to spike inserted into walls of house); *but see United States v. Jones*, 132 S. Ct. 945, 949, 953 (2012) (holding that installation and monitoring of GPS on suspect's vehicle constituted search because of "physical intrusion" "for the purpose of obtaining information" but observing that "[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to [reasonable expectation of privacy] analysis").

2. Use in public

IMSI catcher use in public locations may also trigger Fourth Amendment scrutiny.

An "intrusion on possessory interests" gives rise to a Fourth amendment seizure, even when it occurs in a public place. *United States v. Place*, 462 U.S. 696, 705 (1983); *see also id.* at

707 (seizure occurred when agent told defendant at airport he was going to take luggage). The types of IMSI catcher currently used by the government “capture” a target cell phone and “force” it to disconnect from the carrier’s base station and instead “to register” with the government’s fake base station.⁷⁰ By commandeering a target phone in this fashion, the government seizes it.

IMSI catcher use in public places may also constitute a search, depending on the type of data collected and the duration of the surveillance. For example, IMSI catchers are capable of intercepting content. *See supra* Section II. Although DOJ materials make clear that such functions should be disabled absent a Title III wiretap order (18 U.S.C. § 2518),⁷¹ little is known about state and local government protocols for using these devices. In any event, it is essential to obtain discovery about the type of data that was actually collected by the government and, to the extent voice, email, text messages or other private communications were obtained, the Fourth Amendment and Title III or analogous state wiretap statutes are triggered. *See United States v. U.S. Dist. Ct. for the E. Dist. of Michigan, S. Div.*, 407 U.S. 297, 313 (1972) (“[T]he broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards.”); *Katz v. United States*, 389 U.S. 347, 352 (1967) (caller in phone booth had reasonable expectation of privacy: “To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication”); *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) (reasonable expectation of privacy in content of emails).

In addition, if the government used the IMSI catcher to monitor location over a prolonged period,⁷² its use may constitute a search.⁷³

B. IMSI catchers engage in the electronic equivalent of a “general search” and their use therefore violates the Fourth Amendment

IMSI catchers engage in the electronic equivalent of the general searches prohibited by the Fourth Amendment. The Fourth Amendment was “the product of [the Framers’] revulsion against” “general warrants” that provided British “customs officials blanket authority to search where they pleased for goods imported in violation of the British tax laws.” *Stanford v. Texas*, 379 U.S. 476, 481-82 (1965). “General searches have long been deemed to violate fundamental rights. It is plain that the [Fourth] [A]mendment forbids them.” *Marron v. United States*, 275 U.S. 192, 195 (1927). “[T]he Fourth Amendment categorically prohibits the issuance of any warrant except one ‘particularly describing the place to be searched and the persons or things to be seized.’ The manifest purpose of this particularity requirement was to prevent general searches.” *Maryland v. Garrison*, 480 U.S. 79, 84 (1987); *see also Marron*, 275 U.S. at 196 (particularity requirement prohibits general searches by “prevent[ing] the seizure of one thing under a warrant describing another”). By scooping up all manner of information from a target cell phone, as well as all nearby cell phones, an IMSI catcher engages in “general, exploratory rummaging.” *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971); *see also United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982) (“[T]he wholesale seizure for later detailed examination of records not described in a warrant . . . has been characterized as ‘the kind of investigatory dragnet that the fourth amendment was designed to prevent.’”).

The device scoops up *all* signaling information from a suspect's cell phone, rather than targeting evidence of particular crimes as to which there is probable cause. *See, e.g., Groh v. Ramirez*, 540 U.S. 551, 563 (2004) (finding invalid warrant that authorized seizure of suspect's house and that failed to identify any particular items and explaining that "a search warrant for 'evidence of crime' was '[s]o open-ended' in its description that it could 'only be described as a general warrant'") (quoting *United States v. Stefonek*, 179 F.3d 1030, 1032-33 (7th Cir. 1999)); *United States v. Kow*, 58 F.3d 423, 427-28 (9th Cir. 1995) (warrant overbroad where it authorized widespread seizure of documents at business even though affidavit contained only probable cause pertaining to profit skimming and tax violations); *United States v. Cardwell*, 680 F.2d 75, 77 (9th Cir. 1982) (warrant overbroad where it permitted seizure of all of "appellants' business papers" that were "instrumentality or evidence of violation of the general tax evasion statute"). For example, if an individual is suspected of using a phone to engage in criminal activity in the park during the day, what is the probable cause to obtain signaling data from the phone she uses when she is at home at night? The constitution "demands" that the surveillance "be conducted in such a way as to minimize the" collection of information unsupported by probable cause. *United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992) (adopting minimization and other requirements, in addition to probable cause, for warrants to conduct video surveillance).

In addition, an IMSI catcher also scoops up information from the devices of innocent third parties as to whom the government has no probable cause, or reasonable suspicion, whatsoever. *See United States v. Whitney*, 633 F.2d 902, 907 (9th Cir. 1980) ("The command to search can never include more than is covered by the showing of probable cause to search.") (internal quotation marks, citation omitted).

In short, IMSI catchers operate in indiscriminate fashion, scooping up too much information, from too many people. This is precisely the type of general rummaging prohibited by the Fourth Amendment.

C. Statutory orders do not suffice to authorize IMSI catcher use

At a minimum, however, the government should presumptively obtain a probable cause warrant because the government's use of an IMSI catcher constitutes a Fourth Amendment search and/or seizure. *See supra* Section VI-A; *Kyllo*, 533 U.S. at 40 (surveillance that constitutes "search" is "presumptively unreasonable without a warrant").

DOJ contends that a Pen/Trap or hybrid order suffices. *See supra* Section III-B&C. But these statutory orders – based on "relevant" or "relevant and material" standards (*see* 18 U.S.C. § 3122(b)(2); 18 U.S.C. § 2703(d)) – do not satisfy the Fourth Amendment's probable cause requirement or other safeguards.

Note also that DOJ materials suggest that the government seeks a Pen/Trap order when using an IMSI catcher to obtain a device's unique numeric identifier, but a hybrid order to obtain location information. *See supra* Section III-B&C. Warrants, rather than statutory orders, should

be obtained in both cases. There is no reason to apply a different legal standard depending on the government's motivation in using the IMSI catcher. This is so because IMSI catcher technology operates in the same fashion and captures the same type of signaling data – and thus invades privacy expectations and property interests, and effects seizures to the same degree – whether the government deploys the device for the purpose of obtaining the unique numeric identifier of a suspect's device in a known location, or the location of a suspect whose device's numeric identifier is known. In both instances, the IMSI catcher engages in the same dragnet.

D. Even if the government obtained a warrant, use of an IMSI catcher is still invalid

Even if a court were to conclude that IMSI catchers are not *per se* violative of the Fourth Amendment and assuming law enforcement obtained a warrant, there are likely strong arguments that use of an IMSI catcher was still illegal. It is impossible to anticipate all of the potential arguments, which will depend on the language of the warrant and the execution of the search. This section sets forth potential challenges that address two alternative scenarios, one in which the warrant and application fail to describe the government's intended use of an IMSI catcher and another in which they do.

1. The government's omission of information about new surveillance technology from a warrant application prevents courts from exercising their constitutional oversight function and would render a warrant invalid

A warrant application for authorization to use an IMSI catcher is very likely to be *inaccurate*. *See supra* Section III-C & V at n.61 (discussing FBI policy of non-disclosure). In particular, it may omit the critical fact that the government intends to use an IMSI catcher, provide affirmatively misleading information that the government intends to use a pen register instead, or fail to provide any information on what the technology is and how it works.⁷⁴

New technology often raises complex and cutting edge constitutional questions. *Cf., e.g., Jones*, 132 S. Ct. at 946-47 (addressing whether installation and monitoring of GPS device constitutes a “search” within the meaning of the Fourth Amendment). These are questions for the courts, and not the government unilaterally, to decide. The Fourth Amendment assigns judicial officers a critical role in ensuring that all aspects of a search are supported by probable cause and are not overly intrusive. *See United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986). Judicial supervision is particularly important with evolving technology, where there is a heightened risk of overly intrusive searches. *See United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (hereinafter “CDT”).

Information about the government's intended use of new technology, and how the technology works, is material to pressing constitutional questions, such as whether all aspects of the search are supported by probable cause. The courts cannot exercise their constitutional oversight function if deprived of this information. A warrant application that fails to disclose the

government's intended use of an IMSI catcher, or to provide basic information about the technology, omits material information. Equally troubling is an application that refers to a "pen register device" when the government actually intends to use an IMSI catcher. Both circumstances require suppression. *See United States v. Rettig*, 589 F.2d 418, 422-23 (9th Cir. 1979) (suppressing information obtained from warrant procured on basis of material omission). At a minimum, however, the defendant in such a case should be entitled to an evidentiary hearing on whether the omission of information about the IMSI catcher is intentional and material. *See Franks v. Delaware*, 438 U.S. 154 (1978).

a. A warrant that fails to disclose the government's intended use of an IMSI catcher is predicated on a material omission

Information about the government's intended use of an IMSI catcher is material. When the government omits this information from its warrant application, it interferes with the court's ability to supervise the search and any evidence obtained from such a search should be suppressed.

The misleading statements and/or omissions are likely to involve: (a) failure to state that the government intends to use an IMSI catcher or, worse, an affirmative statement that the government intends to use a "pen register" device, (b) failure to acknowledge that the IMSI catcher will scoop up all signaling information from phones used by the target, including from phones and at times and locations unrelated to suspected criminal activity, (c) failure to acknowledge that the IMSI catcher will scoop up all signaling information from phones used by third parties as to whom the government lacks probable cause or even reasonable suspicion, and/or (d) failure to acknowledge that IMSI catchers are capable of capturing content and to address whether that function has been disabled on the particular device.⁷⁵

"Just as the Fourth Amendment prohibits warrantless searches generally, so too does it prohibit a search conducted pursuant to an ill-begotten or otherwise invalid warrant." *Bravo v. City of Santa Maria*, 665 F.3d 1076, 1083 (9th Cir. 2011). One of the purposes of the Fourth Amendment's particularity requirement is to "ensure[] that the magistrate issuing the warrant is fully apprised of the scope of the search and can thus accurately determine whether the entire search is supported by probable cause." *Spilotro*, 800 F.2d at 963. In *Rettig*, the Ninth Circuit required suppression where the government withheld material information about the intended scope of the search. 589 F.2d at 422-23 (after failing to obtain warrant for cocaine-related evidence, government went to different magistrate seeking warrant for marijuana-related evidence, and then conducted broad search including for cocaine-related items). "By failing to advise the judge of all the material facts, including the purpose of the search and its intended scope, the officers deprived him of the opportunity to exercise meaningful supervision over their conduct and to define the proper limits of the warrant." *Id.* at 422. "A judicial officer cannot perform the function of issuing a warrant particularly describing the places to be searched and things to be seized," if "the agents withh[o]ld [material] information." *Id.* at 423; *see also Liston v. Cnty. of Riverside*, 120 F.3d 965, 974 (9th Cir. 1997) (finding information material where "the magistrate would not have issued the warrant without requiring additional information and in addition imposing specific restrictions on its execution").⁷⁶

Information that the government intends to use an IMSI catcher would prompt a reasonable magistrate to “require[e] additional information.” *Id.* In ruling on a statutory application to use an IMSI catcher, for example, one court conducted “an *ex parte* hearing . . . with the special agent leading the investigation,” and faulted the government’s application for not “explain[ing] the technology, or the process by which the technology will be used to engage in the electronic surveillance.” *In re StingRay*, 890 F. Supp. 2d at 749. The court was specifically troubled that the application contained “no discussion” about the manner in which the government intended to operate the StingRay, and identified the numerous factual issues it believed material to evaluating the government’s application. *See id.* This included information about “how many distinct surveillance sites they intend to use, or how long they intend to operate the StingRay equipment to gather all telephone numbers in the immediate area. It was not explained how close they intend to be to the Subject before using the StingRay equipment. They did not address what the government would do with the cell phone numbers and other information concerning seemingly innocent cell phone users whose information was recorded by the equipment.” *Id.*

In addition, some IMSI catchers are capable of capturing content. *See supra* Section II. Notification that the government intends to use an IMSI catcher would prompt a reasonable magistrate to inquire whether the device the government proposes to use has such a feature and, if so, whether it has been disabled. *Cf.* 18 U.S.C. § 2518 (setting forth heightened standard for wiretap orders).

Factual information of the type discussed above is necessary for the court to exercise its constitutional duty to “define the proper limits of the warrant.” *Rettig*, 420 U.S. at 422. Such limits include restrictions that would minimize the intrusive impact of the IMSI catcher on the suspect, for example, by setting limits on when, where, and for how long the device is operated (if the suspect is only believed to engage in criminal activity in parks in the afternoon, there is no probable cause to collect information from the suspect when he is sleeping at home at night, particularly when he may be using a different phone at that time and location), as well as by prohibiting interception of content (absent compliance with requirements for a Title III wiretap).

These or similar limitations (*e.g.*, prohibitions against using the device in dense residential areas or at night when third parties are likely to be at home, restrictions on the size of geographic area in which the device is used) would also serve to minimize the intrusion on third parties. In addition to limiting the amount of third-party information collected, there is the question of what to do with any such information (delete it immediately, segregate and redact).⁷⁷ It is for the issuing magistrate, not the government, to determine how best to balance the government’s need for information, third-party privacy, and the need to preserve evidence “helpful to the accused.” *United States v. Gamez-Orduno*, 235 F.3d 453, 461 (9th Cir. 2000) (“[S]uppression of material evidence helpful to the accused, whether at trial or on a motion to suppress, violates due process if there is a reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different.”).

Also noteworthy is any case in which the government submits an application seeking authorization to use a “pen register device,” when the government actually intends to use an IMSI catcher. *See supra* Section III & nn.50 & 51 (discussing template DOJ application). Such an application would be especially misleading. A pen register device, by definition, is “a device or process which records . . . signaling information transmitted by *an instrument or facility*, . . . provided, however, that such information *shall not include the contents* of any communication.” 18 U.S.C. § 3127(3) (emphasis added). The statutory definition does not encompass a device that records signaling information from *multiple* instruments in its vicinity, which is precisely what an IMSI catcher does. Nor does it encompass devices, like IMSI catchers, which are capable of capturing *content*. Relying on the statutory definition of “pen register,” a court would be lulled into believing there were no need to seek additional information about the kind of data intercepted by the IMSI catcher from the target, or to impose restrictions related to third parties.

In short, the failure to apprise the court that IMSI catchers scoop up all signaling information from target and third-party cell phones leaves a court in the dark about the “intended scope” of the search and thus deprives the court “of the opportunity to exercise meaningful supervision over [the officers’] conduct and to define the proper limits of the warrant.” *Rettig*, 589 F.2d at 422.⁷⁸ A warrant procured under these circumstances can “bec[o]me an instrument for conducting a general search.” *Id.* at 423. As a result, “all evidence seized during the search must be suppressed.” *Id.*⁷⁹

b. A defendant is entitled to a *Franks* hearing

Alternatively, a defendant should be entitled to an evidentiary hearing under *Franks* to determine whether the affidavit misrepresented or omitted material facts. “To allow a magistrate to be misle[]d . . . could denude the probable cause requirement of all meaning. Accordingly, a Fourth Amendment violation occurs where the affiant intentionally or recklessly omitted facts required to prevent technically true statements in the affidavit from being misleading.” *Liston*, 120 F.3d at 973 (internal quotation marks, citations omitted). A defendant seeking a *Franks* hearing must “make[] a two-fold showing: intentional or reckless inclusion or omission, and materiality.” *United States v. Bennett*, 219 F.3d 1117, 1124 (9th Cir. 2000).

Omissions or misrepresentations pertaining to the government’s intended use of an IMSI catcher are material for the reasons discussed above. *See supra* Section VI-D-1-a. They are also intentional.

In court-filed pleadings, the FBI has acknowledged that it has a longstanding policy of not disclosing information about IMSI catchers.⁸⁰ In addition, an internal email from the United States Attorney’s Office for the Northern District of California shows that “many” law enforcement agents in that district, under the auspices of pen register orders, were using the device – but without “mak[ing] that explicit” in the application; even worse, this occurred *after* the federal magistrates had expressed “collective concerns” that pen register orders would not suffice to authorize use of the device.⁸¹ An email produced in discovery in *Rigmaiden* stated that the investigative team “need[ed] to develop independent probable cause of the search warrant . . . FBI does not want to disclose the [redacted] (understandably so).”⁸² In addition, the Sarasota

Police Department in Florida acknowledged, in an email obtained by the ACLU of Florida through a public records request, that, “at the request of U.S. Marshalls,” local police officers “simply refer to [information from an IMSI catcher] as ‘ . . . information from a confidential source regarding the location of the suspect.’ To date this has not been challenged . . . ”⁸³ All of this demonstrates that the government’s omission of information about IMSI catchers – or affirmative misrepresentation that it is instead using a “pen register” device or obtaining information from a “confidential source” – is hardly innocent.⁸⁴

Even in the absence of such stark revelations, it seems clear that misrepresentations and omissions pertaining to the government’s use of IMSI catchers are intentional. The issue is not whether the government should have followed-up on or disclosed facts not of its own making. *Cf. Bravo*, 665 F.3d at 1087, 1088 (where officer obtained a warrant to search home, even though he knew that suspect had received two-year prison sentence and thus not likely to be living at his prior residence, officer’s “failure to . . . follow up and inquire about [the suspect’s] custody status amounted to at least reckless disregard for the truth”). The government cannot disclaim responsibility for knowing what device it has chosen to use.

Nor can ignorance about the technology excuse any omission. The functioning of the technology has constitutional significance. It is therefore incumbent on the government to understand the technology and disclose it to the courts. *See In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(D)*, Nos. C-12-670M, C-12-671M, 2012 WL 4717778 *702 (S.D. Tex. Sept. 26, 2012) (rejecting application for so-called “cell tower dump,” *i.e.*, all information from specified cell towers: “[I]t is problematic that neither the assistant United States Attorney nor the special agent truly understood the technology involved in the requested applications. Without such an understanding, they cannot appreciate the constitutional implications of their requests. They are essentially asking for a warrant in support of a very broad and invasive search affecting likely hundreds of individuals in violation of the Fourth Amendment.”).

* * *

In short, to the extent the warrant application fails to alert the issuing magistrate that the government intends to use an IMSI catcher, misleadingly states it intends to use a “pen register,” or fails to provide basic information about what the technology is and how it works, the omissions are intentional and material. The defendant in such a case is therefore entitled to suppression or a *Franks* hearing, to ensure that the government is not permitted to conduct searches “pursuant to an ill-begotten or otherwise invalid warrant.” *Bravo*, 665 F.3d at 1083.

2. A warrant that accurately describes the IMSI catcher’s capabilities would be facially invalid

For the reasons discussed above, a warrant and application that *inaccurately* describes the government’s intended use of an IMSI catcher should be held invalid. But it is possible that a warrant and application will *accurately* describe the proposed use of the device. In that, somewhat less likely event, the warrant will almost certainly fail to satisfy particularity or breadth requirements and should thus be held facially invalid.

Particularity. “Particularity is the requirement that the warrant must clearly state what is sought.” *In re Grand Jury Subpoenas v. United States*, 926 F.2d 847, 856 (9th Cir. 1991). This means that the warrant must contain “limitations on which [items] within each category [can] be seized [and] suggest[] how they relate[] to specific criminal activity.” *Kow*, 58 F.3d at 427. A warrant is not sufficiently particular if it “provide[s] the search team with discretion to seize records wholly unrelated to the” “crimes and individuals under investigation.” *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 705 (9th Cir. 2009). A warrant that expressly authorizes the search that an IMSI catcher will actually perform – a dragnet for *all* signaling information from the suspect’s wireless device and *all other* devices in the vicinity of the IMSI catcher – contains no practical limitations on the scope of the search and will authorize the government to search and seize information entirely unrelated to the specific criminal activity of which the target is suspected, as well as information from innocent third parties.

To be sure, courts will sustain warrants with “generic descriptions” of the information to be searched and seized “where the government lacked information necessary to describe the items to be seized more precisely.” *Spilotro*, 800 F.2d at 966. But warrants involving IMSI catchers involve impermissibly “generic descriptions” because of the government’s choice to use a technology that scoops up far more information than what actually “relate[s] to specific criminal activity.” *Kow*, 58 F.3d at 427. That knowing choice does not excuse reliance on “generic descriptions.” Indeed, the fact that searches performed by IMSI catchers are not susceptible of being described with particularity underscores the grave concern that IMSI catchers engage in the very general rummaging prohibited by the Fourth Amendment. *See Garrison*, 480 U.S. at 85 (“By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the [particularity] requirement ensures that the search will be carefully tailored to its justification, and will not take on the character of the wide-ranging exploratory searches the framers intended to prohibit.”); *CDT*, 621 F.3d at 1176 (noting, in context of searches for electronic information, “serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant”).

Overbreadth. Any warrant that accurately describes the search performed by an IMSI catcher but that fails to impose explicit restrictions on how and when it is used would also be overbroad because it would authorize the government to search and seize information from the defendant unrelated to specific suspected criminal activity and also information pertaining to third parties as to whom it lacks any probable cause.

“Courts have repeatedly invalidated warrants authorizing a search which exceeded the scope of the probable cause shown in the affidavit.” *In re Grand Jury Subpoenas*, 926 F.2d at 857. A warrant is overbroad where the affidavit establishes probable cause to seize some but not all materials from the target of an investigation. *See, e.g., Kow*, 58 F.3d at 427-28 (warrant overbroad where it authorized widespread seizure of documents at business even though affidavit contained only probable cause pertaining to profit skimming and tax violations); *Center Art Galleries-Hawaii, Inc. v. United States*, 875 F.2d 747, 750 (9th Cir. 1989) (warrant overbroad where it “failed to limit the warrants to items [at art gallery] pertaining to the sale of Dali artwork despite the total absence of any evidence of criminal activity unrelated to Dali”); *Spilotro*, 800

F.2d at 965 (warrant invalid and “authorization to seize ‘gemstones and other items of jewelry’ [from business] was far too broad” because affidavit only established probable cause pertaining to a few stolen diamonds).

Absent explicit restrictions on how and when it is used, an IMSI catcher would intercept all information from a target’s phone about location and calls made, not merely location and calls pertaining to suspected criminal activity. If used to identify the numeric identifier of the phone(s) used by a suspect, it would also intercept the information from *all* phones used by the suspect, not only the phone used in connection with suspected criminal activity.⁸⁵ *See supra* Section VI-A (discussing why interception of this information gives rise to a search and seizure).

While the suppression analysis will focus largely on the information obtained from the defendant, it is also worth noting the impact on third parties. Courts are sensitive to overbreadth issues when the search extends to third parties as to whom there is no probable cause at all. In *Maryland v. Garrison*, the affidavit established probable cause to search the residence of one individual, who was identified as living on the third floor of a particular apartment building; the building, it turned out, had two units on the third floor and the question was whether the search of the second unit was lawful. 480 U.S. at 81. “Plainly,” the Court emphasized, “if the officers had known, or even if they should have known, that there were two separate dwelling units on the third floor of [the building], they would have been obligated to exclude respondent’s apartment from the scope of the requested warrant.” *Id.* at 85. *Garrison* thus makes clear that officers are obligated to exclude from the scope of a requested warrant third parties as to whom they lack probable cause.⁸⁶

Severability and suppression. The Ninth Circuit “follow[s] the rule that where invalid portions of a warrant may be stricken and the remaining portions held valid, seizures pursuant to the valid portions will be sustained.” *Spilotro*, 800 F.2d at 967. But “[i]f no portion of the warrant is sufficiently particularized to pass constitutional muster, then total suppression is required. Otherwise the abuses of a general search would not be prevented.” *Cardwell*, 680 F.2d at 78 (citation omitted). When confronted with an insufficiently particularized or an overbroad warrant, a court must therefore first determine whether the defective portions of the warrant are severable.

Relevant to the analysis is whether improperly authorized “items were set forth in textually severable portions.” *Spilotro*, 800 F.2d at 968. It is exceedingly unlikely that a warrant authorizing use of an IMSI catcher would use a formulation that distinguishes between signaling information from the suspect’s device that pertains to suspected criminal activity and signaling information that does not, or distinguishes between signaling information from the target device and third-party devices. To the extent the warrant does not contain “identifiable portions [that are] sufficiently specific and particular to support severance,” severance is not available. *Id.* at 967.

In addition, “severance is not available when the valid portion of the warrant is ‘a relatively insignificant part’ of an otherwise invalid search.” *In re Grand Jury Subpoenas*, 926 F.2d at 858 (quoting *Spilotro*, 800 F.2d at 967); *accord Kow*, 58 F.3d at 428. To the extent the

government used an IMSI catcher to conduct a dragnet search for *all* signaling information from the target (even from phones and at times and locations unrelated to suspected criminal activity) and for all signaling information from *all* cell phones in the vicinity of the target (even from third parties as to whom the government lacks probable cause), the information from the target cell phone pertaining to criminal activity would be a “relatively insignificant part” of the warrant and severance would not be available.⁸⁷

Where a warrant is not severable, the remedy is blanket suppression. *See Spilotro*, 800 F.2d at 968 (ordering blanket suppression where warrant not severable); *Cardwell*, 680 F.2d at 78 (same); *Kow*, 58 F.3d at 428, 430 (same).

Good faith exception inapplicable. Courts have typically rejected the argument that the “good faith” exception to the suppression doctrine, *see United States v. Leon*, 468 U.S. 897 (1984), applies where the warrant is facially invalid. *See United States v. Clark*, 31 F.3d 831, 836 (9th Cir. 1994) (where warrant was facially overbroad, “the officers could not reasonably rely on it under the objective test of *Leon*”); *Center Art Galleries-Hawaii*, 875 F.2d at 753 (declining to apply good faith exception where “the warrants contained no meaningful restriction on which documents could be seized”); *Kow*, 58 F.3d at 429 (“when a warrant is facially overbroad, absent *specific assurances* from an impartial judge or magistrate that the defective warrant is valid despite its overbreadth, a reasonable reliance argument fails”). Depending on its language, a warrant authorizing the use of an IMSI catcher is likely “so overbroad that absent some exceptional circumstance, no agent could reasonably rely on them.” *Center Art Galleries-Hawaii*, 875 F.2d at 753.

VI. CONCLUSION

Federal, state, and local law enforcement agencies have been using IMSI catchers to engage in dragnet searches and seizures of information from cell phones without disclosing this use to the courts or criminal defendants. By shrouding this technology in secrecy, the government has succeeded in deploying a highly intrusive form of surveillance. In cases where the government may have used an IMSI catcher, vigorous advocacy is necessary to obtain full discovery and suppression of tainted evidence. Unless criminal defense attorneys pursue these issues aggressively, the government will continue to write its own rules for conducting surveillance, without the benefit of court oversight or an adversarial process.

APPENDIX

Issues to Pursue in Discovery

The following is a non-exhaustive list of issues to pursue in discovery broken into two main topics. One set of issues is intended to ferret out whether the government used an IMSI catcher, and the other presses on the constitutional implications of its use.

A. Was an IMSI catcher used?

1. All subpoenas, court orders, and warrants, as well as applications and affidavits in support thereof, for electronic surveillance, and returns thereto.
2. All information obtained via each such subpoena, court order, or warrant.
3. All documents identifying equipment used to [identify the unique numeric identifier associated with defendant's cell phone] or [identify the geographic location of the defendant's cell phone].
4. All emails, notes, logs, reports (including but not limited to Investigation Details Reports), and any other documents regarding efforts to [identify the unique numeric identifier associated with defendant's cell phone] or [identify the geographic location of the defendant's cell phone].⁸⁸
5. All documents describing or reflecting categories of data (*e.g.*, incoming or outgoing telephone numbers; IP addresses; date, time and duration of call; cell site ID; cell site sector; location area code; signal strength; angle of arrival; signal time difference of arrival; ESN or MIN) obtained through real-time tracking of the location of the defendant's cell phone.⁸⁹
6. All documents reflecting the cell site ID and location area code of the device used to monitor the defendant's cell phone.⁹⁰
7. All documents reflecting the cell site IDs and location area codes collected by the device used to monitor the defendant's cell phone.⁹¹
8. All documents reflecting the GPS coordinates of any device while it was mobile and was used to monitor the defendant's cell phone.⁹²
9. All information obtained through real-time tracking of the location of the defendant's cell phone.⁹³
10. All reports of investigation, location calculations, and other relevant documents authored and/or signed by the individuals who participated in the investigation to [identify to the unique numeric identifier associated with defendant's cell phone] or [identify the geographic location of the defendant's cell phone].
11. All operator's logs, training records, score sheets, certification records, training standards, and training manuals related to the device used to [identify to the unique numeric identifier associated with defendant's cell phone] or [identify the geographic location of the defendant's cell phone].⁹⁴

12. All reports of investigation, location calculations, and other relevant documents reflecting the agencies that participated in the investigation to [identify to the unique numeric identifier associated with defendant's cell phone] or [identify the geographic location of the defendant's cell phone].⁹⁵
13. All test protocols and results of tests performed on the device used to [identify to the unique numeric identifier associated with defendant's cell phone] or [identify the geographic location of the defendant's cell phone], prior to deploying the device on the defendant's cell phone. These test results shall include, but not be limited to, base station survey results of the immediate area where the defendant's cell phone was [identified] or [located].⁹⁶
14. All experts' qualifications, summary of expected testimony, list of cases in which any such expert(s) has testified, and summary of the bases for any expert opinion related to testimony regarding the [identification of the unique numeric identifier associated with defendant's cell phone] or [identification of the geographic location of the defendant's cell phone].

B. If an IMSI catcher was used, the following issues are material to a potential motion to suppress.

1. Topics and document requests that would shed light on the intrusive nature of the IMSI catcher and why its use constituted a search:
 - a. Where was the IMSI catcher used? Was it used to determine that the defendant was inside a private location such as a residence? Was there a trespass to property in connection with its use?
 - (i) All documents reflecting capacity of IMSI catcher to locate cell phones while inside physical structures.
 - (ii) All documents reflecting geographic accuracy with which the IMSI catcher is able to locate the target cell phone.
 - (iii) All documents reflecting path movement of the IMSI catcher, including both the path the device traveled if used on the inside of a vehicle or mounted on an aerial vehicle, and the path the device traveled if carried by a human on foot.
 - b. What kind of information did the IMSI catcher scoop up from the defendant (relevant to whether use constituted a search and also whether search was overbroad, *i.e.*, not limited to information pertaining to defendant's suspected criminal activity)?
 - (i) All documents describing categories of data (*e.g.*, incoming or outgoing telephone numbers; date, time and duration of call; cell site number/sector or other information pertaining to geographic location of cell phone; signal strength; ESN

- or MIN; ping time; content of communications) collected by the IMSI catcher from the defendant's cell phone.
- (ii) All underlying data obtained by the IMSI catcher from the defendant's cell phone.
 - (iii) [If defendant has more than one cell phone and one or more has no connection to any criminal activity:] All documents reflecting the numeric identifiers obtained from defendant's cell phones.
- c. How long was the IMSI catcher used and at what times of day (relevant to whether use constituted a search and also whether search was overbroad, *i.e.*, not limited to information pertaining to defendant's suspected criminal activity)?
- (i) All documents reflecting times during which IMSI catcher was used.
2. Topics and document requests that would shed light on the intrusive nature of the IMSI catcher and why its use constituted a seizure.
- a. Did the IMSI catcher interfere with the defendant's possessory interest in the cell phone?
 - (i) Did the government's use of the IMSI catcher deny the target phone service?
 - (a) All documents related to any agreements or arrangements with the wireless carrier authorizing the IMSI catcher to become part of its network or authorizing the IMSI catcher to monitor a phone that receives service through its network.
 - (b) All documents pertaining to any forwarding of data from defendant's phone to the wireless carrier's network while the IMSI catcher was in operation.⁹⁷
 - (c) All documents reflecting impact of the use of the IMSI catcher on access by the defendant's cell phone to cellular service.
 - (ii) Try to document the fact that the IMSI catcher forces the phone to establish a connection with it and in the process forces the phone to transmit at full power, thus draining the battery faster.⁹⁸
 - (a) All training materials, including but not limited to training records, certification records, training standards, and training manuals related to the device used to [identify to the unique numeric identifier associated with defendant's cell phone] or [identify the geographic location of the defendant's cell phone].⁹⁹

- ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 30 of 46
- (b) All user manuals related to the device used [identify to the unique numeric identifier associated with defendant's cell phone] or [identify the geographic location of the defendant's cell phone].
3. Topics and document requests that would shed light on the constitutionality of any warrant obtained:
- a. What kind of information did the IMSI catcher scoop up from the defendant? *See supra* B-1-b.
 - b. What was the impact on third parties?¹⁰⁰
 - (i) All underlying data obtained by the IMSI catcher, whether or not pertaining to the defendant's cell phone.
 - (ii) All documents reflecting the broadcast radius of the IMSI catcher.
 - (iii) All documents reflecting the number of third-party cell phones with which the IMSI catcher exchanged information.
 - (iv) All documents describing categories of data (*e.g.*, incoming or outgoing telephone numbers; date, time and duration of call; cell site number/sector or other information pertaining to geographic location of cell phone; signal strength; ESN or MIN; ping time) collected by the IMSI catcher from the third-party cell phones.
 - (v) All underlying data obtained by the IMSI catcher from third-party cell phones, replacing any actual unique numeric identifiers with substitute numeric identifiers, to protect third-party privacy interests.
 - (vi) All documents regarding subsequent use or destruction of third-party data obtained by the IMSI catcher.
 - (vii) All documents reflecting impact of the use of the IMSI catcher on access by third-party cell phones to cellular service.
 - (viii) All documents reflecting the data gathered by the IMSI catcher while it conducted base station surveys prior to being used to identify or locate the target cell phone.
 - c. Other
 - (i) All policies and procedures governing IMSI catcher use, including instructions about what court orders if any to seek, what information to present to courts in seeking court authorization, and standard operating procedures for using IMSI catchers to [identify a unique numeric identifier associated with a suspect's cell phone] or [identify the geographic location of a suspect's cell phone].¹⁰¹

The government's obligations under *Brady v. Maryland*, 373 U.S. 83 (1963), and Fed. R. Crim. P. 16 extend to information relevant to a Fourth Amendment motion to suppress. Rule 16 requires the government to disclose in discovery items that are "material to preparing the defense," Fed. R. Crim. P. 16(a)(1)(E), including items that are materials to a possible motion to suppress. *See, e.g., United States v. Thomas*, 726 F.3d 1086, 1096 (9th Cir. 2013) (reversing conviction where government failed to disclose records regarding training and experience of drug-detecting dog); *see also United States v. Budziak*, 697 F.3d 1105, 1111-12 (9th Cir. 2012) ("Materiality is a low threshold; it is satisfied so long as the information in the [document] would have helped [the defendant] prepare a defense."); *United States v. Feil*, 2010 WL 3834978 *1 (N.D. Cal. Sept. 29, 2010) (finding defendants "entitled to discovery on the limited issue of whether the investigation that led to this indictment is tainted by [an illegal] search").

Defendants should be entitled to disclosure of the full extent of the electronic surveillance used against them. Given the grave constitutional concerns raised by IMSI catchers, defendants should have a right to information showing whether the government relied on them; for if it did, defendants would have more than a reasonable probability of prevailing on a motion to suppress. *See Gamez-Orduno*, 235 F.3d at 461 ("[S]uppression of material evidence helpful to the accused, whether at trial or on a motion to suppress, violates due process if there is a reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different.").

Note that the defendant in *Rigmaiden* sought in discovery highly "detailed technical information related to the devices and techniques used during the [location tracking] mission." 844 F. Supp. 2d at 998. The government opposed the discovery, invoking the qualified law enforcement privilege recognized in *Rovario v. United States*, 353 U.S. 53 (1957) (qualified privilege for identity of confidential informants). To avoid disclosure, the government made significant factual and legal concessions – that a StingRay was used and that the device was sufficiently intrusive to constitute a search within the meaning of the Fourth Amendment. *See* 844 F. Supp. 2d at 996. Based on these concessions, the defendant did not obtain all of the information he had sought in discovery. *See Rigmaiden*, 844 F. Supp. 2d at 999 ("Because each of Defendant's reasons for obtaining this information has been satisfied by the government's concessions, no additional disclosure will be required."). But the broad disclosure requests did result in the government making significant factual concessions that were crucial to the defendant's ability to formulate a motion to suppress.

ENDNOTES

¹ Harris, Wireless Products Group Price List, 4 (Sept. 2008), <https://info.publicintelligence.net/Harris-SurveillancePriceList.pdf> (StingRay line of products includes “Intercept Software Package” for GSM phones).

² See Ryan Gallagher, Meet the Machines That Steal Your Phone’s Data, Ars Technica, (Sept. 25, 2013), <http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/> (describing various models of Harris Corporation’s cell site simulators and related equipment); see also Harris, Wireless Products Group, StingRay & AmberJack Product Descriptions, <http://egov.ci.miami.fl.us/Legistarweb/Attachments/34769.pdf> (last visited June 18, 2014); Harris, Wireless Products Group, KingFish (Preliminary) Product Description, 2, <http://egov.ci.miami.fl.us/Legistarweb/Attachments/34771.pdf> (last visited June 18, 2014).

³ See Electronic Privacy Information Center (“EPIC”), EPIC v. FBI – Stingray/Cell Site Simulator, <http://epic.org/foia/fbi/stingray/>. A 2008 PowerPoint on “Cell Site Simulators” includes a slide with the headline: “Increased Investigative Use of Technique” and a large arrow pointing upward (the remainder of the text on the slide is redacted). See Letter from FBI to EPIC Releasing Documents Pursuant to FOIA Request regarding Stingray/Cell Site Simulator Devices, 56 (Dec. 7, 2012), <http://epic.org/foia/fbi/stingray/FBI-FOIA-Release-12072012-OCR.pdf> [hereinafter “FBI FOIA Release to EPIC”] (including “Cellular Tracking and Other Legal Issues,” June 2008 PowerPoint, Slide 28).

⁴ See American Civil Liberties Union (“ACLU”), Stingray Tracking Devices: Who’s Got them?, <https://www.aclu.org/maps/stingray-tracking-devices-whos-got-them> (last visited June 18, 2014).

⁵ For a compilation of known uses of this device by local law enforcement, see ACLU, <https://www.aclu.org/maps/stingray-tracking-devices-whos-got-them> (last visited June 18, 2014). See also, e.g., John Kelly, Cellphone data spying: It’s not just the NSA, USA TODAY, Dec. 8, 2013, <http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/> (records from more than 125 police agencies in 33 states revealed that at least 25 departments own a StingRay); Michael Bott & Thom Jensen, 9 Calif. law enforcement agencies connected to cellphone spying technology, SACRAMENTO NEWS 10, Mar. 6, 2014, <http://www.news10.net/story/news/investigations/watchdog/2014/03/06/5-california-law-enforcement-agencies-connected-to-stingrays/6147381/>.

⁶ See generally Hearing on Electronic Communications Privacy Act (“ECPA”) Reform and the Revolution in Location Based Technologies and Services Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong., 4 (2010) [hereinafter “*Blaze Congressional Testimony*”] available at <http://www.crypto.com/papers/blaze-judiciary-20100624.pdf> (statement of Professor Matt Blaze).

⁷ Letter from US Department of Justice (“DOJ”) to ACLU of Northern California attaching USA Book, Electronic Surveillance Manual Chapter XIV, 2 (Aug. 22, 2013), available at <https://www.aclunc.org/sr03> [hereinafter USA Book, Electronic Surveillance Manual Chapter XIV] (obtained by the ACLU of Northern California in FOIA litigation).

⁸ See Stephanie K. Pell & Christopher Soghoian, A Lot More Than a Pen Register, and Less Than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities, 16 YALE J. OF L. & TECH. 134, 145-46

(2013-14) [hereinafter Pell & Soghoian]; Daehyun Strobel, *IMSI Catcher*, Ruhr-Universität, Bochum, Germany, 13 (July 13, 2007) available at http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf [hereinafter Strobel] (“An IMSI Catcher masquerades as a Base Station and causes every mobile phone of the simulated network operator within a defined radius to log in.”). IMSI catchers vary in their operation, depending on among other things, whether the target phone is on a “GSM” (e.g., AT&T) or “CDMA” (e.g., Verizon) network. This paper focuses on the type of StingRays currently in use.

⁹ DOJ Electronic Surveillance Unit, Electronic Surveillance Manual, 44 (June 2005) [hereinafter Electronic Surveillance Manual], <http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf>.

¹⁰ Jennifer Valentino-DeVries, *Judge Questions Tools That Grab Cellphone Data on Innocent People*, WALL ST. J., Oct. 22, 2012, <http://blogs.wsj.com/digits/2012/10/22/judge-questions-tools-that-grab-cellphone-data-on-innocent-people/>. See also Transcript of Hearing on Motion to Suppress at 16, 23, *Florida v. Thomas*, Fla. Cir. Leon Cnty. Ct. (2010) (No. 2008-CF-3350A), https://www.aclu.org/files/assets/100823_transcription_of_suppression_hearing_complete_0.pdf [hereinafter “*Florida v. Thomas*, Hearing on Motion to Suppress”].

¹¹ Pell & Soghoian, *supra* note 8, at 147 & n.43 (“Investigators can position a StingRay in the vicinity of the target to capture the unique serial number of the target’s phone.”); see also Executive Office for United States Attorneys, *Electronic Investigative Techniques*, 45 U.S. ATTORNEYS’ BULLETIN 5, Sept. 1997 [hereinafter Electronic Investigative Techniques], http://www.justice.gov/usao/eousa/foia_reading_room/usab4505.pdf at 13; *In re Application for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device*, 890 F. Supp. 2d 747, 748 (S.D. Tex. 2012) (addressing request to use an IMSI catcher to identify telephone number of subject of investigation; application for court order stated that device would “detect radio signals emitted from wireless cellular telephones in the vicinity of the [Subject] that identify the telephones (e.g., by transmitting the telephone’s serial number and phone number) to the network for authentication” and that “[b]y determining the identifying registration data at various locations in which the [Subject’s] Telephone is reasonably believed to be operating, the telephone number corresponding to the [Subject’s] Telephone can be identified”); Criminal Complaint, *United States v. Arguijo*, No. Under Seal (D. Ill. Feb. 13, 2012), Affidavit in support of Criminal Complaint at 8 ¶10 n.1, http://www.justice.gov/usao/iln/pr/chicago/2013/pr0222_01d.pdf (“On or about July 27, 2012, pursuant to the Court’s Order, law enforcement officers familiar with Chaparro’s appearance, having previously viewed photographs of him and observed him during prior surveillance, used a digital analyzer device on three occasions in three different locations where Chaparro was observed to determine the IMSI associated with any cellular telephone being carried by Chaparro. Using the digital analyzer device, in conjunction with surveillance of Chaparro, law enforcement determined that the telephone number bearing IMSI 316010151032079 was in the same vicinity in the three separate locations where Chaparro was observed.”).

¹² IMSI is “a unique number burned into a removable security identify module (SIM) card that identifies a cell phone subscriber used in GSM and UMTS networks.” Thomas A. O’Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, 59 U.S. ATTORNEYS’ BULLETIN 6, Nov. 2011 [hereinafter O’Malley],

http://www.justice.gov//usao/eousa/foia_reading_room/usab5906.pdf at 16, 20.

¹³ The ESN, used in a CDMA network, consists of a unique 32-bit number assigned to the phone by the manufacturer. It is stored within the phone's permanent memory, rather than on a removable SIM card, and typically cannot be changed by the phone's user. *See* Telecommunications Industry Association, Electronic Serial Number Manufacturer's Code Assignment Guidelines and Procedures Ver. 2.0, 6-7, 12 (Aug. 2008), http://ftp.tiaonline.org/wcd/WCD%20Meeting%20Sept.%204%202008/WCD-20080904-002_ESN_Guidelines_v2.0.pdf. The ESN is used by a carrier to connect the phone to a subscriber account. *See* MobileBurn, What is "ESN?", <http://www.mobileburn.com/definition.jsp?term=ESN> (last visited June 18, 2014); Andy Hellmuth, What is an ESN, and Why Should I Care?, (Sept. 16, 2011) <http://www.buymytronics.com/blog/post/2011/09/16/What-Is-An-ESN-And-Why-Should-I-Care.aspx>.

¹⁴ The MIN is a “34-bit number that is a digital representation of the 10-digit [telephone] number assigned to a [cell phone].” 3rd Generation Partnership Project 2 “3GPP2”, Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems, § 1.2.1, 1.2 (Dec. 1999), http://www.3gpp2.org/public_html/specs/c.s0016-0with3gcover.pdf. The MIN is “a unique provider-assigned number for each cell phone in the cellular provider’s network.” O’Malley at 20.

¹⁵ *See* DOJ, Office of Enforcement Operations Criminal Division, Electronic Surveillance Issues, 153 (Nov. 2005) [hereinafter Electronic Surveillance Issues], <http://www.justice.gov/criminal/foia/docs/elec-srvlnce-issuse.pdf>; Letter from Harris Corporation to Raul Perez, City of Miami PD, Law Enforcement Trust Fund Sole Source Vendor Letter, 6 (Aug. 25, 2008), <http://egov.ci.miami.fl.us/Legistarweb/Attachments/48003.pdf> (Harris Corporation “AmberJack” operates with other Harris products, “enabling tracking and location of targeted mobile phones”).

¹⁶ *See Florida v. Thomas*, Hearing on Motion to Suppress, *supra* note 10, at 14; USA Book, Electronic Surveillance Manual Chapter XIV, *supra* note 7, at 1.

¹⁷ Electronic Surveillance Manual, *supra* note 9, at 41 (“In order to provide service to cellular telephones, providers have the technical capability to collect information such as the cell tower nearest to a particular cell phone, the portion of that tower facing the phone, and often the signal strength of the phone. Depending on the number of towers in a particular area and other factors, this information may be used to identify the location of a phone to within a few hundred yards . . . Carriers generally keep detailed historical records of this information for billing and other business purposes.”).

¹⁸ *See* Pell & Soghoian, *supra* note 8, at 146-47 (“[U]nlike carrier-assisted surveillance, in which the third-party provider necessarily has knowledge of surveillance performed and copies of records disclosed at the request of law enforcement, the unmediated nature of the StingRay dictates that only the operator of the device has: (1) knowledge that an interception ever took place; and (2) . . . access to the information intercepted. Thus, to the extent that telephone companies are able to act as a proxy for their customers’ privacy interests and may ‘push back’ against overbroad or otherwise improper government surveillance, no such advocate exists for the target when a StingRay is used.”) (footnotes omitted).

¹⁹ *See, e.g.*, PKI Electronic Intelligence, GSM Cellular Monitoring Systems (product brochure), 12, <http://www.docstoc.com/docs/99662489/GSM-CELLULAR-MONITORING-SYSTEMS---PKI-Electronic-#> (last visited June 23, 2014) (device can “locat[e] . . . a target mobile phone with

an accuracy of 2 m[eters]”); Bahia 21 Corporation, Resp. to National Telecommunications Information Administration Notice of Inquiry (Doc. #100504212-0212-01) Requesting Information on Preventing Contraband Cell Phone Use in Prisons, 3 (June 11, 2010), <http://www.ntia.doc.gov/files/ntia/comments/100504212-0212-01/attachments/BAHIA21%20resposne%20to%20NTIA%20NOI.pdf> (a US surveillance vendor offering fixed IMSI catchers to be installed in prisons to detect contraband cell phones, promising 10-15m accuracy of geolocation identification).

²⁰ See *United States v. Rigmaiden*, 844 F. Supp. 2d 982, 996 (D. Ariz. 2012).

²¹ *Florida v. Thomas*, Hearing on Motion to Suppress, *supra* note 10, at 15.

²² See *Blaze Congressional Testimony*, *supra* note 6, at 12 (cell site location information “[i]n legacy systems or in rural areas . . . [may] specify only a radius of several miles, while in a dense urban environment with microcells, it could identify a floor or even a room within a building. How precise sector identity is depends on the particular location of the target and on the layout of the particular carrier’s network.”).

²³ See Pell & Soghoian, *supra* note 8, at 146 & n.36; Electronic Surveillance Manual at 41; Harris, Wireless Products Group Price List, *supra* note 1, at 8 (StingRay line of products includes “Intercept Software Package” for GSM phones); *Active GSM Interceptor*, Ability <http://www.interceptors.com/intercept-solutions/Active-GSM-Interceptor.html> (last visited June 18, 2014) (describing IBIS II device: “The user can control the level of service to the target mobiles, selectively Jam specific mobiles, perform silent calls, call or SMS on behalf of target mobile, change SMS messages ‘on the fly,’ detect change of SIM card or change of handset, and support Direction Finding system and many additional operational features); see also Julian Dammann, Presentation at the University of Bonn Seminar on Mobile Security: IMSI-Catcher and Man-in-the-Middle Attacks, 5 (Feb. 9, 2011), http://cosec.bit.uni-bonn.de/fileadmin/user_upload/teaching/10ws/10ws-sem-mobsec/talks/dammann.pdf [hereinafter Dammann] (“is able to eavesdrop”).

²⁴ See Electronic Surveillance Manual, *supra* note 9, at 41. A wiretap order under Title III requires, among other things, the government to show probable cause to believe that an individual is committing a statutorily enumerated offense, probable cause to believe that “particular communications concerning that offense will be obtained through such interception,” and “normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.” 18 U.S.C. § 2518(3).

²⁵ See, e.g., Pell & Soghoian, *supra* note 8, at 145-46; HANNES FEDERRATH, PROTECTION IN MOBILE COMMUNICATIONS 5 (Günter Müller et al. eds., Multilateral Security in Communications) (1999), available at http://epub.uni-regensburg.de/7382/1/Fede3_99Buch3Mobil.pdf; Strobel, *supra* note 8, at 13 (“possible to determine the IMSIs of all users of a radio cell”). This paper focuses on “active IMSI catchers,” which are the type of IMSI catcher currently and predominantly used by law enforcement. Early models of IMSI catchers were “passive” and merely read transmissions, but did not simulate base stations and force devices to connect with them.

²⁶ Electronic Surveillance Manual, *supra* note 9, at 182.

²⁷ Dammann, *supra* note 23, at 19.

²⁸ Electronic Surveillance Manual, *supra* note 9, at 182 n.48.

²⁹ The devices send signals like those emitted by a carrier’s own base stations. See, e.g., Harris, Wireless Products Group, StingRay & AmberJack Product Descriptions, 1

<http://egov.ci.miami.fl.us/Legistarweb/Attachments/34769.pdf> (last visited June 19, 2014) (“Active interrogation capability emulates base stations”). Those signals, of course, “penetrate walls” (necessarily, to provide connectivity indoors). AT&T, *What You Need to Know About Your Network*, <http://www.att.com/gen/press-room?pid=14003> (last visited June 19, 2014); *see also* E.H. Walker, *Penetration of Radio Signals Into Buildings in the Cellular Radio Environment*, 62 THE BELL SYSTEMS TECHNICAL J. 2719 (1983) available at <http://www.alcatel-lucent.com/bstj/vol62-1983/articles/bstj62-9-2719.pdf>.

³⁰ Strobel, *supra* note 8, at 13.

³¹ See USA Book, Electronic Surveillance Manual Chapter XIV, *supra* note 7, at 1 (“A cell site simulator, digital analyzer, or a triggerfish can electronically *force a cellular telephone to register* its mobile identification number (“MIN,” i.e., telephone number) and electronic serial number (“ESN,” i.e., the number assigned by the manufacturer of the cellular telephone and programmed into the telephone) when the cellular telephone is turned on”) (emphasis added).

³² *Florida v. Thomas*, Hearing on Motion to Suppress, *supra* note 10, at 15; *see also id.* at 12 (“[W]e emulate a cellphone tower. [S]o just as the phone was registered with the real verizon tower, we emulate a tower; we *force* that handset to register with us.”) (emphasis added).

³³ USA Book, Electronic Surveillance Manual Chapter XIV, *supra* note 7, at 1.

³⁴ See Electronic Investigative Techniques, *supra* note 11, at 13-15, 23; Electronic Surveillance Manual, *supra* note 9, at 41; USA Book, Electronic Surveillance Manual Chapter XIV, *supra* note 7, at 1; *see generally* Electronic Surveillance Issues, *supra* note 15.

³⁵ The ACLU of Northern California has filed two FOIA lawsuits to obtain DOJ’s policies, practices, and procedures regarding location tracking in general and StingRays in particular. DOJ has resisted producing the materials and the litigation is on-going. See *ACLU of Northern California et al. v. Dep’t of Justice*, No. 12-cv-4008-MEJ (N.D. Cal. filed July 31, 2012) and *ACLU of Northern California v. Dep’t of Justice*, No. 13-cv-3127-MEJ (N.D. Cal. filed July 8, 2013); *see also* Linda Lye, Fighting for Transparency, ACLU of Northern California Blog (July 31, 2012), <https://www.aclunc.org/blog/fighting-transparency> and Linda Lye, ACLU Sues Government for Information About “Stingray” Cell Phone Tracking, ACLU of Northern California Blog (July 8, 2013), <https://www.aclunc.org/blog/aclu-sues-government-information-about-stingray-cell-phone-tracking>.

³⁶ Reporter Beau Hodai, represented by the ACLU of Arizona, has sued the city of Tucson and the Tucson Police Department for failing to disclose IMSI catcher documents in response to a public records request. See *Hodai v. City of Tucson*, No. C20141225 (Ariz. Super. Ct. filed Mar. 4, 2014). An affidavit by Lieutenant Kevin Hall of the Tucson Police Department attached to the defendants’ verified answer, filed on April 14, 2014, states: “I am not aware of a use of this equipment by the Tucson Police Department wherein a warrant was obtained by the Tucson Police Department” and “In each of the five cases where I personally know that the technology was used, there is no written record of that use in the respective case reports and other documents, and no public record that I can find documenting the use of the technology in those cases.” Hall Aff. at ¶¶10, 14, available at <http://bloximages.chicago2.vip.townnews.com/azstarnet.com/content/tncms/assets/v3/editorial/6/7f/67fb460f-c2f6-51b9-8639-a36371622133/537d2509b468c.pdf.pdf>. And in Sacramento, “[d]espite evidence showing the sheriff’s department is utilizing the device, the Sacramento County District Attorney’s Office and Sacramento Superior Court judges said they have no knowledge of StingRays or similar tools being used in Sacramento.” Thom Jensen & Michael

Bott, *Is sheriff's department using tracking and data-collecting device without search warrants?*, SACRAMENTO NEWS 10, June 23, 2014,

<http://www.news10.net/story/news/investigations/2014/06/23/is-sacramento-county-sheriff-dept-using-stingray-to-track-collect-data/11296461/>.

³⁷ See *Smith v. Maryland*, 442 U.S. 735, 736 & n.1 (1979); *United States v. Garcia-Villalba*, 585 F.3d 1223, 1226 (9th Cir. 2009).

³⁸ 18 U.S.C. § 3127(3) & 3127(4), amended by Patriot Act, Pub. L. No. 107-56, Title II, § 216(c)(2)(A) & (3)(A), 215 Stat. 290 (2001).

³⁹ See Electronic Surveillance Manual, *supra* note 9, at 41, 47-48.

⁴⁰ See *id.* at 182 n.48.

⁴¹ See FBI FOIA Release to EPIC, *supra* note 3, at 32-33, 36-37 (Slides 1-2, 5-6).

⁴² See USA Book, Electronic Surveillance Manual Chapter XIV, *supra* note 7, at 1 (“a pen register/trap and trace order *must be obtained* by the government before it can use its own device to capture the ESN or MIN of a cellular telephone, even though there will be no involvement by the service provider”) (emphasis added).

⁴³ 47 U.S.C. § 1002(a)(2); H.R. Rep. 103-827(I) (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3489-90.

⁴⁴ 47 U.S.C. § 1002(a)(2)(B).

⁴⁵ Electronic Surveillance Manual, *supra* note 9, at 47.

⁴⁶ See *id.* at 42-44; see also RICHARD M. THOMPSON, CONG. RESEARCH SERV., R42109, GOVERNMENTAL TRACKING OF CELL PHONES AND VEHICLES: THE CONFLUENCE OF PRIVACY, TECHNOLOGY, AND LAW, 12 (2011) [hereinafter Thompson], available at <https://www.fas.org/sgp/crs/intel/R42109.pdf>.

⁴⁷ See 47 U.S.C. § 1002(a)(2)(B).

⁴⁸ 18 U.S.C. § 2703(d).

⁴⁹ See *In re Application for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d 304, 310 n.6 (3d Cir. 2010) (citing cases); *Espudo*, 954 F. Supp. 2d at 1038-39 (“A significant majority of courts have rejected the hybrid theory and has found that real-time cell site location data is not obtainable on a showing of less than probable cause. A minority of courts, on the other hand, have found that it is.”) (citations omitted); Thompson, *supra* note 46, at 13-14 (citing cases).

⁵⁰ See Electronic Surveillance Manual, *supra* note 9, at 175-87 (“Combined 3123/2703 Application”).

⁵¹ One of the requests built into the template is authorization to permit installation and use of the “pen register and trap and trace device not only on the Subject Telephone Number[s], but also . . . on any cellular phone that is within close proximity to the government device that may autonomously register with the device” See *id.* at 181-82 (emphasis added). A pen register or trap and trace device would not cause cellular phones within a target phone’s vicinity to register autonomously; an IMSI catcher would. The footnote to this template request goes on to describe the device as one that is “used to receive radio signals, emitted from a wireless cellular telephone, that merely identify that telephone to the network (*i.e.*, registration data).” See *id.* at n.48. This, too, appears to describe the operation of an IMSI catcher. Notably, the footnote also takes the position that the device does *not* constitute a pen register or trap and trace device (and that the application is nonetheless submitted “out of an abundance of caution”), and cites one of the few known cases expressly addressing use of an IMSI catcher. See *id.* (citing *In the Matter*

of the Application of the U.S. for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer, 885 F. Supp. 197, 201 (C.D. Cal. 1995). See *infra* Section IV discussing this and other cases on IMSI catchers.

⁵² Affidavit in Support of N.D. Cal. Order 08-90330 ¶42, at 34, *United States v. Rigmaiden*, No. 08-cr-00814-DGC (D. Ariz. Jan. 4, 2012), ECF No. 920-1 (Lye Decl., Exh. 2), available at <https://www.aclunc.org/sr04>. Sample IMSI catcher orders introduced by the government in the same case similarly provided no information about the unique and intrusive ways in which an IMSI catcher functions. See, e.g., Supplemental Memorandum to Government’s Response to Defendant’s Motion to Suppress, Exhibit 1 ¶¶3-4, at 2, *United States v. Rigmaiden*, No. 08-cr-00814-DGC (D. Ariz. Jan. 4, 2012) [hereinafter “Sample IMSI Catcher Order”], ECF No. 986-1 (Sample IMSI Catcher Order Application from a Warrant for a Tracking Device in District of Arizona proceeding, case number redacted), available at <https://www.aclunc.org/sr05>, (“Applicant requests . . . authorization to install, operate, and monitor the mobile tracking device. . . . The United States seeks the cellular telephone location information on an ongoing and real-time basis, including but not limited to identifying the specific nearest cell sites activated or accessed by the target[’]s cellular telephone, and identifying the signal direction and strength of communications between the activated cell site(s) and the targets[’]s cellular telephone. The United States does not seek the content of any wire or electronic communications. Used in this manner, the cellular telephone location information will generate data to track the general location of the user of the target cellular telephone.”). There is no reference in these *filed* applications and orders to the fact that “any cellular phone that is within close proximity to the government device . . . may autonomously register with the device.” Electronic Surveillance Manual, *supra* note 9, at 182 (sample application for hybrid order to use IMSI catcher).

⁵³ See Sample IMSI Catcher Order, *supra* note 52.

⁵⁴ U.S. CONST. amend IV.

⁵⁵ See 18 U.S.C. §§ 3127(3), (4) (defining pen register and trap and trace devices to include not only incoming and outgoing numbers but also “signaling information”).

⁵⁶ See *supra* Section III-C (discussing hybrid orders).

⁵⁷ See Brief Amici Curiae in Support of Daniel Rigmaiden’s Motion to Suppress at 7, *United States v. Rigmaiden*, No. 08-cr-00814-DGC (D. Ariz. Jan 4, 2012), ECF No. 904-3, available at https://www.aclu.org/files/assets/rigmaiden_amicus.pdf.

⁵⁸ See, e.g., Jennifer Valentino-Devries, *Judges Questioned Use of Cellphone Tracking Devices*, WALL ST. J., Mar. 27, 2013, <http://blogs.wsj.com/digits/2013/03/27/judges-question-use-of-cellphone-tracking-devices/>; Ellen Nakashima, *Little-known surveillance tool raises concerns by judges, privacy activists*, WASH. POST, Mar. 27, 2013, http://www.washingtonpost.com/world/national-security/little-known-surveillance-tool-raises-concerns-by-judges-privacy-activists/2013/03/27/8b60e906-9712-11e2-97cd-3d8c1afe4f0f_story.html; Linda Lye, DOJ Emails Show Feds Were Less Than ‘Explicit’ With Judges On Cell Phone Tracking Tool, ACLU of Northern California Blog (Mar. 27, 2013), <https://www.aclu.org/blog/national-security-technology-and-liberty/doj-emails-show-feds-were-less-explicit-judges-cell>.

⁵⁹ See *Florida v. Thomas*, Hearing on Motion to Suppress, *supra* note 10, at 12 (“[W]e emulate a cellphone tower. So just as the phone was registered with the real Verizon tower, we emulate a tower; we force that handset to register with us. We identify that we have the correct handset

and then we're able to, by just merely direction finding on the signal emanating from that handset – we're able to determine a location.”).

⁶⁰ The brief filed by the defendant in the intermediate appellate court stated that “The ESN and initial location data obtained from the cell phone company, together with the Stingray antenna mounted on the police vehicle, led officers to the corner of a private apartment building where the defendant’s cellular phone was located.” Brief of Defendant-Appellant at 8, *Wisconsin v. Tate*, No. 2012AP336 (Wis. Ct. App. June 5, 2011), available at <https://www.aclunc.org/sr02>. The case was argued in the state Supreme Court on October 3, 2013, but as of the date of this publication, no opinion had yet issued. See Wisconsin Court System, *State v. Bobby L. Tate Case History*,

<http://wscca.wicourts.gov/appealHistory.xsl;jsessionid=1FC6F48B94D421C1C2ED4BA85548AB98?caseNo=2012AP000336&cacheId=B14C504915CF7D52C2700564DA05E6C8&recordCount=1&offset=0&linkOnlyToForm=false&sortDirection=DESC> (last visited June 27, 2014).

⁶¹ See City’s Verified Answer, *Hodai v. City of Tucson*, No. C20141225 (Ariz. Super. Ct. filed Mar. 4, 2014) (aff. of Bradley S. Morrison at 2), available at <http://bloximages.chicago2.vip.townnews.com/azstarnet.com/content/tncms/assets/v3/editorial/6/7f/67fb460f-c2f6-51b9-8639-a36371622133/537d2509b468c.pdf.pdf>.

⁶² See *supra* Section III.

⁶³ According to emails obtained by the ACLU of Florida through a public records request, police officers with the Sarasota Police Department in Florida “[i]n reports or depositions” “simply refer [to information from an IMSI catcher] as ‘... information from a confidential source regarding the location of the suspect.’” They have done so “at the request of the U.S. Marshalls.” See Email from Kenneth Castro, Sergeant, Sarasota Police Department, to Terry Lewis, (Apr. 15, 2009, 11:25 EST) [hereinafter “Email from Kenneth Castro”], available at https://www.aclu.org/sites/default/files/assets/aclu_florida_stingray_police_emails.pdf.

⁶⁴ DOJ’s Electronic Surveillance Manual contains a template “Application for Order Permitting Government To Use Its Own Pen Register/Trap and Trace Equipment (Triggerfish/Digital Analyzer or Similar Device),” which states that the application seeks “an order authorizing the installation and use of a pen register to identify the Electronic Serial Number (ESN) and Mobile Identification Number (MIN) of a cellular telephone (being used by_ (if known)_ (within a (color, make, model of vehicle) (bearing _ state license plate number_)).” Note that although the internal DOJ title for the template refers to the “Triggerfish/Digital Analyzer or Similar Device,” the actual text of the template application nowhere references any device other than a pen register/trap and trace. See Electronic Surveillance Manual, *supra* note 9, at 171-72.

⁶⁵ Particularly in the context of a drug case where a defendant used so-called “burner” phones, frequently replacing one phone with another, the government may have obtained the new telephone number through the “Hemisphere Project,” in which the “government pays AT&T to place its employees in drug-fighting units around the country. Those employees sit alongside Drug Enforcement Administration agents and local detectives and supply them with the phone data from as far back as 1987.” Scott Shane & Colin Moynihan, *Drug Agents Use Vast Phone Trove Eclipsing N.S.A.’s*, N.Y. TIMES, Sept. 1, 2013 at A1, available at <http://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html>. By matching calling patterns, the Hemisphere Project is able to identify replacement phone numbers as targets of an investigation discard old ones. Do not expect to find any reference to the Hemisphere Project, as law enforcement agents are trained “to never refer to Hemisphere in

any official document” and to “keep the program under the radar.” Office of Nat’l Drug Control Policy, *Los Angeles Hemisphere*, Slides 8, 12, available at *Synopsis of the Hemisphere Project*, N.Y. TIMES, Sept. 1, 2013, <http://www.nytimes.com/interactive/2013/09/02/us/hemisphere-project.html>.

⁶⁶ First Submission of Consolidated Exhibits Relating to Discovery and Suppression Issues, Exhibit 34 at 51, *United States v. Rigmaiden*, No. 08-cr-00814-DGC (D. Ariz. Jan 4, 2012), ECF No. 587-2, (Email from Denise L Medrano, Special Agent, Phoenix Field Office, to Albert A. Childress (July 17, 2008 6:01 AM)) (emphasis added), available at <https://www.aclunc.org/sr06>; see also *id.* Exhibit 38 at 12, ECF No. 587-3, (Email from Fred Battista, Assistant United States Attorney, to Shawna Yen (July 17, 2008 3:56 PM): “The main effort now may be to tie the target to the case without emphasis on the [redacted].”), available at <https://www.aclunc.org/sr07>.

⁶⁷ See, e.g., *Thomas v. State*, 127 So. 3d 658, 659-60 (Fla. Ct. App. 2013) (technology used to track suspect to his apartment in a large apartment complex); *United States v. Rigmaiden*, 2013 WL 1932800 *3 (D. Ariz. 2013) (technology used to track suspect to “unit 1122 of the Domicilio apartment complex in Santa Clara”).

⁶⁸ See USA Book, Electronic Surveillance Manual Chapter XIV, *supra* note 7, at 1; *Florida v. Thomas*, Hearing on Motion to Suppress, *supra* note 10, at 12 (“So just as the phone was registered with the real Verizon tower, we emulate a tower; we *force* that handset to register with us.”); *id.* at 17 (“once the equipment comes into play and we *capture* that handset, to make locating it easier, the equipment *forces* that handset to transmit at full power”) (emphases added).

⁶⁹ See *Florida v. Thomas*, Hearing on Motion to Suppress, *supra* note 10, at 15 (“[U]sing portable equipment we were able to actually basically stand at every door and every window in that [apartment] complex and determine, with relative certainty you know, the particular area of the apartment that that handset was emanating from”).

⁷⁰ See *id.* at 12, 15.

⁷¹ See USA Book, Electronic Surveillance Manual Chapter XIV, *supra* note 7, at 1.

⁷² We are not currently aware of IMSI catchers being used over prolonged periods, but this is an issue that should be pursued in discovery.

⁷³ Five justices of the Supreme Court agree that prolonged electronic location tracking, even while a suspect travels in public areas, violates reasonable privacy expectations because it generates a “precise [and] comprehensive” record about intimate details, such as “familial, political . . . and sexual associations.” See *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring); accord *id.* at 964 (Alito, J., concurring). See also *Commonwealth of Massachusetts v. Augustine*, 467 Mass. 230, 254 (2014) (government’s collection of two weeks’ worth of cell site location information from cellular provider invaded reasonable expectations of privacy); *State of New Jersey v. Earls*, 214 N.J. 564, 588 (2013) (holding that New Jersey Constitution “protects an individual’s privacy interest in the location of his or her cell phone”); *People of the State of New York v. Weaver*, 12 N.Y.3d 433, 444-45 (2009) (installation and monitoring of GPS device on vehicle to monitor suspect’s movements over 65-day period constitute search requiring a warrant under New York Constitution); *State of Washington v. Jackson*, 150 Wash. 2d 251, 262, 264 (2003) (installation and use of GPS on vehicle constitutes search and seizure under Washington Constitution because “24-hour a day surveillance possible through use of” device “intrud[es] into private affairs”); *State of Oregon v. Campbell*, 306 Or. 157, 172 (1988) (“use of radio transmitter to locate defendant’s automobile” constituted search under Oregon Constitution; “[a]ny device that enables the police quickly to locate a person or object anywhere within a 40-mile radius, day

or night, over a period of several days, is a significant limitation on freedom from scrutiny”); *State of South Dakota v. Zahn*, 812 N.W.2d 490, 497-98 (2012) (installation and monitoring of GPS device on suspect’s vehicle over 26-day period invaded reasonable expectations of privacy and constituted search within meaning of Fourth Amendment).

⁷⁴ In *Rigmaiden*, the government ultimately acknowledged it used an IMSI catcher, but its affidavit in support of the warrant nowhere referred to the device. The affidavit instead made fleeting references to an unspecified “mobile tracking device” and the only description of how the device works stated “[t]he mobile tracking equipment ultimately generate[s] a signal that fixes the geographic position of the Target [Device].” Affidavit in Support of N.D. Cal. Order 08-90330 ¶42, at 34, *United States v. Rigmaiden*, No. 08-cr-00814-DGC (D. Ariz. Jan. 4, 2012), ECF No. 920-1 (Lye Decl., Exh. 2), available at <https://www.aclunc.org/sr04>. Similarly, in *In re StingRay*, the government’s application requested authorization to install and use “a pen register and trap and trace device”; apparently it was only after the court conducted an *ex parte* hearing with the special agent leading the investigation that the agent “indicated that this equipment designed to capture these cell phone numbers was known as a ‘stingray.’” 890 F. Supp. 2d at 748. The application did “not explain the technology, or the process by which the technology will be used to engage in the electronic surveillance to gather the Subject’s cell phone number.” *Id.* at 749.

⁷⁵ Depending on the language of the warrant, a separate argument turning on *scope* may also be available. See *United States v. Hurd*, 499 F.3d 963, 964 (9th Cir. 2007) (in evaluating whether search falls outside the scope of a warrant, court looks to “the circumstances surrounding the issuance of the warrant, the contents of the warrant, and the circumstances of the search”) (internal quotation marks, citation omitted). If the contents of the warrant nowhere reference an IMSI catcher, it may be possible to argue that the government’s use of the IMSI catcher fell outside the warrant’s *scope* and was thus warrantless.

⁷⁶ *Bravo* and *Liston* are civil cases, but claims by a criminal defendant about materially misleading statements in an affidavit and civil claims of “judicial deception” are governed by the same legal standard. See *Liston*, 120 F.3d at 972.

⁷⁷ In *Rigmaiden*, the government deleted third-party information immediately after it used the IMSI catcher to locate the defendant. See 2013 WL 1932800 at *20. Immediate deletion of this information may mitigate some of the harm to third-party privacy interests, but it also deprives the defendant of concrete evidence regarding the impact of IMSI catchers on third parties as to which the government lacked probable cause, and the extent to which information about the defendant was or was not a “relatively insignificant part of” the government’s overall dragnet. *Spilotro*, 800 F.2d at 967. These issues bear directly on the warrant’s overbreadth and whether blanket suppression is the appropriate remedy. A magistrate alerted to the existence of the third party issue may choose to develop a procedure other than wholesale data purging, such as “[s]egregation and redaction” of third-party information “by specialized personnel or an independent third party.” See *CDT*, 621 F.3d at 1180 (Kozinski, C.J., concurring).

⁷⁸ In *Rigmaiden*, the court denied the motion to suppress, opining that the application’s failure to “disclose that the mobile tracking device would capture from other cell phones,” was a mere “detail of execution which need not be specified under” *Dalia v. United States*, 441 U.S. 238, 258 (1979). *Rigmaiden*, 2013 WL 1932800 at *20. The court distinguished *Rettig* on the ground that in the case before it, the “agents . . . did not seek to capture third-party cell phone and aircard information so they could use it in a criminal investigation, nor is there any evidence that they

used the third-party information in that manner.” *Id.* But the Ninth Circuit in *Rettig* explicitly faulted the government for failing to disclose not only the purpose of the search but also its intended scope. *See* 589 F.2d at 422 (“By failing to advise the judge of all the material facts, including the purpose of the search *and its intended scope*, the officers deprived him of the opportunity to exercise meaningful supervision over their conduct and to define the proper limits of the warrant.”) (emphasis added). Moreover, it is difficult to reconcile core Fourth Amendment prohibitions on searches lacking in probable cause with the *Rigmaiden*’s court’s characterization of this issue as a mere “detail of execution.”

⁷⁹ In *Rigmaiden*, the court found that the *Leon* good faith doctrine applied because the ““agents were using a relatively new technology, and they faced a lack of legal precedent regarding the proper form of a warrant to obtain the location information they sought.”” 2013 WL 1932800 at *31. “There is no precedent,” the court stated, “suggesting that the agent was required to include in his warrant application technical details about the operation of the mobile tracking device.” *Id.* at *32. But it is precisely the lack of legal precedent about IMSI catcher technology and its intrusive effect on third parties that imposes a duty on the officers to seek guidance from the judicial officer. *See Ctr. Art Galleries-Haw.*, 875 F.2d at 753 (“When the officer seeking a warrant is aware of an overbreadth problem, . . . we can reasonably expect the officer to bring the problem to an impartial magistrate’s or judge’s attention and to seek specific assurances that the possible defects will not invalidate the warrant.”); *see also CDT*, 621 F.3d at 1178 (Kozinski, C.J., concurring) (discussing “the government’s duty of candor in presenting a warrant application”).

⁸⁰ *See* City’s Verified Answer, *Hodai v. City of Tucson*, No. C20141225 (Ariz. Super. Ct. filed Mar. 4, 2014) (aff. of Bradley S. Morrison at 2), available at <http://bloximages.chicago2.vip.townnews.com/azstarnet.com/content/tncms/assets/v3/editorial/6/7f/67fb460f-c2f6-51b9-8639-a36371622133/537d2509b468c.pdf.pdf>. (“[T]he FBI has, as a matter of policy, for over 10 years, protected this specific electronic surveillance equipment and techniques from disclosure, directing its agents that while the product of the identification or location operation can be disclosed, neither details on the equipment’s operation nor the tradecraft involved in use of the equipment may be disclosed.”).

⁸¹ The May 23, 2011 email chain was obtained by the ACLU of Northern California through a FOIA request and is available at <https://www.aclu.org/technology-and-liberty/us-v-rigmaiden-doj-emails-stingray-applications>; *see also* Linda Lye, DOJ Emails Show Feds Were Less Than ‘Explicit’ With Judges On Cell Phone Tracking Tool, ACLU of Northern California Blog (Mar. 27, 2013), <https://www.aclu.org/blog/national-security-technology-and-liberty/doj-emails-show-feds-were-less-explicit-judges-cell>.

⁸² First Submission of Consolidated Exhibits Relating to Discovery and Suppression Issues, Exhibit 34 at 51, *United States v. Rigmaiden*, No. 08-cr-00814-DGC (D. Ariz. Jan 4, 2012), ECF No. 587-2, (Email from Denise L Medrano, Special Agent, Phoenix Field Office, to Albert A. Childress (July 17, 2008 6:01 AM)) (emphasis added), available at <https://www.aclunc.org/sr06>.

⁸³ Email from Kenneth Castro, *supra* note 63.

⁸⁴ *Id.*

⁸⁵ As DOJ explains, an IMSI catcher intercepts “necessary signaling data” consisting of a target device’s unique numeric identifier and location whenever the phone is on, and even if it is not being used; when the phone makes or receives a call, an IMSI catcher captures not only the device’s unique numeric identifier and location, but also “the call’s incoming or outgoing status,

the telephone number dialed, [and] the date, time, and duration of the call.” USA Book, Electronic Surveillance Manual Chapter XIV, *supra* note 7, at 1.

⁸⁶ See also *Bravo*, 665 F.3d at 1084-85 (reversing grant of summary judgment for government defendants in civil challenge to lawfulness of search warrant where officer obtained warrant to search home where suspect had previously resided but officer had no evidence that current residents were involved in crime); *Liston*, 120 F.3d at 973-74 (officer not entitled to qualified immunity where he obtained warrant to search home and “for sale” and “sold” signs in front yard indicated third parties other than suspect occupied home).

⁸⁷ While the government is likely to argue that criminal defendants do not have standing to raise third party issues, the argument could be made that information about the IMSI catcher’s the impact on third parties bears on questions of overbreadth and severability.

⁸⁸ In *Rigmaidens*, references to “StingRays” appeared in documents pertaining to the investigation. See Response to Government’s Memorandum Regarding Law Enforcement Privilege, Exhibit 39 at 62, *United States v. Rigmaidens*, No. 08-cr-00814-DGC (D. Ariz. Jan 4, 2012), ECF No. 536-4 (rough notes prepared by IRS-CI Agent Denise L. Medrano) (handwritten checklist: “utility search[,]...tax return search[,] Post office – verifying forwarding info[,] Run plates[,] Review Video[,] Accurint[,] StingRay”), available at <https://www.aclunc.org/sr08>; First Submission of Consolidated Exhibits Relating to Discovery and Suppression Issues, Exhibit 26 at 32, *United States v. Rigmaidens*, No. 08-cr-00814-DGC (D. Ariz. Jan 4, 2012), ECF No. 587-2 (United States Postal Inspection Service Investigation Details Report) (“During the course of this investigation and conferring with TSD agents with the FBI and USPIS, we determined that doing a normal ‘Trap and Trace’ on the aircard would suffice. [redacted] Essentially we would ping the number associated to the card instead of collecting data from the aircard’s connection. . . . On 7/16/08, we were informed that they were able to track a signal and were using a ‘Stingray’ to pinpoint the location of the aircard.”), available at <https://www.aclunc.org/sr09>.

⁸⁹ A Pen/Trap device would capture the following types of data: phone numbers/IP addresses, location area code (which identifies a group of cell sites and is not related to a phone number area code), cell site ID, cell site sector, and possibly signal strength, singal angle of arrival, and signal time difference of arrival (also called signal time of flight). An IMSI catcher would also capture the foregoing types of data, *except* cell site IDs and location area codes being accessed by the target phone. When a phone connects with and accesses the carrier’s network, it accesses cell site IDs and location area codes. When it instead connects with an IMSI catcher, it is no longer accessing the carrier’s network and hence is no longer accessing cell site IDs and location area codes. If the data produced by the government in response to this request includes cell site IDs and location area codes – and those cell site IDs and location area codes match those of the carrier – the device used was a Pen/Trap.

⁹⁰ A Pen/Trap device collects cell site IDs and location area codes but would not have its own cell site ID and location area code. An IMSI catcher, however, has its own cell site ID and location area code – and this cell site ID and location area code would not typically match any in the wireless carrier’s network infrastructure. If the government provides data in response to this request, the device used was an IMSI catcher. This assumes, however, that the prosecution correctly understood the request and did not mistakenly provide cell site IDs and location area codes *collected* by the surveillance device, rather than the cell site ID and location area code *of* the surveillance device. It would be prudent to couple discovery on this issue with a subpoena to the carrier for all location area codes, active cell sites, locations of active cell sites, and the

approximate coverage areas of each active cell site within range of where the defendant's phone was located or identified at the time it was monitored. This would allow comparison between any cell site ID/location area code provided in response to this request with that of the actual carrier.

⁹¹ See *supra* n. 90.

⁹² A typical Pen/Trap device will not log its own GPS coordinates, but an IMSI catcher would. It may not however be programmed to retain its GPS coordinates. If the government provides GPS coordinates of the device used to monitor the target phone – and those coordinates reflect multiple geographical locations, or a single geographical location that is not the location of an actual cell site – the device is an IMSI catcher.

⁹³ It may be prudent to propose that identifying information pertaining to third parties be redacted and replaced with unique numeric identifiers.

⁹⁴ See *United States v. Cedano-Arellano*, 332 F.3d 568, 571 (9th Cir. 2003) (narcotics dog's training logs and certification discoverable under Rule 16). Training materials and reports signed by individuals participating in the investigation (requests 10 and 11) would facilitate the identification of the individuals involved in deploying the IMSI catcher.

⁹⁵ If the investigation were led by a local police department but the FBI or United States Marshals Service participated in tracking the phone, this might be an indication that a federal agency provided its IMSI catcher.

⁹⁶ Law enforcement may use an IMSI catcher to collect information on the carrier's network. An IMSI catcher can be used to conduct a base station survey. A Pen/Trap device would not. If a base station survey is produced in response to this request, an IMSI catcher was used.

⁹⁷ To prevent an interference with service to the defendant's phone, the government would have had to make some kind of arrangement with the carrier that would allow the IMSI catcher to become part of its network or develop a mechanism to forward data from the phone to the carrier's network. If one of these arrangements occurred, some documentation should exist.

⁹⁸ See *Florida v. Thomas*, Hearing on Motion to Suppress, *supra* note 10, at 17 ("[O]nce the equipment comes into play and we *capture* that handset, to make locating it easier, the equipment *forces that handset to transmit at full power.*"') (emphasis added.)

⁹⁹ See *Cedano-Arellano*, 332 F.3d at 571 (narcotics dog's training logs and certification discoverable under Rule 16). Training materials may provide information regarding the operation of the device, which might in turn shed light on forced registration and increased power output.

¹⁰⁰ While the government will likely argue that a defendant has no standing to raise third party issues, there is an argument that the impact on third parties is relevant to overbreadth and severability. See *supra* at Section VI-D-2.

¹⁰¹ This may shed light on whether any omission about IMSI catchers from a warrant affidavit is intentional.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 45 of 46



This publication can be found online at:

<https://www.aclunc.org/publications/stingrays-most-common-surveillance-tool-government-wont-tell-you-about>

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 46 of 46



A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP:¹
WHAT THE STINGRAY TEACHES US ABOUT HOW CONGRESS SHOULD
APPROACH THE REFORM OF LAW ENFORCEMENT SURVEILLANCE
AUTHORITIES²

Stephanie K. Pell* & Christopher Soghoian**

16 YALE J.L. & TECH. 134 (2013)

ABSTRACT

In June 2013, through an unauthorized disclosure to the media by ex-NSA contractor Edward Snowden, the public learned that the NSA, since 2006, had been collecting nearly all domestic phone call detail records and other telephony metadata pursuant to a controversial, classified interpretation of Section 215 of the USA PATRIOT Act. Prior to the Snowden disclosure, the existence of this intelligence program had been kept secret from the general public, though some members of Congress knew both of its existence and of the statutory interpretation the government was using to justify the bulk collection. Unfortunately, the classified nature of the Section 215 metadata program prevented them from alerting the public directly, so they were left to convey their criticisms of the program directly to certain federal agencies as part of a non-public oversight process. The efficacy of an oversight regime burdened by such strict secrecy is now the subject of justifiably intense debate. In the context of that debate, this Article examines a very different surveillance technology—one that has been used by federal, state and local law enforcement agencies for more than two decades without invoking even the muted scrutiny Congress applied to the Section 215 metadata program. During that time, this technology has steadily and significantly expanded the government's surveillance capabilities in a manner and to a degree to date largely unnoticed and unregulated. Indeed, it has never been explicitly authorized

¹ “A little more than kin, and less than kind.” WILLIAM SHAKESPEARE, HAMLET act 1, sc.

2.

² The authors would like to thank Susan Freiwald and Jim Green for their feedback and assistance.

* Principal, SKP Strategies, LLC; Non-resident Fellow at Stanford Law School’s Center for Internet and Society; former Counsel to the House Judiciary Committee; former Senior Counsel to the Deputy Attorney General, U.S. Department of Justice; former Counsel to the Assistant Attorney General, National Security Division, U.S. Department of Justice; and former Assistant U.S. Attorney, Southern District of Florida.

** Principal Technologist, Speech, Privacy & Technology Project, American Civil Liberties Union; Visiting Fellow, Information Society Project, Yale Law School. The opinions expressed in this article are this author’s alone, and do not reflect the official position of his employer.

by Congress for law enforcement use. This technology, commonly called the StingRay, the most well-known brand name of a family of surveillance devices, enables the government, directly and in real-time, to intercept communications data and detailed location information of cellular phones—data that it would otherwise be unable to obtain without the assistance of a wireless carrier. Drawing from the lessons of the StingRay, this Article argues that if statutory authorities regulating law enforcement surveillance technologies and methods are to have any hope of keeping pace with technology, some formalized mechanism must be established through which complete, reliable and timely information about new government surveillance methods and technologies can be brought to the attention of Congress.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 2 of 38

A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

I. INTRODUCTION	136
II. A BRIEF DESCRIPTION OF A STINGRAY AND ITS CAPABILITIES	144
III. IN BETWEEN OR BEYOND THE REACH OF STATUTORY LANGUAGE.....	148
A. <i>Real-time Cell Phone Tracking and Secrecy</i>	149
B. <i>The StingRay and Secrecy</i>	154
1. <i>The 1995 Digital Analyzer Magistrate Opinion</i>	157
2. <i>2012 StingRay Magistrate Opinion</i>	160
IV. WARNINGS FOR LEGISLATORS	163
V. SUGGESTIONS FOR REFORM	165
VI. CONCLUSION	169

I. INTRODUCTION

Beginning in June 2013, the details of several National Security Agency (NSA) classified surveillance programs were revealed in a series of articles by journalists who had received documents from ex-NSA contractor Edward Snowden.³ Among the many disclosures and subsequent releases of information by the Administration and Members of Congress was the revelation that, since 2006, the NSA has been collecting domestic call detail records and other domestic telephony metadata⁴ in bulk, pursuant to a controversial interpretation of Section 215 of the USA PATRIOT Act

³ See Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN, June 5, 2013, <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order> (“The National Security Agency is currently collecting the telephone records of millions of US customers of Verizon, one of America’s largest telecoms providers, under a top secret court order issued in April.”); see also Danny Yadron and Evan Perez, *T-Mobile, Verizon Wireless Shielded from NSA Sweep*, WALL ST. J., June 14, 2013, <http://online.wsj.com/article/SB10001424127887324049504578543800240266368.html> (explaining that the NSA “doesn’t collect information directly from T-Mobile USA and Verizon Wireless . . . [but the NSA] still capture[s] information, or metadata, on 99% of U.S. phone traffic because nearly all calls eventually travel over networks owned by U.S. companies that work with the NSA”).

⁴ The Administration defines this telephony metadata as including “information about what telephone numbers were used to make and receive the calls, when the calls took place, and how long the calls lasted. . . . [T]his information does *not* include any information about the content of those calls—the Government cannot, through this program, listen to or record any telephone conversations.” Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act on Section 215, at 2 (Aug. 9, 2013) [hereinafter Administration White Paper on Section 215], <http://info.publicintelligence.net/DoJ-NSABulkCollection.pdf>.

(PATRIOT Act).⁵ Section 215 is an intelligence collection authority permitting the government to compel “tangible things” from third parties that are “relevant” to an “authorized investigation” in order: (1) “to obtain foreign intelligence information not concerning a United States person”; or (2) to “protect against international terrorism or clandestine intelligence activities.”⁶ The public has also learned that this massive quantity of data is collected and stored in a centralized database in order to enable future searches by the NSA—that is, if and when there is a reasonable articulable suspicion that an identifier (e.g. a phone number) is associated with a particular foreign terrorist organization⁷ or with terrorism.⁸ The goal of the program is “to enable the government to identify communications among known and unknown terrorism suspects, particularly those located inside the United States.”⁹

⁵ For the most complete factual and legal explanation of the 215 metadata program from the Administration to date, see Administration White Paper on Section 215, *supra* note 4. Since the time the Administration chose to declassify and disclose the Section 215 White Paper to the public, two different federal district courts have issued dueling opinions on the legality of this intelligence program. See *ACLU v. Clapper*, No. 13-3994 (WHP) (S.D.N.Y. Dec. 27, 2013) (holding that the 215 bulk collection metadata program is lawful as both a statutory and constitutional matter); *Klayman v. Obama*, No. 13-0851 (RJL) (D.D.C. Dec. 16, 2013) (finding that the plaintiffs have demonstrated a substantial likelihood of success on a claim that the Section 215 metadata program violates the Fourth Amendment).

⁶ 50 U.S.C. § 1861(a)(1).

⁷ See Transcript: Newseum Special Program—NSA Surveillance Leaks: Facts and Fiction 8 (June 26, 2013) (statement of Robert Litt, General Counsel of the Office of Director of National Intelligence), <http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/887-transcript-newseum-special-program-nsa-surveillance-leaks-facts-and-fiction> (“The metadata that is acquired and kept under this program can only be queried when there is reasonable suspicion, based on specific, articulable facts, that a particular telephone number is associated with specified foreign terrorist organizations. And the only purpose for which we can make that query is to identify contacts.”); see also Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J. L. & PUB. POL’Y (forthcoming 2013), <http://justsecurity.org/wp-content/uploads/2013/10/Just-Security-Donohue-PDF.pdf> (explaining that the Foreign Intelligence Court (FISC) “requires that the NSA establish a ‘reasonable, articulable suspicion’ that a seed identifier used to query the data be linked to a foreign terrorist organization before running it against the bulk data. Once obtained, information responsive to the query can be further mined for information. The NSA can analyze the data to ascertain second- and third-tier contacts, in steps known as ‘hops.’”).

⁸ Privacy and Civil Liberties Oversight Board (PCLOB) Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court 8-9, <http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf> [hereinafter PCLOB Report].

⁹ *Id.* at 8.

A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

One major criticism of this domestic surveillance program is that the “common sense” reading of the statutory text of Section 215 does not, on its face, appear to permit collection on this scale. More specifically, critics argue that the contents of an entire massive database of records—in this case the records of nearly every domestic telephone call¹⁰—cannot simply

¹⁰ See Yadron and Perez, *supra* note 3. But see Ellen Nakashima, *NSA is Collecting Less Than 30 Percent of U.S. Call Data, Officials Say*, WASH. POST, Feb. 7, 2014, http://www.washingtonpost.com/world/national-security/nsa-is-collecting-less-than-30-percent-of-us-call-data-officials-say/2014/02/07/234a0e9e-8fad-11e3-b46a-5a3d0d2130da_story.html (“The National Security Agency is collecting less than 30 percent of all Americans’ call records because of an inability to keep pace with the explosion in cellphone use, according to current and former U.S. officials. . . . In 2006, a senior U.S. official said, the NSA was collecting ‘closer to 100’ percent of Americans’ phone records from a number of U.S. companies.”). For the sake of argument, suppose we assume those sources are correct and the NSA is collecting call records pertaining to no more than 30 percent of all domestic calls (presumably not much less, since the officials who were the sources of that figure in the article certainly did not choose that number arbitrarily but according to some rationale regarding an upper limit the government feels it can defend in attempting to mitigate larger figures claimed by other authors to date). Such a figure would still describe a sample justifiably characterized as “massive” in size, leaving the necessity, much less the legality, of collecting a cache of information so large, still quite open to question, whether or not *some* of the records in question are found to be actually relevant to an investigation.

The Administration has attempted to defend its interpretation of relevance:

It is well-settled in the context of other forms of legal process for the production of documents that a document is “relevant” to a particular subject matter not only where it directly bears on that subject matter, but also where it is reasonable to believe that it could lead to other information that directly bears on that subject matter. . . .

In light of that basic understanding of relevance, courts have held that the relevance standard permits requests for the production of entire repositories of records, even when any particular record is unlikely to directly bear on the matter being investigated, because searching the entire repository is the only feasible means to locate the critical documents. More generally, courts have concluded that the relevance standard permits discovery of large volumes of information in circumstances where the requester seeks to identify much smaller amounts of information within the data that directly bears on the matter. Federal agencies exercise broad subpoena powers or other authorities to collect and analyze large data sets in order to identify information that directly pertains to the particular subject of an investigation. Finally, in the analogous field of search warrants for data stored on computers, courts permit Government agents to copy entire computer hard drives and then later review the entire drive for the specific evidence described in the warrant.

be deemed relevant because *some* of the records in that database are actually relevant to an investigation.¹¹

Administration White Paper on Section 215, at 9-10, *supra* note 4 (internal citations omitted).

¹¹ See Orin Kerr, *The Problem With the Administration “White Paper” on the Telephony Metadata Program*, VOLOKH CONSPIRACY (Aug. 12, 2013, 2:34 PM), <http://www.volokh.com/2013/08/12/problem-withthe-administration-white-paper-on-the-telephony-metadata-program> (arguing that the Administration position as expressed in its Section 215 White Paper does not adequately address “whether a massive database of billions of records can be deemed ‘relevant’ because some records inside the database are relevant”); see also Brief of Amicus Curiae, Professors of Information Privacy and Surveillance Law at 10-17, *In Re* Electronic Privacy Information Center, No. 13-58 (Aug. 12, 2013), <http://www.law.indiana.edu/front/etc/section-215-amicus-8.pdf> (arguing that call detail records and telephone metadata on all domestic Verizon calls could not be relevant to an authorized investigation); Donohue, *supra* note 7, at 48-49 (arguing that the telephony metadata program “violates the express statutory language . . . with regard to the language ‘relevant to an authorized investigation’; [and, among other ways,] in relation to [Section 215’s] requirement that the information sought can be obtained under subpoena duces tecum”).

In a recently declassified March 2009 Order from the Foreign Intelligence Surveillance Court (FISC), authorizing domestic bulk collection of metadata under Section 215, Chief Judge Reggie Walton acknowledges that the bulk collection of metadata “pertaining to communications of United States (‘U.S.’) persons located within the U.S. who are not the subject of an FBI investigation” could “not otherwise be legally captured in bulk.” *In re Production of Tangible Things From [REDACTED]*, No. BR 08-13, at 2-3 (FISA Ct. Mar. 2, 2009), http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf.

Nevertheless, the FISC appears to authorize the program because of:

- (1) the government’s explanation, under oath of how the collection of and access to such data are necessary to analytical methods that are vital to the national security of the United States; and (2) minimization procedures that carefully restrict access to the BR metadata and includes specific oversight requirements.

Id. at 11-12.

Three Members of the PCLOB (Chairman David Medine and Board Members Jim Dempsey and Judge Patricia Wald have concluded that the 215 metadata program fails to comply with Section 215’s statutory language. The major arguments for the program’s non-compliance with Section 215 of the PATRIOT Act can be summarized as follows:

First, the telephone records acquired under the program have no connection to any specific FBI investigation at the time of their

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 6 of 38

A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

While the existence of this intelligence program had been kept from the general public prior to the summer 2013 Snowden disclosures and subsequent declassification of information by the Executive branch, some members of Congress knew of its existence and were privy to the statutory interpretation the government was employing to justify the bulk collection of domestic telephone records. Indeed, during a floor debate in 2011, Senator Ron Wyden warned his colleagues that “when the American people find out how their government has secretly interpreted the PATRIOT Act, they will be stunned and they will be angry.”¹²

As this Article goes to print, the Executive and Legislative branches of government are finally engaging the public in a much more robust, transparent discussion about the Section 215 metadata program. Moreover,

collection. Second, because the records are collected in bulk potentially encompassing all telephone calling records across the nation they cannot be regarded as “relevant” to any FBI investigation as required by the statute without redefining the word relevant in a manner that is circular, unlimited in scope, and out of step with the case law from analogous legal contexts involving the production of records. Third, the program operates by putting telephone companies under an obligation to furnish new calling records on a daily basis as they are generated (instead of turning over records already in their possession) an approach lacking foundation in the statute and one that is inconsistent with FISA as a whole. Fourth, the statute permits only the FBI to obtain items for use in its investigations; it does not authorize the NSA to collect anything.

PCLOB Report, *supra* note 8, at 10.

Two other PCLOB Members (Elisabeth Collins Cook and Rachel Brand) did not agree, however, that the 215 metadata program lacked statutory authorization. *See Separate Statement by Board Member Elisabeth Collins Cook at 1,* <http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Cook-Statement.pdf>; *Separate Statement by Board Member Rachael Brand at 3,* <http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Brand-Statement.pdf>.

For a defense or more detailed analysis of the Administration’s interpretation of relevance under Section 215, *see Steven G. Bradbury, Understanding the NSA Programs: Bulk Acquisition of Telephone Metadata Under Section 215 and Foreign-Targeted Collection Under Section 702*, 1 LAWFARE RESEARCH PAPER SERIES (Sept. 1, 2013), <http://www.lawfareblog.com/wp-content/uploads/2013/08/Bradbury-Vol-1-No-3.pdf>; David S. Kris, *On the Bulk Collection of Tangible Things*, 1 LAWFARE RESEARCH PAPER SERIES (Sept. 29, 2013), <http://www.lawfareblog.com/wp-content/uploads/2013/09/Lawfare-Research-Paper-Series-No.-4-2.pdf>.

¹² Press Release, Senator Ron Wyden, In Speech, Wyden Says Official Interpretations of Patriot Act Must be Made Public (May 26, 2011), <http://wyden.senate.gov/newsroom/press/release/?id=34eddcd8-2541-42f5-8f1d-19234030d91e>.

as the Administration continues declassification of Section 215-related documents, several Members of Congress are calling for reforms to the statute, some arguing for termination of the entire Section 215 bulk collection program.¹³ Even President Obama has suggested that the government should no longer hold the data, although the Administration has not yet taken a position on who or what entity should warehouse the voluminous call records and other telephony business records.¹⁴

Meanwhile, a clearer picture of earlier cryptically worded criticisms of the program voiced by members of Congress has emerged. We now know that some members of Congress who were aware of the government's legal interpretation of Section 215 actively urged the Executive branch to engage in a more public discussion of the issue in a manner that would not harm national security. In other words, as controversial as the Section 215 program has come to be in light of the Snowden revelations, prior to those unauthorized disclosures an established process had already enabled at least some measure of congressional oversight and review.¹⁵ That process, in turn, enabled Senators Russ Feingold, Richard Durbin, Wyden, and Mark Udall to warn the public and other members of Congress that the

¹³ See, e.g., The USA Freedom Act of 2013, S. 1599, 113th Cong. (2013); The USA Freedom Act of 2013, H.R. 3361, 113th Cong. (2013) (prohibiting bulk collection of American's records by, among other things, limiting the use of Section 215 to records or tangible things pertaining to: "(A) a foreign power or agent of a foreign power, (B) the activities of a suspected agent of a foreign power who is the subject of . . . [an] authorized investigation, or (C) an individual in contact with, or known to, a suspected agent of a foreign power").

¹⁴ See President Obama's Prepared Remarks on Signals Intelligence Programs 7 (Jan. 17, 2014), <http://justsecurity.org/wp-content/uploads/2014/01/President-Speech-on-Intelligence-Reforms.pdf> ("I am therefore ordering a transition that will end the Section 215 bulk metadata program as it currently exists, and establish a mechanism that preserves the capabilities we need without the government holding this bulk meta-data."); *see also* PCLOB Report, *supra* note 8, at 102 ("[S]anctioning the NSA's program under Section 215 requires an impermissible transformation of the statute . . . Because Section 215 does not provide a sound legal basis for the NSA's bulk telephone records program, we believe the program must be ended."). *But see* Separate Statements of Board Members Elisebeth Collins Cook and Rachael Brand, *supra* note 11 (dissenting from the PCLOB's recommendation to shut down the 215 metadata program).

¹⁵ See *The USA PATRIOT Act: Hearing before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 8 (2009) (oral testimony of Todd M. Hinnen, Deputy Assistant Attorney General), http://judiciary.house.gov/_files/hearings/printers/111th/111-35_52409.PDF ("The business records provision [Section 215] allows the government to obtain any tangible thing it demonstrates to the FISA court is relevant to a counterterrorism or counterintelligence investigation. . . . It also supports an important, sensitive collection program about which many members of the Subcommittee or their staffs have been briefed.")

A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

government was misusing its Section 215 authority, albeit in opaque and suggestive language necessitated by the classified status of the surveillance program.¹⁶ While it is fair to argue that congressional oversight of government intelligence programs is far from ideal, we must at least acknowledge that the government's expansive interpretation and use of Section 215 was known and debated by some Members of Congress—some approving of the program,¹⁷ some not—even if it could not be directly named or described in public until after Edward Snowden's disclosures. The efficacy of an oversight regime burdened by such strict secrecy is now the subject of justifiably intense debate.

In the context of that debate, this Article examines a very different surveillance technology—one that has been used by federal, state and local law enforcement agencies for more than two decades without invoking even the muted scrutiny Congress applied to the 215 metadata program.¹⁸ In that time, this technology has steadily and significantly expanded the government's surveillance capabilities in a manner and to a degree to date largely unnoticed and unregulated—indeed, it has never been explicitly authorized by Congress for law enforcement use.¹⁹ This technology, commonly called the StingRay, the most well-known brand name of a family of surveillance devices known more generically as “IMSI catchers,” is used by law enforcement agencies to obtain, directly and in real time, unique device identifiers and detailed location information of cellular phones—data that it would otherwise be unable to obtain without the

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 9 of 38

¹⁶ See Christopher Soghoian, *Senators Hint at DOJ's Secret Reinterpretation and Use of Section 215 of the Patriot Act*, SLIGHT PARANOIA, May 24, 2011, <http://paranoia.dubfire.net/2011/05/senators-hint-at-doj-s-secret.html> (describing statements by Senators hinting at the existence of an alternate use of Section 215).

¹⁷ See Ed O'Keefe, *Transcript: Dianne Feinstein, Saxby Chambliss Explain, Defend NSA Phone Records Program*, WASH. POST, June 6, 2013, <http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program> (defending the 215 metadata program, Senator Dianne Feinstein stated, “As far as I know, this is the exact three month renewal of what has been the case for the past seven years. This renewal is carried out by the FISA Court under the business records section of the Patriot Act. Therefore, it is lawful.”).

¹⁸ See Glen L. Roberts, *Who's On The Line? Cellular Phone Interception at its Best*, FULL DISCLOSURE, (1991), archived at <http://blockyourid.com/~gbpprorg/2600/harris.txt> (describing the marketing by the Harris Corporation of TriggerFish passive surveillance devices to law enforcement agencies at the National Technical Investigators Association conference in 1991).

¹⁹ See *infra* Part III.B.

assistance of a wireless carrier.²⁰ Whether installed in a vehicle, mounted on a drone, or carried by hand, this unregulated and technologically unmediated surveillance technology can, for example, send signals through the walls of homes to locate and identify nearby cell phones without the assistance of a wireless carrier and without providing any notice to the targets of the surveillance operation.²¹

This Article describes how the StingRay's unmediated collection capabilities do not fit well into the post-9/11 (or, for that matter, pre-9/11) Pen Register and Trap and Trace statute ("Pen/Trap"),²² the criminal surveillance authority normally used by federal law enforcement agencies to acquire certain types of non-content communications data in real-time. The lack of specific statutory authorization has not, however, served as a practical barrier to use of this technology by law enforcement agencies. Indeed, for several years prior to the passage of the PATRIOT Act, the official Department of Justice (DOJ) policy was that, since no specific statutory or Fourth Amendment prohibition forbade the practice, law enforcement could use StingRays without any form of judicial oversight.²³ After the PATRIOT Act broadened the definitional section of the Pen/Trap statute, DOJ interpreted the statute to authorize the collection of nearly all non-content information exchanged between a mobile device and a cell tower and, accordingly, advised prosecutors to obtain a Pen/Trap order when employing IMSI-catchers in an investigation.²⁴

The StingRay, therefore, illustrates how the legislature's authority can be effectively short-circuited when: (1) the government stretches existing statutory definitions to accommodate a new type of collection capability or surveillance technology not contemplated by Congress; and (2) there is no established mechanism to ensure legislative notice and review that would enable Congress affirmatively to choose whether or not to regulate the government's use of new or existing surveillance methods and technologies.

Drawing from the lessons of the StingRay, this Article argues that, if statutory authorities regulating law enforcement surveillance technologies

²⁰ See *infra* Part II. Some IMSI catchers also have the capacity to intercept content communications, though we are unaware of any public evidence regarding the extent to which law enforcement uses this capacity, if at all. See *infra* note 46.

²¹ *Id.*

²² 18 U.S.C. §§ 3121–3127 (2012).

²³ See *infra* Part III.B.

²⁴ See *id.* It is currently unclear from publicly available information, however, when and under what circumstances DOJ—due to potential Fourth Amendment issues or other policy considerations—may advise prosecutors to seek additional types of judicial authorization under existing statutes.

A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

and methods are to have any hope of keeping pace with technology, some formalized mechanism must be established through which complete, reliable and timely information about new and existing government surveillance methods and technologies shall be brought to the attention of Congress. That information, among other things, must include: (1) how the government interprets existing law to permit or, conversely, not to prohibit its use of a particular collection method; and (2) how it uses such technologies in criminal investigations.

Moreover, through a discussion of how the StingRay has evaded formal congressional oversight, this Article identifies several specific characteristics of any new or existing surveillance technologies or methods that should guide Congress in assessing the need for new regulation, as well as periodic assessment of any potential need to update existing statutory authorities to accommodate technological change and innovation. Finally, under the theory that Congress cannot begin to address the policy challenges posed by new surveillance technologies in the absence of adequate notice about their existence and actual or reasonably likely use by law enforcement, this Article proposes a way for Congress to create a mechanism to ensure that it receives such notice.

II. A BRIEF DESCRIPTION OF A STINGRAY AND ITS CAPABILITIES²⁵

Mobile phones communicate by radio signal with a wireless carrier's network of cellular base stations or "cell sites." These cell sites are generally located on cell towers that serve geographic areas of varying sizes.²⁶ The regular communication between phone and cell sites enables the carrier to route calls, text messages and Internet data to and from a subscriber's mobile phone. To facilitate this process, cellular phones periodically register themselves with the nearest cell site so that the network can connect incoming calls and text messages to the subscriber's phone.²⁷ This registration process, as well as the act of making a call or transmitting data, automatically generates location data of varying degrees of precision.²⁸ Government agencies can compel a provider to disclose

²⁵ For a more detailed technical description and analysis of the StingRay, see Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and its Impact on National Security and Consumer Privacy* (2014) (on file with the Journal).

²⁶ See Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 126 (2012).

²⁷ *Id.* at 126-27.

²⁸ *Id.* at 126-33.

location data, whether the data was automatically generated by the wireless carrier in the normal course of business or specifically created in response to a surveillance request to “ping” a phone.²⁹ Such “carrier-assisted surveillance” can reveal a phone’s historical, current, or prospective location (e.g., real-time tracking),³⁰ as well as other types of data, such as numbers called³¹ and the addresses of web pages viewed from a mobile device.³²

Carrier-assisted surveillance is not, however, the only means through which law enforcement can acquire such information. By impersonating a cellular network base station, a StingRay—a surveillance device that can be carried by hand, installed in a vehicle, or even mounted on a drone³³—tricks all nearby phones and other mobile devices into identifying themselves (by revealing their unique serial numbers) just as

²⁹ *Id.* at 131-32. See also Comments of CTIA—The Wireless Association on U.S. Department of Justice Petition for Expedited Rulemaking at 17, *In re* Petition for Expedited Rulemaking To Establish Technical Requirements and Standards Pursuant to Section 107(b) of the Communications Assistance for Law Enforcement Act, Docket No. RM-11376 (FCC July 25, 2007), <http://fjallfoss.fcc.gov/ecfs/comment/view?id=5514711157> (“Law enforcement routinely now requests carriers to continuously ‘ping’ wireless devices of suspects to locate them when a call is not being made . . . so law enforcement can triangulate the precise location of a device and [seek] the location of all associates communicating with a target.”); see also *Devega v. State*, 689 S.E.2d 293, 299 (Ga. 2010) (“[T]he investigators requested that Devega’s cell phone provider ‘ping’ his phone, which the officers described as sending a signal to the phone to locate it by its global positioning system (GPS). The company complied and informed the police that the phone was moving north on Cobb Parkway.”).

³⁰ See generally Pell & Soghoian, *supra* note 26, at 126-132.

³¹ See generally collections of files posted at http://www.markey.senate.gov/documents/2013-10-03_ATT_re_Carrier.pdf and http://www.markey.senate.gov/documents/2013-12-09_VZ_CarrierResponse.pdf (describing their disclosure of real-time ‘pen register’ and ‘trap and trace’ data to law enforcement agencies).

³² *Id.* See Christopher Soghoian, *8 Million Reasons for Real Surveillance Oversight*, SLIGHT PARANOIA, Dec. 1, 2009, <http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html> (quoting Paul Taylor, Electronic Surveillance Manager, Sprint Nextel, stating: “On the Sprint 3G network, we have IP data back 24 months, and we have, depending on the device, we can actually tell you what URL they went to.”) See also Verizon Wireless, Law Enforcement Resource Team (LERT), Apr. 20, 2009, <http://info.publicintelligence.net/VerizonLawEnforcementResourceTeam.pdf> (a presentation to law enforcement agencies by Verizon Wireless revealing that the company retains “IP destination information” for “30 days”).

³³ See Jennifer Valentino-DeVries, *Judge Questions Tools That Grab Cellphone Data on Innocent People*, WALL ST. J., Oct. 22, 2012, <http://blogs.wsj.com/digits/2012/10/22/judge-questions-tools-that-grab-cellphone-data-on-innocent-people> (“StingRay equipment can be carried by hand or mounted on vehicles or even drones.”).

A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

they would register with genuine base stations in the immediate vicinity.³⁴ As each phone in the area identifies itself, the StingRay can determine the location from which the signal came.³⁵ The StingRay and other similar devices also have the capacity, if so configured, to intercept data transmitted and received by the phone, including the content of calls, text messages, numbers dialed, and web pages visited.³⁶ This process is accomplished without any visual indication to the target that she is under surveillance or any mediating involvement on the part of the carrier whose network the StingRay is impersonating.³⁷ In circumstances where the government either cannot acquire, or chooses not to compel, assistance from a provider, the StingRay may be the surveillance technique of choice.³⁸ Moreover, unlike carrier-assisted surveillance, in which the third-party provider necessarily has knowledge of surveillance performed and copies of records disclosed at the request of law enforcement, the unmediated nature of the StingRay dictates that only the operator of the device has: (1) knowledge that an

³⁴ See Daehyun Strobel, IMSI Catcher, Seminar Work 17 (Ruhr-Universitat Bochum, 2007), http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf (“An IMSI Catcher masquerades as a Base Station and causes every mobile phone of the simulated network operator within a defined radius to log in. With the help of a special identity request, it is able to force the transmission of the IMSI.”).

³⁵ In fact, a different device made by the same company that manufactures the StingRay is used to locate devices. However, for clarity’s sake, we use the term StingRay in this article to refer to all of the devices in that family of products. See Harris Corp., Sole Source Vendor Letter 6 (2008), <http://egov.ci.miami.fl.us/Legistarweb/Attachments/48003.pdf> (describing the Harris AmberJack Direction Finding System).

³⁶ See Harris Corp, Price List 4 (2008), <https://info.publicintelligence.net/Harris-SurveillancePriceList.pdf> (listing an optional “GSM Intercept Software package” for the StingRay).

³⁷ See Executive Office for United States Attorneys, *Cell Site Simulators, Triggerfish, Cell Phones*, USA BOOK 18 (2008), https://www.aclu.org/pdfs/freespeech/cellfoia_release_074130_20080812.pdf (obtained through FOIA by the American Civil Liberties Union) (“A cell site simulator . . . is a mobile device that can electronically force a cell phone to register its telephone number (MIN), electronic serial number (ESN) and information about its location, when the phone is turned on. This can be done without the user knowing about it, and without involving the cell phone provider.”). USA Bulletins such as these are published by the Executive Office of United States Attorneys (EOUSA) and distributed to United States Attorney’s Offices across the country. They cover a range of topics and issues (like law enforcement surveillance methods) of interest to federal prosecutors, including new case law, law enforcement tools and practices, statutory authorities, and internal DOJ guidance. See also Strobel, *supra* note 34, at 21 (“In most cases, the [use of an IMSI catcher] cannot be recognized immediately by the subscriber.”).

³⁸ Intelligence agencies operating on foreign soil and thus presumably unable to compel the assistance of telephone companies could, for example, use a StingRay for communications interception.

interception ever took place;³⁹ and (2) or access to the information intercepted. Thus, to the extent that telephone companies are able to act as a proxy for their customers' privacy interests and may "push back" against overbroad or otherwise improper government surveillance,⁴⁰ no such advocate exists for the target when a Stingray is used. In short, the unmediated nature of StingRay technology makes it essentially "invisible" in operation and leaves behind no retrievable trace that is subject to future detection.⁴¹

Consider, for example, a situation where law enforcement agents can physically identify a target during the course of an investigation, but do not know the telephone she is currently using, perhaps because the target frequently cycles through disposable "burner" cell phones.⁴² Investigators can position a StingRay in the vicinity of the target to capture the unique serial number of the target's phone.⁴³ In this case, law enforcement collects the identifying data in real-time because the StingRay, masquerading as the

³⁹ In those circumstances where a court knowingly grants a Pen/Trap order authorizing law enforcement use of a StingRay in a criminal investigation, the judge would have knowledge that law enforcement intended to collect communications data but would not likely know when the surveillance occurred or the scope and amount of data collected. See *infra* Part III.B. for a discussion of federal magistrate opinions considering government applications to use cellular interception devices pursuant to the Pen/Trap statute.

⁴⁰ At a House Judiciary Committee hearing in 2011, Congressman Robert C. Scott asked Todd Hinnen, then the Acting Assistant Attorney General for National Security at the Department of Justice, "why would [a service provider] . . . have an incentive to hire lawyers to protect [their subscribers' privacy] rights?" Mr. Hinnen responded by stating his belief that "telecommunication providers and Internet service providers take the privacy of their customers and subscribers very seriously and I think are often an effective proxy for defending those rights." *Permanent Provisions of the PATRIOT Act: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 69 (2011) (statement of Acting Assistant Att'y Gen. for National Security, Todd M. Hinnen), http://judiciary.house.gov/hearings/printers/112th/112-15_65486.PDF.

⁴¹ *Cell Site Simulators, Triggerfish, Cell Phones*, *supra* note 37, at 18 ("This can be done without the user knowing about it").

⁴² See *The Wire: Amsterdam*, at 00:42:23 (HBO television broadcast Oct. 10, 2004) ("They make a couple of calls with a burner, throw it away. Go on to the next phone, do the same." "There's more of those things laying around the streets of West Baltimore than empty vials." "Well, how the fuck you supposed to get a wire up on that?" "Yeah, well, first it was payphone and pagers. Then it was cell phones and face-to-face meets. Now this. The motherfuckers do learn. Every time we come at them, they learn and adjust.").

⁴³ See Complaint at 8 n.1, United States v. Arguijo et al. (N.D. Ill. Feb. 13, 2012) (under seal), http://www.justice.gov/usao/iln/pr/chicago/2013/pr0222_01d.pdf ("Law enforcement officers . . . used a digital analyzer device on three occasions in three different locations where Chaparro was observed to determine the IMSI associated with any cellular telephone being carried by Chaparro.").

A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

cell site with the strongest signal,⁴⁴ receives the information immediately and directly as it is communicated by the mobile phones, leaving no trace of the interception with the third party provider.⁴⁵ Moreover, while law enforcement may only seek to identify or locate the target's mobile device, a StingRay will also, as a matter of course, collect data from many other mobile devices in the surrounding area.⁴⁶

III. IN BETWEEN OR BEYOND THE REACH OF STATUTORY LANGUAGE

Perhaps the most disconcerting aspect of the Section 215 metadata program to some surveillance scholars, beyond the sheer volume of information that was collected about hundreds of millions of Americans' domestic communications, is that a common sense reading of Section 215 does not support the government's interpretation that such broad, indiscriminate collection is permissible.⁴⁷ Indeed, one lawmaker who was an author of the PATRIOT Act has stated, "the government must request specific records relevant to its investigation . . . To argue otherwise renders the provision meaningless . . . It's like scooping up the entire ocean to guarantee you catch a fish."⁴⁸ The government's interpretation of intelligence authorities, where we have come to expect (if not accept) a lack of transparency with respect to the type and scope of collection allowed

⁴⁴ See MMI Research Ltd v. Cellxion Ltd. & Ors., [2009] EWHC (Pat) 418, [140] (Wales), <http://www.bailii.org/ew/cases/EWHC/Patents/2009/418.html> ("The [signal] strength of the simulated cell is maintained at a stronger value than the [signal] strength of the authentic network cells detected by the mobile to be tapped. When the mobile to be tapped begins to set up a call, the false cell, as the most powerful station, receives a request for a channel.").

⁴⁵ See Strobel, *supra* note 34, at 5 ("The IMSI Catcher is an expensive device to identify, track and tap a mobile phone user in such a way, that even the network operator cannot notice anything.").

⁴⁶ Although the focus of this essay is on certain legal and policy implications surrounding law enforcement collection of *metadata* via a StingRay, it is also worth noting that StingRay technology is capable of intercepting communications *content*. It remains unclear, however, which law enforcement agencies, if any, use such intercept capabilities during surveillance operations. See Harris GCSD Price List, *supra* note 36, at 4 (listing an optional "Sting[R]ay GSM intercept software package" for sale).

⁴⁷ See Brief of Amicus Curie, Professors of Information Privacy and Surveillance Law, *supra* note 11, at 9 ("The government acknowledges that the vast majority of data collected under the Verizon Order has not been relevant to any investigation, and its argument that the NSA can assess relevance on its own after the data are collected violates the plain language of § 215.").

⁴⁸ Jennifer Valentino-Devries and Siobhan Gorman, *Secret Court's Redefinition of 'Relevant' Empowered Vast NSA Data-Gathering*, WALL ST. J., July 8, 2013, http://online.wsj.com/article_email/SB10001424127887323873904578571893758853344-IMyQjAxMTAzMDAwNzEwNDcyWj.html (quoting Rep. Sensenbrenner).

under various statutes, is not, however, the only area where such opacity exists. The StingRay, a surveillance technology that is used not only by the intelligence community, but also by the military and law enforcement agencies,⁴⁹ raises some of the same transparency issues. Indeed, the StingRay's capacity for invasive surveillance (i.e. sending signals through walls and into homes⁵⁰ and overbroad collection of innocent third party information⁵¹) could well provoke the same kind of surprise and dismay with respect to the government's interpretation of the Pen/Trap statute as sufficiently authorizing its use. This Part will describe those issues after first discussing real-time cell phone tracking as an example of how surveillance methods can fall into interpretive gaps within and between statutes.

A. Real-time Cell Phone Tracking and Secrecy

In the context of criminal investigations, there are only two statutory authorities that explicitly authorize the interception of communications information in real-time: the Wiretap Act⁵² and the Pen/Trap statute.⁵³ Consequently, when the government wants to use a new surveillance

⁴⁹ See John Kelly, *Cellphone data spying: It's not just the NSA*, USA TODAY, Dec. 8, 2013, <http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/> ("Initially developed for military and spy agencies, the Sting[R]ays remain a guarded secret by law enforcement and the manufacturer, Harris Corp. of Melbourne, Fla.")

⁵⁰ These devices send signals like those emitted by a carrier's own base stations. See, e.g., Harris Corp. Product Sheet 1, http://servv89pn0aj.sn.sourcedns.com/~gbpprorg/2600/Harris_StingRay.pdf ("Active interrogation capability emulates base station."). Those signals, of course, "penetrate walls" (necessarily, to provide connectivity indoors). See *What You Need to Know About Your Network*, AT&T, <http://www.att.com/gen/press-room?pid=14003>; see also E.H. Walker, *Penetration of Radio Signals Into Buildings in the Cellular Radio Environment*, 62 THE BELL SYS. TECH. J. 2719 (1983), <http://www.alcatel-lucent.com/bstj/vol62-1983/articles/bstj62-9-2719.pdf>.

⁵¹ See *infra* Part II.

⁵² 18 U.S.C. §§ 2511–2520 (2012) (authorizing the interception of wire, oral or electronic communications—including communications content—by law enforcement to investigate crimes enumerated in the statute upon satisfying various elements set out in the statute).

⁵³ 18 U.S.C. §§ 3121–3127 (2012) (authorizing law enforcement to install and use a pen register device to "recor[d] or decod[e] . . . [non-content] dialing, routing, addressing, or signaling information . . . transmitted by an instrument or facility for which a wire or electronic communication is transmitted [or] provided" and to install and use a trap and trace device to "captur[e] the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication").

A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

method to collect data in real-time, it must first determine whether the technology or acquisition method fits under these existing statutory collection authorities. It must also conduct a Fourth Amendment analysis in order to determine if a search warrant must first be obtained. Cell phone location tracking represents one example of how the government analyzes and implements a real-time law enforcement collection method that has not been explicitly authorized by Congress.

It has already been described in the literature⁵⁴ and documented to a recent Congress⁵⁵ that nothing in the Electronic Communications Privacy Act (ECPA), which includes both the Wiretap Act and Pen/Trap statute,⁵⁶ articulates a legal standard Congress intended the government to meet before acquiring real-time cellular location data (i.e. tracking a mobile

⁵⁴ See Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L. J. 117, 134-35 (2012) (explaining how “[l]ocating the proper law enforcement access standard for prospective location data in the current law is, in some respects, like the quest for the Holy Grail, the search for the fountain of youth, or the hunt for a truly comfortable pair of high heels—one is unlikely to find them”); see also Kevin S. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance*, 41 U.S.F. L. REV. 589, 606-09 (2007) (analyzing how the Wiretap Act and Pen/Trap statute do not provide the requisite authority for such “tracking” and the Stored Communications Act (SCA) only authorizes retrospective access to previously stored communications content and non-content information).

⁵⁵ See ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. 82-83 (2010) [hereinafter *Location Hearing*], http://judiciary.house.gov/hearings/printers/111th/111-109_57082.pdf (written statement of Judge Stephen Wm. Smith, U.S. Magistrate Judge, describing the difficulty he and other magistrate judges experienced in determining the proper law enforcement access standard for real-time location information: “Moreover, none of the other categories of electronic surveillance seemed to fit. The pen register standard was ruled out by a proviso in a 1994 statute known as CALEA. The wiretap standard did not apply because CSI does not reveal the contents of a communication. The Stored Communications Act (SCA) standard did not seem to apply for two reasons: the definition of ‘electronic communication’ specifically excludes information from a tracking device; and the structure of the SCA was inherently retrospective, allowing access to documents and records already created, as opposed to prospective real time monitoring.”).

⁵⁶ Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.). This Article uses the term ECPA to describe the first three titles of the Electronic Communications Privacy Act: Title I (“Interception of Communications and Related Matters”), 100 Stat. at 1848, which amended the Wiretap Act (codified as amended at 18 U.S.C. §§ 2511–2520 (2012)); Title II (“Stored Wire and Electronic Communications and Transactional Records Access”), commonly referred to as the Stored Communications Act (SCA) (codified as amended at 18 U.S.C. §§ 2701–2712 (2012)); and Title III (“Pen Registers and Trap and Trace Devices”), commonly referred to as the Pen/Trap Devices statute, (codified as amended at 18 U.S.C. §§ 3121–3127 (2012)).

device in real-time) from a carrier. Indeed, the only hint from Congress suggesting a standard for law enforcement access to real-time location data is found in the Communications Assistance for Law Enforcement Act (CALEA), whose limited prescription instructs that “any information that may disclose the physical location of [a telephone service] subscriber” may not be acquired “solely pursuant to the authority for pen registers and trap and trace devices.”⁵⁷ So CALEA points only to the insufficiency of a Pen/Trap order to support a government request for real-time or “prospective” (as opposed to “historical”) location data. It provides, however, no specific affirmative guidance as to what level of process would provide sufficient support.

Left without explicit direction from Congress, DOJ created the controversial “hybrid-order” theory by stitching together the elements of a Pen/Trap order and an 18 U.S.C. § 2703(d) order for the disclosure of stored electronic communications found in ECPA’s Stored Communication’s Act (SCA).⁵⁸ Since at least 2005, criminal investigators have applied for both types of orders from judges when seeking to compel carriers to track a cellular phone in real-time.⁵⁹ Over time, however, some magistrate judges have accepted this hybrid theory and some have not. Those who have rejected the hybrid theory have required law enforcement agents to apply for a warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure.⁶⁰

The appropriate standard for law enforcement access to real-time location data is, however, still an open question for both Congress and the courts. In the interim, a patchwork of non-binding magistrate and district court decisions has emerged,⁶¹ with only one federal circuit court addressing the issue.⁶² For now, the state of the law can be described fairly as a chaotic, “inconsistent legal landscape” that provides no clarity for law enforcement, courts, criminal defense attorneys or those citizens and advocacy organizations interested the protection of privacy.⁶³

⁵⁷ 47 U.S.C. § 1002(a)(2) (2012).

⁵⁸ See Pell & Soghoian, *supra* note 26, at 135-36.

⁵⁹ *Id.*

⁶⁰ See *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 753–64 (S.D. Tex. 2005); *In re E.D.N.Y. Application*, 396 F. Supp. 2d 294, 322 (E.D.N.Y. 2005).

⁶¹ See Pell & Soghoian, *supra* note 26, at 137-41.

⁶² See *United States v. Skinner*, 690 F.3d 772 (2012) (explaining that the defendant did not have a reasonable expectation of privacy in the location that his cell phone was broadcasting, i.e., “the data given off by . . . his phone.”). *Id.* at 777.

⁶³ Pell & Soghoian, *supra* note 26, at 140.

A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

Scholars and some courts have criticized the hybrid theory on a number of grounds, ranging from its constitutionality⁶⁴ to whether, notwithstanding the constitutional question, Congress would have intended to permit the government's joining of historical and real-time surveillance statutes to authorize law enforcement access of real-time location data.⁶⁵ Absent better direction from Congress with respect to the appropriate standard for law enforcement access to real-time location data, the government would need, however, to arrive at some view of the appropriate process to follow when engaging in this form of surveillance. Considering that DOJ has used the hybrid theory to acquire real-time location data since at least 2005, that wireless carriers receive tens of thousands of court orders requiring the disclosure of location data per year,⁶⁶ and that, to date, there is still no real clarity in the law, it is fair to argue that judicial review has not adequately tested whether the government's hybrid theory: (1) fully complies with the Fourth Amendment;⁶⁷ (2) is consistent with congressional intent; or even (3) is consistent with the plain meaning of the relevant statutes.

Magistrate Judge Stephen Wm. Smith, an early critic of warrantless real-time tracking,⁶⁸ offers an important perspective on why appellate

⁶⁴ See Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 677, 717 (2011) (arguing that courts should require a warrant for access to location data in all cases because such acquisition is a search under the Fourth Amendment).

⁶⁵ *In re E.D.N.Y. Application*, 396 F. Supp. 2d 294, 322 (E.D.N.Y. 2005); see also *In re W.D.N.Y. Application*, 415 F. Supp. 2d 211, 219 (W.D.N.Y. 2005) (“[T]he challenge here is to the statutory justification for . . . [the government’s] application. . . . The Court does not agree with the government that it should impute to Congress the intent to ‘converge’ the provisions of the Pen Statute, the SCA, and CALEA to create a vehicle for disclosure of prospective cell information on a real time basis on less than probable cause.”).

⁶⁶ Letter from Sprint to Rep. Edward J. Markey, Co-Chairman, Congressional Bipartisan Privacy Caucus 10 (May 23, 2012), <http://web.archive.org/web/20121110192245/http://markey.house.gov/sites/markey.house.gov/files/documents/Sprint%20Response%20to%20Rep.%20Markey.pdf> (“Over the past five years, Sprint has received . . . 196,434 court orders for location information.”).

⁶⁷ One Circuit has held, however, that a defendant does not have a reasonable expectation of privacy in the real-time location broadcasted by his cell phone, at least with respect to his movements along public thoroughfares. In this case, the government obtained court orders (but apparently not a warrant) to “ping” the defendant’s phone. *Skinner*, 690 F.3d at 776-781.

⁶⁸ See *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority (In re 2005 S.D. Tex. Application)*, 396 F. Supp. 2d 747, 753–64 (S.D. Tex. 2005) (rejecting the government’s “hybrid theory” and finding that compelled disclosure of prospective cell site data is more akin to the tracking device placed under a vehicle, as defined in 18 U.S.C. § 3117 (defining a tracking device as “an electronic or mechanical

review of real-time location tracking and other types of government surveillance subject to ECPA is a rare occurrence: for the most part, the government is the *only* party with the ability and potential incentive to appeal unfavorable judgments.⁶⁹ ECPA surveillance orders are issued *ex parte* and often remain sealed long past an investigation's end.⁷⁰ A target of a sealed ECPA order is thus unlikely to become aware of the government's acquisition of her information unless an investigation proceeds to charges. It is at that point, as a criminal defendant, that a target can challenge the ECPA order. If an investigation never proceeds to an indictment, the innocent target will never learn that a third party disclosed her information to the government.⁷¹ Moreover, while the third party provider receives the order compelling disclosure of information, such disclosure order is often accompanied by a gag order.⁷² The third party provider could challenge the gag order, as well as the primary disclosure order, but instances where companies have "pushed back" against law enforcement ECPA orders in criminal investigations have not, to date, resulted in a steady stream of appellate court review.⁷³ In sum, as Judge Smith observes, "[t]hrough a potent mix of indefinite sealing, nondisclosure (i.e. gagging), and delayed-notice provisions, ECPA surveillance orders all but vanish into a legal void."⁷⁴

The issues identified by Judge Smith lend discomfiting credence to Justice Alito's recent observation that, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."⁷⁵ But for the legislature to act, it must, at a minimum, have accurate information about how government agencies interpret their existing surveillance authorities, as well as the nature of new, unregulated surveillance technologies now in use. Judge Smith notes that, although the location tracking of cell phones first came to Congress' attention in 1994, nearly two decades have passed without any amendment to ECPA

device which permits the tracking of the movement of a person or object.")); *see also* 18 U.S.C. § 3117(b) (2012).

⁶⁹ Stephen Wm. Smith, *Gagged, Sealed and Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 323-29 (2012).

⁷⁰ *Id.* at 315.

⁷¹ See Memorandum and Order, No. 10-291-M-01 (D.D.C. Nov. 1, 2010), <https://www.dcd.uscourts.gov/dcd/sites/dcd/files/mag10-291.pdf> (holding that the notice requirements in Rule 41 are satisfied by notifying the email provider, rather than the target of the surveillance order).

⁷² Smith, *supra* note 69, at 323.

⁷³ *Id.* at 328.

⁷⁴ *Id.* at 314.

⁷⁵ United States v. Jones, 132 S. Ct. 945, 964 (2012).

A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

clarifying the appropriate law enforcement access standard.⁷⁶ While there is rarely one reason for why Congress is or is not able to pass legislation on a particular issue, one important factor affecting Congress' ability to legislate in the area of law enforcement access to location data is that Congress has not had current, accurate data on the nature and extent of cell phone surveillance for many years.⁷⁷ As we will discuss below, the StingRay presents even greater challenges to transparency and congressional awareness of government surveillance.

B. The StingRay and Secrecy

Much less is known about law enforcement use of StingRays in criminal investigations than is known about more traditional cell phone location tracking. What little is known comes mostly from a limited number of magistrate judge opinions, a tenacious criminal defendant seeking discovery in his own prosecution,⁷⁸ and a few obscure DOJ guidance documents.⁷⁹ This section discusses DOJ's interpretation of the Pen/Trap statute as authorizing law enforcement use of StingRays. It argues that, given the StingRay's powerful, unmediated and largely indiscriminate surveillance capabilities, a common sense reading of the text does not

⁷⁶ Smith, *supra* note 69, at 316.

⁷⁷ *Id.* Indeed, public information about the scale of location requests by law enforcement was not available to Congress until 2012 when then Representative (now Senator) Ed Markey received data from wireless carriers. *See, e.g.*, Pell & Soghoian, *supra* note 26, at 158-59 (noting that during the time Congress was considering reforms to ECPA in 2010—in contrast to information about Wiretap and Pen/Trap surveillance—Congress did not “even have a sense of the number and scope of law enforcement requests for location information”). Of the carriers that provided data to then Rep. Markey, only Sprint provided specific numbers about law enforcement requests for location data. *See* Letter from Sprint to Rep. Edward J. Markey, *supra* note 66 (“[O]ver the past five years, Sprint has received . . . 196,434 court orders for location information.”). Additional carrier responses are available at *Markey Letters to Wireless Carriers on Law Enforcement Requests*, WEBPAGE OF SEN. EDWARD MARKEY, http://www.markey.senate.gov/Markey_Letters_to_Wireless_Carriers.cfm (last visited Dec. 16, 2013).

⁷⁸ *See United States v. Rigmaiden*, 2013 WL 1932800 (D. Ariz. May 8, 2013). The government prosecuted Rigmaiden for his role in a scheme in which he allegedly obtained fraudulent tax refunds for hundreds of deceased persons and third parties. Law enforcement agents used a StingRay device to identify Rigmaiden as the alleged perpetrator of these crimes. In the course of pre-trial discovery and motion practice, Rigmaiden, a pro-se defendant, filed substantial discovery requests and motions to suppress evidence, some of which related to the government's use of a StingRay. *See Order, United States v. Rigmaiden*, Case 2:08-cr-00814-DGC, (No. 1009) (Mar. 08, 2013) (on file with the Journal).

⁷⁹ *See supra* Part II.

provide adequate notice to legislators that the Pen/Trap statute purportedly authorizes law enforcement use of a StingRay in criminal investigations. Such lack of notice, when compounded with the propensity for ECPA orders to vanish into a legal void⁸⁰ without revealing how DOJ and magistrate judges are interpreting surveillance authorities, severely restricts (even undermines) the ability of Congress to conduct meaningful oversight of government surveillance and to regulate new surveillance technologies and methods.

The crux of our argument is not that it is impossible to read the plain text of the Pen/Trap statute as being applicable to the StingRay but that, as collection capabilities expand in power and scope (as we have seen occur with the NSA's domestic telephony data collection program), government lawyers may interpret the text of statutes to authorize greater surveillance powers than a plain reading of the text would disclose or suggest. Moreover, through examining two magistrate court opinions discussing StingRay technology, we will illustrate the limited ability magistrate judges have to restrain government power when there is no statute directly authorizing or limiting a surveillance method or technology. First, however, we will discuss the parameters of the Pen/Trap statute itself.

The Pen/Trap statute authorizes law enforcement agencies, upon obtaining a Pen/Trap order from a court, to compel providers to disclose, in real-time, various types of transactional information pertaining to wire or electronic communications.⁸¹ The statute references a "telephone line or other facility to which the pen register or trap and trace is to be attached or applied,"⁸² and the standard for such issuance is extraordinarily low.⁸³ Indeed, the government need only certify that the information "likely to be obtained is relevant to an ongoing criminal investigation."⁸⁴

Assuming that the magistrate judge finds that the Pen/Trap statute authorizes the kind of collection that the government seeks, then, upon such

⁸⁰ See Smith, *supra* note 69, at 314.

⁸¹ See 18 U.S.C. §§ 3121-3124 (2012) (defining the relevant transactional information as "dialing, routing, addressing, and signaling information used in the processing and transmitting of wire or electronic communications" (Section 3121); describing the Pen/Trap application process (Section 3122); explaining the circumstances and standards governing a court's issuance of a Pen/Trap order (Section 3123); and mandating requirements for third party assistance for installation of a Pen/Trap order (Section 3124)).

⁸² 18 U.S.C. § 3123(b)(1)(A) (2012).

⁸³ Location Hearing, Written Statement of Judge Smith, *supra* note 55, at 92 Exhibit A (illustrating the Pen/Trap standard as the lowest of standards found in the surveillance statutes requiring court approval).

⁸⁴ 18 U.S.C. §§ 3122(b)(2), 3123(a)(1) (2012).

A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

certification, the court must grant the application.⁸⁵ It is for this reason that at least one circuit court has characterized the role of magistrate judges in such instances as being “ministerial in nature.”⁸⁶ In other words, when granting the Pen/Trap order, the magistrate does not examine or analyze whether there are sufficient facts to support the government’s certification that the information sought is relevant to an ongoing criminal investigation.

The Pen/Trap statute arguably authorizes the government to compel production of a broad array of both telephony and Internet data.⁸⁷ While DOJ’s public manual on “Searching and Seizing Computers” does not give a detailed list of all of the specific types of transactional information that can be obtained with a Pen/Trap Order, it notes that the statute’s reference to “‘dialing, routing, addressing [and/or] signaling information’ encompasses almost *all* non-content information in a communication.”⁸⁸

Given the broad array of real-time data that the Pen/Trap statute appears to authorize the government to compel from a third party provider, does a plain reading of the statute suggest that it also authorizes law enforcement to use a sophisticated technological device to impersonate a cell site operated by the target’s cellular provider and collect such

⁸⁵ See 18 U.S.C. § 3123(a) (“Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.” (emphasis added)).

⁸⁶ United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995) (“The judicial role in approving use of trap and trace devices is ministerial in nature.”).

⁸⁷ The statute defines the non-content data that the government can acquire with a Pen/Trap order as “dialing, routing, addressing, and signaling information used in the processing and transmitting of wire or electronic communications.” 18 U.S.C. § 3121(c).

⁸⁸ Computer Crime and Intellectual Prop. Section, Criminal Div., *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, U.S. DEP’T OF JUSTICE, at 154 (3rd ed. 2009) [hereinafter DOJ Manual] (emphasis added).

<http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf>. With respect to telephony metadata, the Electronic Frontier Foundation (EFF) has interpreted the scope of the DOJ’s statement to include: the numbers a phone calls and receives; the starting and ending of each call; the duration of each call; whether each call was connected or went to voicemail; and (although a disputed, controversial use of Pen/Trap) “post-cut-through dialed digits” (digits after a call is connected, like a banking PIN number or a prescription refill number). With respect to Internet metadata, EFF speculates that the Pen/Trap statute may authorize real-time collection of addresses of sent and received email; the time each email is sent or received; the size of each email that is sent or received; IP (Internet Protocol) addresses to include IP addresses of other computers a target computer exchanges information with, as well as the communications ports and protocols used (which, in turn, can be used to determine the types of communications sent and the types of applications used). See “*Pen Registers*” and “*Trap and Trace Devices*,” EFF SURVEILLANCE SELF-DEFENSE BLOG, <https://ssd.eff.org/wire/pen-registers>.

information, without the assistance of a third party? Moreover, does a plain reading of the statute suggest that law enforcement is authorized to use a device that may, in the process of collecting data about a target's device, also collect data about a significant number of innocent third parties, depending on how the device is used?⁸⁹ In posing these questions, we are moving beyond a mere inquiry as to whether the statute conceivably authorizes this type of surveillance to ask whether legislators are on notice that the statute can be, and is being, interpreted to authorize surveillance that potentially impacts so many innocent people.

1. *The 1995 Digital Analyzer Magistrate Opinion*

The first published opinion (and one of only a few that are public) that helps to address some of these questions came in 1995, when Magistrate Judge Edwards took the position that no authority, including the Fourth Amendment, either authorizes or limits the government's use of a far more rudimentary predecessor of the StingRay⁹⁰—a device commonly referred to as a “digital analyzer” or “TriggerFish.”⁹¹

In this case, the government applied for a Pen/Trap order to employ a digital analyzer to intercept the signals from cellular phones used by five named subjects in a criminal investigation.⁹² Magistrate Judge Edwards found, however, that because the digital analyzer was not intended to be, nor could it be, physically attached to the cellular phone, the Pen/Trap statute was not applicable to its use.⁹³ Judge Edwards also found, pursuant

⁸⁹ See John Kelly, *Cellphone data spying: It's not just the NSA*, USA TODAY, Dec. 8, 2013, <http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/> (“Typically used to hunt a single phone's location, the system intercepts data from all phones within a mile, or farther, depending on terrain and antennas.”)

⁹⁰ Whereas the StingRay actively interacts with cellular phones and sends signals into the homes of the target and anyone else in the vicinity, the Triggerfish passively intercepts and decodes the signals sent between cellular base stations and phones. *See generally* Pell & Soghoian, *supra* note 25.

⁹¹ *In re Application of the United States of America for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer*, 885 F. Supp. 197 (C.D. Cal. 1995). The government submitted an *ex parte* application for an order permitting agents of the Orange County Regional Narcotics Suppression Program (“RNSP”) to use a digital analyzer. *Id.* at 198-99.

⁹² The agents likely needed to use this technology because they did not know the particular phone numbers of the devices that the targets were using, *id.* at 199, and thus could not seek more specific surveillance assistance from their wireless carriers.

⁹³ The court further explained its reasoning:

The statutory definition of a ‘trap and trace device’ does not include the limitation in the definition of a pen register described above, limiting the devices to those that are attached to a telephone line. *See* 18 U.S.C.

A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

to *Smith v. Maryland*,⁹⁴ that the government's use of a digital analyzer raised no Fourth Amendment concerns.⁹⁵ This ruling was consistent with DOJ's position, first publically documented in 1997, that neither the Fourth Amendment nor any statutory authority prohibited its use of the digital analyzer, as long as the acquisition of non-content data did not involve the assistance of carriers.⁹⁶ While not a legal requirement, DOJ still advised prosecutors to seek a Pen/Trap order when using a digital analyzer as a Pen/Trap device. Thus, in 1995, it appears DOJ sought court authorization via the Pen/Trap statute merely "out of an abundance of caution."⁹⁷

§ 3127(4). Nonetheless, it appears from the construction of related sections of the statutes governing trap and trace devices that they include only devices that are attached to a telephone line. Specifically, 18 U.S.C. § 3123(b) requires that an order for use of both pen registers and trap and trace devices include 'the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached. . . .' This limitation on the proscription against pen registers and trap and trace devices to prohibit only devices that are 'attached' to a telephone line cannot be assumed to be inadvertent. In other statutes relating to interceptions of telephone communications, Congress encompassed, generally, any types of interceptions of wire, oral, or electronic communications—regardless of whether the intercepting device was 'attached' to a telephone line. *See, e.g.*, 18 U.S.C. § 2511. That Congress did not impose equally comprehensive restrictions on lesser interceptions that do not raise 4th Amendment issues, such as those made with pen registers and trap and trace devices, is neither surprising nor inconsistent. In any event, it must be remembered that the prohibition against the use of pen registers and trap and trace devices without court order is found in a criminal statute. *See* 18 U.S.C. § 3121(d). Under well-settled principles, the statute should be strictly construed, and any ambiguity in its scope must be construed narrowly.

Id. at 200.

⁹⁴ 442 U.S. 735 (1979).

⁹⁵ *In re Application of the United States of America for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer*, 885 F. Supp. at 199. The court noted that "[n]umbers dialed by a telephone are not the subject of a reasonable expectation of privacy . . . [and] no logical distinction is seen between telephone numbers called and a party's own telephone number (or [device serial] number), all of which are regularly voluntarily exposed and known to others." *Id.*

⁹⁶ *See* Executive Office for United States Attorneys, *Electronic Investigative Techniques*, USA BULLETIN, Sept. 1997, at 13-15, http://www.justice.gov/usao/eousa/foia_reading_room/usab4505.pdf ("it does not appear that there are constitutional or statutory constraints on the warrantless use of such a [digital analyzer] device.").

⁹⁷ *In re Application of the United States of America for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer*, 885 F. Supp. at 200.

Although ultimately ruling that the Pen/Trap statute did not regulate—and thus did not prohibit—government use of a digital analyzer, the judge expressed serious reservations about its capabilities and use. Specifically, the judge expressed concern about the potential intrusion upon the privacy of innocent third parties. That is, if the court authorized the government to use a digital analyzer to identify the particular phones used by known targets, such an order would essentially permit agents to sweep the relevant surrounding areas and intercept signals emitted from *all* phones in those areas. Indeed, Judge Edwards recognized that “depending upon the effective range of the digital analyzer, telephone numbers and calls made by others than the subjects of the investigation could be inadvertently intercepted.”⁹⁸ Moreover, although the agents were not seeking to intercept communications content, the digital analyzer was capable of being used for that purpose.⁹⁹

The court also noted that its authorization could permit the government to collect data about large numbers of phones without any recordkeeping or reporting requirements, thus preventing effective congressional oversight of the surveillance tool.¹⁰⁰ The court contrasted this lack of record production with the statutory reporting requirements to Congress in the Pen/Trap statute, such as “the use of court orders that identified particular telephones and the investigative agency” and “periodic reports to Congress stating the numbers of such orders.”¹⁰¹ Noting these differences and others,¹⁰² the court stated that the government’s application “would not insure sufficient accountability.”¹⁰³

The court’s reasoning appears to illustrate broader concerns about a circumvention of congressional authority that would occur if the court

⁹⁸ *Id.* at 201.

⁹⁹ See *Electronic Investigative Techniques*, *supra* note 96, at 14 (“Although [a digital analyzer] device is also capable of intercepting both the numbers dialed from the cellular phones and the voice (wire) communications to and from cellular telephones, the digital analyzer is programmed so it will not intercept cellular conversations or dialed numbers when it is used for the limited purpose of seizing ESNs and/or the cellular telephone’s number.”); see also Electronic Surveillance Unit, *Electronic Surveillance Manual: Procedures and Case Law Forms*, U.S. DEPT OF JUSTICE 40 (2005), <http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf> (“Digital analyzers/cell site simulators/triggerfish and similar devices may be capable of intercepting the contents of communications and, therefore, such devices must be configured to disable the interception function, unless interceptions have been authorized by a Title III order.”).

¹⁰⁰ *In re Application of the United States of America for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer*, 885 F.Supp. at 201-02.

¹⁰¹ *Id.* (citing 18 U.S.C. §§ 3123(b), 3126).

¹⁰² *Id.*

¹⁰³ *Id.* at 201.

A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

granted the government's request, even "in an abundance of caution." By granting an order pursuant to a statute whose definitional elements did not conform to the surveillance technique at issue, the court risked giving: (1) a potentially incorrect interpretation of a statute; or worse (2) judicial approval of a surveillance technique that Congress appeared neither explicitly to authorize or prohibit under the statutory authority presented in the government's application—all without the corresponding accountability mechanisms that Congress mandated in the statute cited in the government's application.

Though it expressed concern about the surveillance capabilities of this technology, the court could not restrain its use by law enforcement. Ironically, the court's denial of the government's application likely reinforced DOJ's stance that it did not need any court authorization for future use of a digital analyzer.¹⁰⁴ At least in this instance, however, it was clear to the court exactly *what* it was being asked to authorize. A more recent opinion suggests that courts are being asked to grant applications for the use of StingRays in criminal investigations without appropriate knowledge about what the technology actually does—information that is necessary to determine both whether the Pen/Trap statute authorizes its use and whether the use of a StingRay constitutes a search under the Fourth Amendment.

2. 2012 *StingRay Magistrate Opinion*

By 2005, if not earlier, DOJ had adopted the position that the Pen/Trap statute, as amended by the 2001 PATRIOT Act, "appears to encompass all of the non-content information passed between a cell-phone and the provider's tower."¹⁰⁵ Accordingly, DOJ advised prosecutors to seek a Pen/Trap order for all non-content data that agents acquired directly.¹⁰⁶ This was a significant change to DOJ's earlier 1997 guidance, which had interpreted the law to permit unmediated surveillance (e.g. performed directly via cellular surveillance technology rather than with the assistance of carriers) without the necessity of a Pen/Trap or other court order.

In 2012, a federal magistrate judge from Texas issued an order denying an application submitted by agents from the Drug Enforcement Agency for the use of a StingRay.¹⁰⁷ The case involved a surveillance target

¹⁰⁴ See *Electronic Investigative Techniques*, *supra* note 96, at 14.

¹⁰⁵ See 2005 *Electronic Surveillance Manual*, *supra* note 99, at 45.

¹⁰⁶ *Id.* at 47-48.

¹⁰⁷ *In re Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device*, 890 F. Supp. 2d 747, 748 (S.D. Tex. 2012).

that switched from using a phone known to agents to an unknown phone.¹⁰⁸ The government therefore sought a Pen/Trap order “to detect radio signals emitted from wireless cellular telephones in the vicinity of the [Subject] that identify the telephones.”¹⁰⁹ The agents submitted their application pursuant to the Pen/Trap statute¹¹⁰ and 18 U.S.C. § 2703(c)(1), a provision of ECPA’s Stored Communications Act,¹¹¹ and the government informed Magistrate Judge Owsley that it was “based on a standard application model and proposed order approved by [DOJ].”¹¹²

Since the subject was known to law enforcement (whereas the phone number the target was using was unknown), agents planned to identify the phone by capturing device identification data “at various locations in which the [subject’s] telephone [would] reasonably [be] believed to be operating.”¹¹³ After reviewing the application, the judge conducted an *ex parte* hearing where an agent leading the investigation indicated that the “equipment designed to capture the cell phone numbers was known as a ‘[S]ting[R]ay.’”¹¹⁴

Ultimately, the court denied the government’s application.¹¹⁵ Judge Owsley expressed concern that the application did not adequately explain the technology or “how many distinct surveillance sites they intend[ed] to use, or how long they intend[ed] to operate the [S]ting[R]ay equipment to gather all telephone numbers in the immediate area.”¹¹⁶ Moreover, the court noted that no explanation was given, either in writing or verbally, as to what would be done with the “innocent . . . information” collected from the phones of uninvolved individuals who just happened to be in the vicinity of

¹⁰⁸ *Id.*

¹⁰⁹ *Id.*

¹¹⁰ 18 U.S.C. §§ 3122(a)(1), 3127(5) (2012).

¹¹¹ It is not clear from the 2012 magistrate opinion what purpose this citation to ECPA’s Stored Communications Act served in terms of providing additional authority of unmediated, direct collection of non-content data in this investigation. The 2005 Guidance indicated that only a Pen/Trap order was required for use of devices to collect non-content data directly. See *2005 Electronic Surveillance Manual*, *supra* note 99, at 47-48. DOJ may, however, have provided updated guidance reflecting a different or more nuanced legal position. As of the writing of this Article this new guidance, if it exists, is not publically available. The citation to the Stored Communications Act does have a strange similarity to the prospective location data “hybrid order.” See discussion *supra* Part III.A.

¹¹² *In re Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device*, 890 F. Supp. 2d 747, 749 (S.D. Tex. 2012).

¹¹³ *Id.* at 748.

¹¹⁴ *Id.*

¹¹⁵ *Id.* at 752.

¹¹⁶ *Id.* at 749.

A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

the surveillance target.¹¹⁷ Finally, the court expressed concern that neither the prosecutor nor the DEA agent appeared to understand the technology at issue and “seemed to have some discomfort in trying to explain it.”¹¹⁸

At a 2013 symposium at Yale Law School, Judge Owsley suggested that:

The practice of the feds’ not making clear the planned use of a StingRay when seeking surveillance authorization could be widespread. . . . I may have seen them before and not realized what it was, because what they do is present an application that looks essentially like a pen register application So any magistrate judge that is typically looking at a lot of pen register applications and not paying a lot of attention to the details may be signing an application that is authorizing a Sting[R]ay.¹¹⁹

Indeed, a StingRay or similar tracking device appeared to be used in a case that made its way to the Seventh Circuit.¹²⁰ Because the circuit court opinion and underlying district court opinion¹²¹ never refer to such a device, whether by a specific or generic name or other identifying description, the only real indication that the Pen/Trap order authorized law enforcement use of a StingRay-type device was through DOJ’s disclosure of a copy of the opinion in response to a Freedom of Information Act (FOIA) request

¹¹⁷ *Id.*

¹¹⁸ *Id.*

¹¹⁹ Ryan Gallagher, *Feds Accused of Hiding Information From Judges About Covert Cellphone Tracking Tool*, SLATE, Mar. 28, 2013, http://www.slate.com/blogs/future_tense/2013/03/28/StingRay_surveillance_technology_used_without_proper_approval_report.html; see also Jennifer Valentino-Devries, Jennifer Valentino-Devries, ‘Stingray’ Phone Tracker Fuels Constitutional Clash, WALL ST. J., Sept. 22, 2011, <http://online.wsj.com/article/SB1000142405311904194604576583112723197574.html> (reporting that when a prosecutor was asked by the judge how a court order or warrant could be obtained without telling the judge what technology was being used, the prosecutor responded “it was standard practice, your honor”).

¹²⁰ United States v. Amaral-Estrada, 509 F.3d 820, 822 (7th Cir. 2007) (explaining that “the DEA sought and received a court order from a magistrate judge for the application and use of a pen register and trap-and-trace device, and to determine certain telephone information using the cellular telephone number on Sosa-Verdeja’s phone.”).

¹²¹ United States v. Bermudez, et al., 2006 WL 3197181, at *1 (S.D. Ind. June 30, 2006) (explaining that “by using an electronic device and the cellular site information obtained based on a court order signed by Magistrate Judge Foster, [a law enforcement officer] was able to pinpoint the multi-unit residence located at 5352 West Deming Place as the precise location of a particular cell phone”).

regarding StingRay devices filed by one of this Article's authors.¹²² Moreover, additional documents obtained from an ACLU FOIA request indicate that Pen/Trap applications presented to magistrate judges in the Northern District of California did not make law enforcement's intended use of StingRays "explicit."¹²³

Notwithstanding his broader concerns, Judge Owsley's decision to deny the application appears to stem from a definitional problem he identified in the Pen/Trap statute that, ultimately, the government did not adequately address. While recognizing that the PATRIOT Act broadened the Pen/Trap definitions, "amplify[ing] the various types of information that are available such as routing and signaling information,"¹²⁴ Judge Owsley read language contained in Section 3123(b)(1) of the statute as "straightforward in that a telephone number or similar identifier is *necessary* for a pen register."¹²⁵ Accordingly, he found that the language in the statute "mandate[s] that this Court have a telephone number or some similar identifier before issuing an order authorizing a pen register."¹²⁶ Because the government did not provide any support to the contrary suggesting that the statute authorized collection of non-content data from *unidentified* devices, Judge Owsley denied the application without prejudice.¹²⁷

IV. WARNINGS FOR LEGISLATORS

Together, these two magistrate opinions (one pre- and the other post-PATRIOT Act) raise questions as to whether the Pen/Trap statute can properly be interpreted as authorizing the use of a StingRay or similar

¹²² Letter from Kenneth Courter, Acting Chief, FOIA/PA Unit, Criminal Division, U.S. Dep't of Justice, to Christopher Soghoian (Sept. 30, 2013).

<http://files.cloudprivacy.net/stingray-FOIA-7th-Circuit-doc.pdf>.

¹²³ See email from Miranda Kane to USACAN-Attorneys-Criminal, U.S. Dep't of Justice (May 23, 2011, 11:55 AM),

https://www.aclu.org/files/assets/doj_emails_on_stingray_requests.pdf (indicating that magistrate judges in the Northern District of California raised collective concerns about whether a pen register is sufficient to authorize use of StingRay and TriggerFish technology that simulates a cell tower and can be placed inside a van to help pinpoint an individual's location with and that the Pen/Trap applications presented to magistrates were not making law enforcement's intended use of the technology "explicit").

¹²⁴ *In re Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device*, 890 F. Supp. 2d 747, 751 (S.D. Tex. 2012).

¹²⁵ *Id.* (emphasis added).

¹²⁶ *Id.*

¹²⁷ *Id.* at 751-52.

A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

unmediated surveillance technology to acquire non-content communications data. Beyond parsing the statutory language, however, these opinions illustrate how the government seeks to accommodate the use of new and powerful surveillance technologies through aggressive interpretation of existing statutory language that neither directly authorizes nor prohibits their use.

More critically, for legislators looking at how they can create or improve a process for regulating and overseeing law enforcement use of new surveillance technologies and collection methods, the 1995 digital analyzer opinion illustrates the limited ability a magistrate judge has to constrain government surveillance that is neither authorized nor prohibited directly by statutory language. The court's sense of futility is manifest in the conundrum of whether it is appropriate to authorize government use of a new technology merely "in an abundance of caution." By denying the government's Pen/Trap application essentially on the grounds that it was unnecessary, Judge Edwards likely reinforced DOJ's view that no form of judicial oversight was necessary for law enforcement use of the surveillance technology. While this may have been the appropriate legal answer, it raises significant oversight concerns.

As previously indicated, when a digital analyzer or StingRay collects data, no corresponding third party records are created—the information intercepted is in the sole possession of the agents using the StingRay.¹²⁸ If there is no judicial oversight, then there is no trace or record of StingRay surveillance in a particular case other than law enforcement's own elective record keeping systems. While it is not impossible for the information to surface as part of the discovery process of a criminal prosecution,¹²⁹ such disclosures would depend on how discovery rules were applied in particular cases. In other words, records production in the context of the criminal discovery process is not a solid, reliable avenue for legislators to learn, in a timely fashion, about law enforcement use of new surveillance technologies and government legal interpretations supporting their use.

Conversely, the 1995 digital analyzer opinion also illustrates how congressional authority and oversight can be short circuited if a court, "in an abundance of caution," grants an application for use of a new invasive surveillance technology when that method is not directly authorized by statute and is not apparent to a legislator through a common sense reading of the statutory text. In this instance, a court risks giving judicial imprimatur to a new surveillance technology in the context of a system in which, as

¹²⁸ See *supra* Part II.

¹²⁹ See *United States v. Rigmaiden*, 2013 WL 1932800 (D. Ariz. May 8, 2013).

Judge Smith has explained, appellate review of ECPA *ex parte* surveillance orders is rare.¹³⁰ The appellate process is thus unlikely to expose law enforcement use of the technology or government interpretations of the statutes purportedly authorizing such use within anything approaching a timely notice period that would facilitate either congressional oversight or legislative action.¹³¹ Moreover, as Judge Owsley has noted, it is possible that magistrate judges have authorized law enforcement use of StingRays in various cases without even knowing or understanding what they were authorizing. If true, this practice adds an additional layer of complication to congressional notice and oversight, since only elements of the Executive branch may know about law enforcement use of new surveillance technologies in criminal investigations.

V. SUGGESTIONS FOR REFORM

After many months of almost weekly disclosures about classified NSA intelligence programs, we have begun to understand how, at times, government agencies will interpret statutory language to authorize bulk, indiscriminate collection in a way that is not apparent from a plain reading of the statutory text. While some members of Congress were aware of this type of collection in the context of the Section 215 metadata program, we have argued that the StingRay has significantly expanded the government's surveillance capabilities in criminal investigations while it has, nevertheless, gone largely unnoticed and unregulated. Indeed, a plain reading of the Pen/Trap statute would not put a legislator on sufficient notice that the government was interpreting the statute to authorize StingRay surveillance.¹³² While we are not suggesting that no congressional

¹³⁰ See *supra* Part III.A.

¹³¹ See discussion, *supra*, Part III.A.

¹³² DOJ's conclusion that Pen/Trap now encompasses all non-content data between a cell phone and a cell tower relies, in part, on its analysis of the relevant but "scant" legislative history which suggested that the new definitions were intended to apply to "all communications media, instead of focusing on traditional telephone calls." *2005 Electronic Surveillance Manual*, *supra* note 99, at 46. Examining, for example, House language referencing "a packet requesting a telnet session—a piece of information passing between machines in order to establish a communication session for the human user," DOJ suggests that the term "provides a close analogy to the information passing between a cell phone and the nearest tower in the initial stages of a cell phone call." *Id.* at 46-47. Moreover, in contrast to earlier Pen/Trap definitions that referenced the attachment of a Pen/Trap device to a phone line, the House Report recognized that Pen/Trap devices could "collect information remotely." *Id.* at 47. We find it difficult to conclude from DOJ's analysis of this "scant" legislative history that Congress had specific and sufficient notice regarding

A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

staffer or Member of Congress is aware of the StingRay family of technologies and their capabilities, there is no public evidence that Congress has formally evaluated the privacy implications of law enforcement use of such unmediated, indiscriminate surveillance methods.¹³³ Moreover, given the scant number of published cases illustrating a court's analysis and interpretation of statutes that may authorize law enforcement use of the StingRay family of technologies, it would be unrealistic to expect judicial review to facilitate meaningful notice to Congress in anything approaching a timely fashion.¹³⁴ The StingRay, therefore, illustrates a larger gap in congressional oversight insofar as new, invasive surveillance technologies and collection methods not directly authorized by Congress can be used, often for decades, without any reliable notice to Congress about their use. Simply put, before Congress can begin to regulate new surveillance technologies and methods, it must have some notice of their nature and actual or likely use. An authoritative, reliable mechanism is needed to produce information that can provide such notice.

As part of the Administration's response to the summer 2013 Snowden disclosures, which began with the revelation of the 215 metadata program, President Obama announced his intention to convene an outside group of experts to conduct a full review of NSA surveillance programs and issue a report about how these programs impact security, privacy and foreign policy.¹³⁵ This expert panel has since issued its report, which provided, among other things, recommendations about possible reforms to

the privacy implications of the StingRay and, in amending the Pen/Trap statute, knowingly authorized law enforcement use of this technology.

¹³³ The one exception we know of is a January 28, 2014 public State Congressional oversight hearing (meeting) in the Minnesota House of Representatives House Civil Law Committee that explored state and local law enforcement use of cellular interception devices. *See* Minn. H.R. Civil Law Committee Audio & Video Archives, http://www.house.leg.state.mn.us/audio/archivescomm.asp?comm=88003&ls_year=88. The hearing took place because a bi-partisan group of State legislators' concerns about the technology were not satisfied by written correspondence from the Minnesota Public Safety Commissioner. *See* Camey Thibodeau, *Cell Phone Tracking Devices Available to Police*, FARIBAULT DAILY NEWS, Feb. 4, 2014, http://www.southernminn.com/faribault_daily_news/news/local/article_b6719fc2-2656-51c4-89e3-861e6179b2fe.html ("Privacy concerns related to the devices were addressed at an oversight hearing held this week by the Minnesota House Civil Law Committee.").

¹³⁴ *See* cell phone location tracking discussion, *supra* Part II.A.

¹³⁵ *See Transcript: President Obama's August 9, 2013 news conference at the White House*, WASH. POST, Aug. 9, 2013, http://articles.washingtonpost.com/2013-08-09/politics/41225505_1_civil-liberties-oversight-board-open-debate-surveillance-programs (outlining steps, post-Snowden disclosures, to foster debate and reform of intelligence collection programs including the President's intent to convene an outside group of experts to review surveillance technologies and capabilities).

the Section 215 metadata program.¹³⁶ A far more detailed report focusing on the Section 215 metadata program was subsequently released by the Privacy and Civil Liberties Oversight Board (PCLOB).¹³⁷ The PCLOB is an independent, bi-partisan Executive Branch agency authorized by Congress in the context of the “war on terrorism” to ensure, among other things, that “liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism.”¹³⁸

While Congress has currently authorized PCLOB oversight only of government efforts to protect the nation from terrorism (and the recent PCLOB report on Section 215 and the operations of the FISC is part of that oversight effort), there is no impediment to congressional expansion of the PCLOB’s mandate to review, advise, and counsel more generally on surveillance technologies and methods that permeate current criminal investigations (or those that could reasonably be predicted to do so in the future), even if they do not necessarily relate to government efforts to protect the Nation against terrorism. Congress could, for example, task the PCLOB with studying the specific surveillance technologies and methods that are in use or reasonably likely to be used by various law enforcement agencies in criminal investigations and the legal authorities the government believes authorizes or, conversely, does not prohibit their use. The goal of such an assessment should be the production of written recommendations by the PCLOB to Congress specifying which technologies are in need of

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 34 of 38

¹³⁶ Notably, the report recommended that bulk records collected under the 215 metadata program should no longer be held by the government, but rather, by a private third party. *See LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT’S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES* 25 (2013), <http://www.lawfareblog.com/wp-content/uploads/2013/12/Final-Report-RG.pdf>.

¹³⁷ *See supra* note 8. The PCLOB’s Chairman, David Medine, when referring to the summer 2013 disclosures stated that “Our [the PCLOB’s] challenge is to understand exactly how these programs work, but speak about them publicly in a way that Americans can understand the programs and evaluate them. We will work in some cases to have information declassified, if it permits us a greater opportunity to explain how these programs work . . . Our view is to try to enhance counterterrorism efforts but also enhance Americans’ privacy and civil liberties.” Cogan Schneier, *Privacy and Civil Liberties Board Works to Inform Public on NSA Leaks*, FED. NEWS RADIO, July 25, 2013, <http://www.federalnewsradio.com/411/3400357/Privacy-and-Civil-Liberties-board-works-to-inform-public-on-NSA-leaks>.

¹³⁸ 42 U.S.C. § 2000(c)(2) (2012). Some aspects of the PCLOB’s report pertaining to the Section 215 metadata program and dissenting views from two PCLOB Members are discussed in the Introduction and accompanying footnotes.

A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

direct authorization or prohibition, and which statutory authorities need to be updated and amended to accommodate or prohibit their use.

In service of this goal, Congress should further direct the PCLOB to write public reports at regular intervals (which could also, if necessary, include non-public or classified addenda) making such recommendations and directly identifying privacy issues associated with law enforcement's use of new surveillance technologies or collection methods, as well as old technologies like the StingRay, whose current or likely future use gives rise to new privacy concerns.¹³⁹ Moreover, for purposes of conducting the investigation and analysis leading to its written recommendations, Congress should both direct and empower the PCLOB to talk with all relevant government agencies, surveillance technology manufacturers, outside technologists and any other parties or entities that would provide relevant information.¹⁴⁰

The StingRay and its capabilities invoke several important questions that should guide the PCLOB in making recommendations about technologies and methods Congress should regulate directly. This brief list is illustrative, though in no sense exhaustive, of some inquiries the PCLOB should consider:

- (1) Is the technology or technique in question invasive of common and legal conceptions of personal privacy?;

¹³⁹ We would suggest that once Congress expands PCLOB's mandate and authorizes additional funding and staff for this purpose, PCLOB be given a year to produce the first report, followed by intervals of three years for new reports so that, following the first report, there is a sufficient period of time to assess how law enforcement may be using new technologies or collection methods and the privacy implications associated with such use.

¹⁴⁰ Under current statutory authority, for example, the PCLOB has the power to: "procure the temporary or intermittent services of experts and consultants," 42 U.S.C. § 2000(j)(3); "have access from any department, agency, or element of the executive branch, or any Federal officer or employee of any such department, agency, or element, to all relevant records, reports, audits, reviews, documents, papers, recommendations, or other relevant material, including classified information consistent with applicable law;" "interview, take statements from, or take public testimony from personnel of any department, agency, or element of the executive branch, or any Federal officer or employee of any such department, agency, or element;" "request information or assistance from any State, tribal, or local government" and; "at the direction of a majority of the members of the Board, submit a written request to the Attorney General of the United States that the Attorney General require, by subpoena, persons (other than departments, agencies, and elements of the executive branch) to produce any relevant information, documents, reports, answers, records, accounts, papers, and other documentary or testimonial evidence." *Id.* at § 2000(g)(1)(A)-(D).

- (2) Does it challenge a common-sense understanding of the statutory text that the government interprets to authorize its use?;
- (3) Is it an indiscriminate collection method that intercepts data from innocent cell phones in the coverage area of the mobile device being targeted?;
- (4) Is it an unmediated surveillance method that leaves no trace of its use beyond internal government agency records?; and
- (5) Might it, without such oversight or other regulation, otherwise remain hidden from any degree of public perception or scrutiny?

These questions suggest what we would describe as a minimal examination of the privacy implications and potential need for regulation of law enforcement use of any new technology or novel technique, particularly an unmediated surveillance device like the StingRay. The lines of inquiry encompass the interaction between a specific surveillance technology or technique and relevant cultural norms regarding the expectation of privacy, the specific legal interpretations the government would employ to support its use, the scope of the data collection involved, as well as the physical index, if any, present during its use and the record or trace, if any, it leaves afterwards.

VI. CONCLUSION

Knowledge and perception must precede oversight. Congress cannot understand or regulate a surveillance technology it cannot “see” clearly, whether through conceptual understanding of its operation before the fact or actual analysis of the history of its use. The StingRay is a law enforcement surveillance technology that has, for nearly two decades, evaded direct congressional scrutiny, much less informed authorization or regulation. Moreover, the StingRay illustrates how law enforcement agencies can use surveillance technologies and methods, justified by expansive and potentially problematic interpretations of existing statutes, for years before they ever come to the attention of Congress—if they ever do. We have thus argued that an authoritative, reliable procedure must be established to put Congress on notice about the functions, capabilities and historical use, if any, of new surveillance technologies and methods if the law is ever to keep pace with technological change. As they are for the

A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

newest of technologies, the need for such procedures is applicable even to decades-old technologies like the StingRay, whose expanding surveillance capabilities, combined with its increasing frequency of use by law enforcement at ever-descending costs,¹⁴¹ invoke privacy implications not heretofore appreciated.

Indeed, we are entering an era where law enforcement agencies have the technical capability to hack into the computers and phones of surveillance targets, allowing them covertly to activate webcams and microphones, search through documents, and obtain a person's web browsing history.¹⁴² These capabilities have been acquired and used without

¹⁴¹ For a discussion of the declining costs of cellular interception technology and corresponding frequency of use by law enforcement, see generally Pell & Soghoian, *supra* note 25.

¹⁴² See Jennifer Valentino-DeVries and Danny Yadron, *FBI Taps Hacker Tactics to Spy on Suspects*, WALL ST. J., Aug. 3, 2013, <http://online.wsj.com/article/SB10001424127887323997004578641993388259674.html> ("Law-enforcement officials in the U.S. are expanding the use of tools routinely used by computer hackers to gather information on suspects . . . With such technology, the bureau can remotely activate the microphones in phones running Google Inc.'s Android software to record conversations, one former U.S. official said. It can do the same to microphones in laptops without the user knowing."); see also Craig Timberg and Ellen Nakashima, *FBI's search for 'Mo,' Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, WASH. POST, Dec. 6, 2013, http://www.washingtonpost.com/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html ("Such high-tech search tools, which the FBI calls "network investigative techniques," have been used when authorities struggle to track suspects who are adept at covering their tracks online. The most powerful FBI surveillance software can covertly download files, photographs and stored e-mails, or even gather real-time images by activating cameras connected to computers, say court documents and people familiar with this technology. . . . The FBI has been able to covertly activate a computer's camera — without triggering the light that lets users know it is recording — for several years, and has used that technique mainly in terrorism cases or the most serious criminal investigations, said Marcus Thomas, former assistant director of the FBI's Operational Technology Division in Quantico."); see also Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, WIRED, Sept. 13, 2013, <http://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi/> ("[T]he FBI yesterday acknowledged that it secretly took control of Freedom Hosting last July, days before the servers of the largest provider of ultra-anonymous hosting were found to be serving custom malware designed to identify visitors. . . . Security researchers dissected the [FBI] code and found it exploited a security hole in Firefox to identify users of the Tor Browser Bundle, reporting back to a mysterious server in Northern Virginia.").

For examples of actual court documents pertaining to law enforcement hacking, see Search Warrant Application, 1:12-sw-05685-KMT (D. Colo. Oct. 9, 2012) (application from the ATF for a warrant seeking permission to use a "Network Investigative Technique" to remotely search the computer of an individual believed to be making bomb threats); *In re*

any public congressional hearings or other open debate, much less any explicit legislative mandate. As it hints at technological disruptions to come and how the legal disorder they bring may unfold, the StingRay offers strong evidence that now is the time to establish a reliable mechanism that will be a continuous source of useful guidance to Congress as more powerful surveillance tools emerge and evolve to challenge the very notion of privacy as they strengthen the ability of the government to monitor and control the lives of its citizens. For more new and powerful surveillance tools shall certainly emerge in the coming age than are “dreamt of in [our] philosophy” of personal privacy or its current practical expression in our laws.¹⁴³

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 38 of 38

Warrant to Search a Target Computer at Premises Unknown, No. H-13-234M (S.D. Tex. Apr. 22, 2013),

<http://files.cloudprivacy.net/Order%20denying%20warrant.MJ%20Smith.042213.pdf> (court order denying an application from the FBI to surreptitiously install data extraction software on the computer of a target). Reporter Jennifer Valentino-Devries noted that “[t]he judge’s order said the data the FBI could obtain includes ‘search terms that the user entered into any Internet search engine, and records of user-typed Web addresses.’ The government also is seeking email contents, documents and chat-messaging logs on the computer, as well as to take photographs for 30 days using the computer’s built-in camera, the document states.”) *Judge Denies FBI Request to Hack Computer in Probe*, WALL ST. J., Apr. 24, 2013,

<http://online.wsj.com/article/SB10001424127887324743704578443011661957422.html>.

¹⁴³ “There are more things in heaven and earth Horatio, Than are dreamt of in your philosophy.” WILLIAM SHAKESPEARE, HAMLET act 1, sc. 5.

ELECTRONICALLY FILED
 7/2/2015 12:12 PM
 2014-CH-15338
 CALENDAR: 11
 PAGE 1 of 2
 CIRCUIT COURT OF
 COOK COUNTY, ILLINOIS
 CHANCERY DIVISION
 CLERK DOROTHY BROWN

SnoopSnitch

SnoopSnitch is an Android app that collects and analyzes mobile radio data to make you aware of your mobile network security and to warn you about threats like fake base stations (IMSI catchers), user tracking and over-the-air updates. With SnoopSnitch you can use the data collected in the GSM Security Map at gsmmap.org and contribute your own data to GSM Map.



This application currently only works on Android phones with a Qualcomm chipset and a stock Android ROM (or a suitable custom ROM with Qualcomm DIAG driver). It requires root privileges to capture mobile network data.

Documentation

For details on SnoopSnitch please refer to the FAQ.

Requirements:

- Qualcomm-based Android phone (see device list)
- **Stock** Android ROM, version 4.1 or later

Note: Custom Android ROMs like CyanogenMod may or may not work, depending on the availability of a Qualcomm DIAG kernel driver (DIAG_CHAR).
- **Root privileges** on phone

Incompatible Devices:

The following devices have been found to be incompatible and can **not** be used with SnoopSnitch:

- **Unsupported.** Devices with custom ROM such as CyanogenMod which lacks the Qualcomm DIAG kernel driver (DIAG_CHAR)
- **Unsupported.** Every device without Qualcomm chipset
- **Unsupported.** Samsung Galaxy S2 & S3
- **Unsupported.** Nexus 5 with stock Android
- **Unsupported.** Huawei Ascend Y300

Download:

- Pre-compiled .apk (SHA1: d55fcb3e849e0e18a7a307e6c2125e04ddeb7fd0)
- Pre-compiled .apk from Google Play Store
- Pre-compiled .apk from F-Droid
- Source Code:

```
git clone --recursive https://opensource.srlabs.de/git/snoopsnitch.git
```

SnoopSnitch is released under the GPL v3 license (cf. source:COPYING). The app is known to built under Linux and OS X, see source:README for build instructions.

Disclaimer

The tests include an active part. First, your phone will place outgoing calls to a dedicated number. This number will always be busy and never answer in order to rule out voice charges as best as we can.

Second, your phone will send SMS short messages to an invalid number. In some cases, we saw operators charging for these kind of transactions transactions. Hence, please have an eye on your phone bill when performing active tests using SnoopSnitch. To control for involuntary charges, we strongly advise the use of a dedicated pre-paid SIM card for these tests.

Furthermore, our call server will call your phone and send test SMS during the active test. To avoid unnecessary costs on our side, **DO NOT PICK UP OR REJECT AUTOMATIC CALLS FROM OUR SERVER.** If you pick up a call or have a mailbox or auto-answer

Exhibit 1-AP

feature configured that picks up the call automatically you may get blacklisted and cannot use our service anymore. Please see our [Banned](#) wiki page for details.

Instructions

1. Make sure you have rooted the phone
2. Install application from [Google Play app store](#) or below
3. Run the app, execute active tests, upload security events and suspicious activity

Mailing list

A public mailing list for discussions is [here](#)

For specific questions to the snoopsnitch-team that do not require or permit public discussion, please contact us directly at **snoopsnitch [you know what to put here]**
srlabs.de

Version history

Version 0.9.7

- Improve detection of type 1 catchers and silent calls
- Reduce false positive rate
- Upload anonymized metadata additionally to radio traces
- Various enhancements and bug fixes

Version 0.9.5

- Make detection run automatically on boot
- Support LTE active tests
- Improve detection of 2G/3G catchers
- Detect empty WAP pushes

Version 0.9.4

- Improve type 1 catcher and silent SMS detection
- Implement network info screen
- Detect malfunctioning baseband interface
- Various enhancements and bug fixes

Version 0.9.3

- Support Android 5
- Fix initialization issue on newer devices
- Translation to German and Dutch

Version 0.9.2

- Fixed app lock-up issues
- Improved device compatibility check
- Handled unsupported LTE gracefully

Version 0.9.1

- Fix problem where SnoopSnitch would leave the phone muted after a test
- Remove issue with disappearing (Skype) dialing dialogs
- Resolved performance issue in analysis

Version 0.9.0

- Initial public release

[sc_map_overview.png \(702 KB\)](#) Alex, 12/23/2014 11:11 PM

[sc_map_details.png \(432 KB\)](#) Alex, 12/23/2014 11:11 PM

[sc_catcher_hour.png \(105 KB\)](#) Alex, 12/26/2014 04:18 PM

[sc_dashboard.png \(95.5 KB\)](#) Alex, 12/26/2014 04:25 PM

[SnoopSnitch-0.9.0.apk \(3.9 MB\)](#) Alex, 12/26/2014 04:33 PM

[SnoopSnitch-0.9.1.apk \(3.9 MB\)](#) Alex, 12/29/2014 12:48 PM

[SnoopSnitch-0.9.2.apk \(3.9 MB\)](#) Alex, 01/08/2015 03:06 PM

[SnoopSnitch-0.9.3.apk \(4.01 MB\)](#) Alex, 01/19/2015 10:19 AM

[SnoopSnitch-0.9.4.apk \(4.04 MB\)](#) Alex, 02/23/2015 06:28 PM

[SnoopSnitch-0.9.5.apk \(4.12 MB\)](#) Alex, 03/20/2015 07:42 PM

[SnoopSnitch-0.9.7.apk \(4.14 MB\)](#) Jakob, 05/13/2015 03:51 PM

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 2 of 2

Law Offices

191 N. Wacker Drive
Suite 3700
Chicago, IL
60606-1698

(312) 569-1000
(312) 569-3000 fax
www.drinkerbiddle.com

CALIFORNIA
DELAWARE
ILLINOIS
NEW JERSEY
NEW YORK
PENNSYLVANIA
WASHINGTON D.C.
WISCONSIN

VIA E-MAIL

Matthew Topic
Loevy & Loevy
312 N. May Street
Suite 100
Chicago, Illinois 60607
matt@loevy.com

Re: NOTICE OF RESPONSE
REQUEST RECEIVED: January 9, 2015
FOIA FILE NO.: 15-0098

Dear Mr. Topic:

The City of Chicago has retained Drinker Biddle & Reath LLP to assist in responding to your Illinois Freedom of Information Act ("FOIA") request received by the Chicago Police Department ("CPD") on January 9, 2015, a copy of which is attached. On January 23, 2015, you agreed to extend CPD's response date to January 30, 2015. On January 30, 2015, you further agreed to extend CPD's response date to February 5, 2015.

Your request has been reviewed by CPD and Drinker Biddle & Reath LLP, and documents responsive to your request have been searched for and/or produced by the Bureau of Organized Crime Division. Upon review, CPD hereby responds to your requests as follows:

1. *All records provided by Jack Costa to the office of the Chief of the BOC as described in Sgt. Costa's affidavit submitted with CPD's motion to dismiss in Martinez v. Chicago Police Department, 2014 CH 15338, excluding the records deemed responsive to the FOIA requests at issue in that case and described in CPD's motion to dismiss.*

CPD understands this request as seeking documents related to cell site simulator equipment that Sergeant Jack Costa provided to the office of the Chief of the Bureau of Organized Crime at the request of that office as referenced in his December 10, 2014, affidavit other than any such documents that have been deemed responsive to the FOIA requests at issue in case number 2014 CH 15338. The enclosed documents are responsive to this request.

On February 4, 2015, you sent an email to CPD asking that the following language be added to the end of this request: "and excluding records within the scope of

February 5, 2015

Matthew Topic
February 5, 2015
Page 2

the request at issue in 2014 CH 9565 in light of Judge Kennedy's ruling denying CPD's motion to dismiss that case." A copy of that email is attached to this letter.

CPD does not understand Judge Kennedy's ruling as providing any guidance on what records CPD should have provided in response to the FOIA request at issue in 2014 CH 9565. Indeed, the ruling does not reference any specific records that CPD should have produced in response to the FOIA request at issue in 2014 CH 9565, nor does it provide definitive or final guidance on the scope of that request.

Accordingly, CPD has not limited the scope of the production of records responsive to FOIA request No. 15-0098 as a result of your February 4, 2015, email, in an effort to avoid any disputes regarding what documents should or should not have been produced based on that email. CPD believes this is consistent with reading your FOIA request broadly.

There are documents responsive to your request that CPD has withheld or redacted based on applicable statutory exemptions. Section 7(1) of FOIA provides that "[w]hen a request is made to inspect or copy a public record that contains information that is exempt from disclosure under this Section, but also contains information that is not exempt from disclosure, the public body may elect to redact the information that is exempt."

Documents responsive to this request have been withheld or redacted under the following exemptions:

Section 7(1)(a) of FOIA provides that "information specifically prohibited from disclosure by federal or State law or rules and regulations implementing federal or State law" is exempt from release under the Act. 5 ILCS 104/7(1)(a). Documents responsive to this request have been withheld because disclosure is prohibited by federal rules and law, including the following federal laws:

- (i) 22 U.S.C. § 2778. The Arms Export Control Act and implementing regulations restrict the dissemination of technical information relating to regulated defense articles, including the equipment that is the subject of your request. Specifically, technical details concerning this equipment are subject to the non-disclosure provisions of the International Traffic in Arms Regulations (ITAR), 22 C.F.R. Parts 120-130. The ITAR requires anyone, prior to making an export of technical information, to obtain a license from the Department of State. Technical information need not leave the borders of the United States to be deemed an export. Providing technical information without a license to anyone intending to publicize the information could constitute a violation of the Arms Export Control Act. Documents responsive to this request contain information prohibited from disclosure by ITAR.

(ii) 18 U.S.C. § 3123. The Federal Pen Register Statute provides that orders authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that the order be sealed until otherwise directed by the court. In addition, disclosure of certain responsive documents is prohibited by state law, as certain responsive documents have been placed under seal by an Illinois state court.

Section 7(1)(d)(v) of FOIA exempts documents that “disclose unique or specialized investigative techniques other than those generally used and known. . . .” 5 ILCS 7(1)(d)(v). Documents responsive to this request have been withheld because they disclose information regarding a unique and specialized investigative technique not otherwise known to members of the public, namely, the capabilities, settings, limitations, and deployment of cell site simulator equipment.

Section 7(1)(f) of FOIA exempts “[p]reliminary drafts, notes, recommendations, memoranda and other records in which opinions are expressed, or policies or actions are formulated” 5 ILCS 7(1)(d)(v). Portions of the enclosed documents and withheld documents fall within this exemption because they contain an internal policy discussion regarding the equipment subject to the request.

Section 7(1)(g) of FOIA exempts “[t]rade secrets and commercial or financial information obtained from a person or business where the trade secrets or commercial or financial information are furnished under a claim that they are proprietary, privileged or confidential, and that disclosure of the trade secrets or commercial or financial information would cause competitive harm to the person or business, and only insofar as the claim directly applies to the records requested.” 5 ILCS 140/7(1)(g). Some of the enclosed documents contain third-party commercial and financial information obtained from a business under a claim that the information is confidential and proprietary. In addition, CPD has withheld from documents responsive to this request as they contain trade secrets and commercial information obtained from Harris Corporation under a claim that they are proprietary, the disclosure of which would cause competitive harm.

Section 7(1)(i) of FOIA exempts “[v]aluable formulae, computer geographic systems, designs, drawings and research data obtained or produced by any public body when disclosure could reasonably be expected to produce private gain or public loss. . . .” 5 ILCS 10/7(1)(i). Documents responsive to this request include information regarding the specific capabilities, settings, limitations, deployment, and depictions of cell site simulator equipment, which is exempt under this provision.

Section 7(1)(v) of the Illinois FOIA exempts “[v]ulnerability assessments, security measures, and response policies or plans that are designed to identify, prevent, or respond to potential attacks upon a community’s population or systems, facilities, or installations, the destruction or contamination of which would constitute a clear and present danger to the health or safety of the community. . . .” 5 ILCS 140/7(1)(v). Certain responsive

Matthew Topic
February 5, 2015
Page 4

documents disclose the specific capabilities, limitations, and deployment of cell site simulator equipment and thus are exempt under the provision.

2. *All policies, procedures, directives, orders, and other such records that govern access by Chicago Police Department officers to Harris Corporation manuals for cell site simulators.*

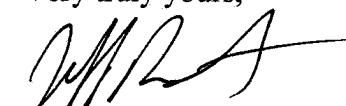
CPD has been unable to locate any documents responsive to this request.

CPD's online library of directives is available at <http://home.chicagopolice.org/inside-the-cpd/department-directives-system/>. Section 8.5(a) of FOIA provides that “[n]otwithstanding any provision of this Act to the contrary, a public body is not required to copy a public record that is published on the public body's website. The public body shall notify the requester that the public record is available online and direct the requester to the website where the record can be reasonably accessed.” 5 ILCS 140/8.5(a). CPD searched this online library of directives as part of its search for records potentially responsive to your request and found no responsive documents, but you may also conduct your own search of the online library of directives to determine whether it contains any documents responsive to your request.

3. *Records sufficient to identify by name the specific Chicago Police Department officers who have ever had access or been authorized to have access to any Harris Corporation manuals for cell site simulators.*

CPD has been unable to locate any documents responsive to this request.

Very truly yours,


Jeff Perconte

Enclosure

Matthew Topic
February 5, 2015
Page 5

You have the right of review of this denial by the Illinois Attorney General's Public Access Counselor (PAC). You can file a request for review by writing to:

Public Access Counselor
Office of the Attorney General
500 2nd Street
Springfield, Illinois 62706

You may also seek judicial review of a denial under 5 ILCS 140/11 by filing a lawsuit in the State Circuit Court.

FOIA Request

Matt Topic [matt@loevy.com]

Sent: Friday, January 09, 2015 9:25 AM

To: FOIA

Cc: Collins, Daniel J. [Daniel.Collins@dbr.com]; Freddy M [freddyinchicago@gmail.com]; Kelsey Lutz [kelsey@loevy.com]

My client, Freddy Martinez, requests PDF copies of the following records to be delivered to me by email to this address, or if that is not feasible, by a mutually agreeable alternative mechanism of delivery (please contact me to discuss if needed):

1. All records provided by Jack Costa to the office of the Chief of the BOC as described in Sgt. Costa's affidavit submitted with CPD's motion to dismiss in Martinez v. Chicago Police Department, 2014 CH 15338, excluding the records deemed responsive to the FOIA requests at issue in that case and described in CPD's motion to dismiss.
2. All policies, procedures, directives, orders, and other such records that govern access by Chicago Police Department officers to Harris Corporation manuals for cell site simulators.
3. Records sufficient to identify by name the specific Chicago Police Department officers who have ever had access or been authorized to have access to any Harris Corporation manuals for cell site simulators.

This is not a commercial request. Please do not communicate with me through any means other than by email to this email address.

Matthew Topic
Loevy & Loevy

312 N. May Street, Suite 100
Chicago, IL 60607
312-789-4973 (office)
773-368-8812 (cell)
matt@loevy.com

The sender of this email is an attorney. The information contained in this communication is confidential, may be attorney-client privileged, may be attorney work product, and is intended only for the use of the addressee. It is the property of the sender. Unauthorized use, disclosure or copying of this communication or any part thereof is strictly prohibited and may be unlawful. If you have received this communication in error, please notify me immediately by return e-mail, and destroy this communication and all copies thereof, including all attachments.

Perconte, Jeff

From: Matt Topic <matt@loevy.com>
Sent: Wednesday, February 04, 2015 6:30 AM
To: FOIA
Cc: Collins, Daniel J.; Freddy M; Kelsey Lutz; Perconte, Jeff
Subject: Re: FOIA Request

I have realized an error in item #1. We hereby modify that item to the following, with the addition shown in underline:

1. All records provided by Jack Costa to the office of the Chief of the BOC as described in Sgt. Costa's affidavit submitted with CPD's motion to dismiss in Martinez v. Chicago Police Department, 2014 CH 15338, excluding the records deemed responsive to the FOIA requests at issue in that case and described in CPD's motion to dismiss and excluding records within the scope of the request at issue in 2014 CH 9565 in light of Judge Kennedy's ruling denying CPD's motion to dismiss that case.

This same change should be made with regard to Mr. Martinez's other pending FOIA requests: those requests were not intended to seek records within the scope of the request at issue in 2014 CH 9565 in light of Judge Kennedy's ruling denying CPD's motion to dismiss that case.

Thanks.

7/2/2015 12:12 PM
2014-CH-15338
Mail
PAGE 7 of 8

Matthew Topic
Loevy & Loevy

312 N. May Street, Suite 100
Chicago, IL 60607
312-789-4973 (office)
773-368-8812 (cell)
matt@loevy.com

The sender of this email is an attorney. The information contained in this communication is confidential, may be attorney-client privileged, may be attorney work product, and is intended only for the use of the addressee. It is the property of the sender. Unauthorized use, disclosure or copying of this communication or any part thereof is strictly prohibited and may be unlawful. If you have received this communication in error, please notify me immediately by return e-mail, and destroy this communication and all copies thereof, including all attachments.

On Fri, Jan 9, 2015 at 9:25 AM, Matt Topic <matt@loevy.com> wrote:

My client, Freddy Martinez, requests PDF copies of the following records to be delivered to me by email to this address, or if that is not feasible, by a mutually agreeable alternative mechanism of delivery (please contact me to discuss if needed):

1. All records provided by Jack Costa to the office of the Chief of the BOC as described in Sgt. Costa's affidavit submitted with CPD's motion to dismiss in Martinez v. Chicago Police Department, 2014 CH 15338, excluding the records deemed responsive to the FOIA requests at issue in that case and described in CPD's motion to dismiss.

2. All policies, procedures, directives, orders, and other such records that govern access by Chicago Police Department officers to Harris Corporation manuals for cell site simulators.
3. Records sufficient to identify by name the specific Chicago Police Department officers who have ever had access or been authorized to have access to any Harris Corporation manuals for cell site simulators.

This is not a commercial request. Please do not communicate with me through any means other than by email to this email address.

Matthew Topic
Loevy & Loevy

312 N. May Street, Suite 100

Chicago, IL 60607

312-789-4973 (office)

773-368-8812 (cell)

matt@loevy.com

The sender of this email is an attorney. The information contained in this communication is confidential, may be attorney-client privileged, may be attorney work product, and is intended only for the use of the addressee. It is the property of the sender. Unauthorized use, disclosure or copying of this communication or any part thereof is strictly prohibited and may be unlawful. If you have received this communication in error, please notify me immediately by return e-mail, and destroy this communication and all copies thereof, including all attachments.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 8 of 8

Crime, Corruption and Cover-ups

in the Chicago Police Department



Anti-Corruption Report Number 7

January 17, 2013

Authored by:

John Hagedorn
Bart Kmiecik
Dick Simpson
Thomas J. Gradel
Melissa Mouritsen Zmuda
David Sterrett

With

Ivana Savic
Justin Escamilla
Magdalena Waluszko
Dalibor Jurisic
Tricia Chebat

Published by University of Illinois at Chicago
Department of Political Science

Exhibit 1-AR

The Chicago Police Department has a legacy of both heroism and corruption. On the one hand, the department's officers risk their lives on a daily basis to enforce the law, protect the public and preserve the peace. On the other hand, Chicago has a checkered history of police scandals and an embarrassingly long list of police officers who have crossed the line to engage in brutality, corruption and criminal activity.

An analysis of five decades of news reports reveals that since 1960, a total of 295 Chicago Police officers have been convicted of serious crimes, such as drug dealing, beatings of civilians, destroying evidence, protecting mobsters, theft and murder.

Moreover, the listing of police convicted of crimes undoubtedly underestimates the problem of corruption in the Chicago Police Department (CPD). The list does not include undetected and unreported illegal activity, serious misconduct resulting in internal disciplinary action, and officers who retire rather than face charges.

Our analysis of police corruption in Chicago yields four major findings.

First, corruption has long persisted within the CPD and continues to be a serious problem. There have been 102 convictions of Chicago police since the beginning of 2000.

Second, police officers often resist reporting crimes and misconduct committed by fellow officers. The "blue code of silence," while difficult to prove, is an integral part of the department's culture and it exacerbates the corruption problems. However last November, a federal jury found that the City of Chicago and its police culture were partially responsible for Officer Anthony Abbate's brutal beating of a female bartender. After the civil trial to assess damages, the victim's attorney declared, "We proved a code of silence at every level in the Chicago Police Department."¹

Third, overtime a large portion of police corruption has shifted from policemen aiding and abetting mobsters and organized crime to officers involved with drugs dealers and street gangs. Since the year 2000, a total of 47 Chicago law enforcement officers were convicted of drug and gang related crimes. The department's war on drugs puts police officers, especially those working undercover, in dangerous situations where they must cooperate with criminals to catch criminals. These endeavors require that CPD superiors provide a high degree of leadership and oversight to keep officers on the straight and narrow.

Fourth, internal and external sources of authority, including police superintendents and Mayors, have up to now failed to provide adequate anti-corruption oversight and leadership.

The case of Lieutenant Jon Burge, Commander of Area 2 Detective Division, accused of

torturing suspects to extract confessions is the most notorious, high-profile example of the lack of accountability in the department involving several state's attorneys and mayors. The "blue wall of silence" protected Burge and his many accomplices. Despite numerous courts overturning convictions and several media exposés, the CPD leadership and Mayor's office denied and evaded evidence that Burge and 64 other officers tortured more than 100 African-American suspects over several decades. In addition, dozens, if not hundreds, of police officers, who were present at the stations while the torture occurred or who heard about it from co-workers, failed to report the torture to the proper authorities.

The Cook County State's Attorney never prosecuted a single officer for any crimes related to torture. And, there is no evidence that the Police Department ever disciplined any officer for failing to come forward with information about the tortures.

Finally, the United States Attorney stepped in and prosecuted Jon Burge. Last year, he was convicted in federal court, not for torture but for lying about it under oath. The dozens of other police officers involved in the torture cases were not prosecuted. By 2012, the statute of limitation had expired.

In this report, as well as in the previous six anti-corruption reports published by the Political Science Department, public corruption has been defined as an illegal or unethical act committed by a public official for his or her self interest rather than for the public good.

While we relied on a set of 295 criminal convictions of police offices to analyze and classify police corruption, it should be noted that most unethical behavior and non-criminal misconduct also fits the definition of corruption. Also while some non-criminal misconduct committed by individual officers may not its self be "corruption," it is often swept under the rug or covered-upped by the department to avoid embarrassment. Toleration of such misconduct is definitely "corruption."

Toleration of corruption, or at least resigned acceptance, appears to be the order of the day for at least the past 50 years. The department's Internal Affairs Division (IAD), the Independent Police Review Authority (IPRA), Police Board (PB), the department's top brass, the Mayor's office, and State Attorneys have all failed to aggressively and effectively reign in police corruption. In recent years, only the U.S. Attorney's Office has made a serious effort to curb police corruption.

In 2007, police consultant Lou Reiter testified in court that the department's lack of effective oversight was the product of "deliberate indifference" by CPD leaders.² The lack of an effective crackdown on police misconduct can be inferred from a 2007 study by University of Chicago law professor Craig Futterman.³ He found that only 19 of 10,149 (or less than 2%)

civilian complaints of excessive force, illegal searches, racial abuse, sexual abuse and false arrests between 2002 and 2004 led to police suspensions of a week or more.

The listing in our report of [the 295](#) convicted police officers and their illegal activities demonstrate that corruption in Chicago Police Department is not confined to a few isolated cases. While people can debate whether the CPD has a culture that promotes corruption, the findings clearly show that the CPD has at the very least a culture that tolerates police misconduct and corruption.

Police corruption not only undermines public trust in law enforcement, but also corruption related prosecutions, lawsuits, defense and settlements cost taxpayers millions of dollars. Jon Burge cases have cost local taxpayers more than \$53 million since 1998.⁴ Moreover since 2003, the City of Chicago has spent more than \$82.5 million to defend police against misconduct charges with about a quarter of that total related to Burge.⁵ In addition, the city paid \$21 million in 2009 for compensatory damages in a wrongful conviction case involving Juan Johnson⁶, and \$18 million in 2001 to settle a case involving an unarmed woman shot by police⁷.

The city also spends hundreds of thousands of dollars investigating police misconduct each year. Clearly these cases of police abuse and corruption have cost taxpayers several hundreds of millions of dollars at a time when all levels of government have to cut services and raise taxes.

The CPD's heavy focus on drug and gang activity, and the "blue code of silence" both present serious obstacles to reducing police corruption. Police officers loyalty to their colleagues understandably runs deep, but law enforcement officials should not ignore the criminal acts of their co-workers. Speaking out against a fellow officer can be difficult, and even dangerous. Only a few years ago a high profile police officer, Jerome Finnegan, hired a gang hit man to kill fellow officers who were preparing to testify against him.⁸ Encouraging officers to report corrupt or criminal acts of their colleagues and increasing oversight over officers is not easy. Nor will it be easy to reduce corruption when police are so heavily involved with gangs and lucrative drug dealing networks.

Proposals in the last section of this report recommend a combination of external review and internal incentives. They are based the experience of police departments from around the world and on academic studies. These proposed reforms are designed to create effective oversight structures and a culture of honest service within the CPD. If adopted, these reforms would help alleviate the serious problem of corruption in the police department.

History of Chicago Police Department Corruption

For nearly a century, Chicago's political machines included police protection for gambling and prostitution and for vice lords like Mike McDonald and Big Jim Colisimo. In the 1920s, prohibition led to beer war violence and an alliance of Capone's mob with Republican Mayor William Hale Thompson. While the 1930s New Deal saw the Democratic Party taking power while the alliance between City Hall and Frank Nitti's Outfit continued to reign.

Reports from many sources, including Landesco's *Organized Crime in Chicago*, Lindberg's *To Serve and Collect*, Drake & Cayton's *Black Metropolis*, and Karen Abbot's *Sin in the Second City*, document rampant police corruption in the first half of the 20th century.

After the 1960 Summerdale scandal, where a police unit worked as a burglary crew, Mayor Richard J. Daley hired Orlando W. Wilson as his new Superintendent of Police. Wilson, a criminologist from The University of California Berkeley, was told to professionalize and clean up the CPD. According to Ovid Demaris in his corruption classic, *Captive City*, Wilson remarked to Congress in 1962 that of the 985 mob murders since the 1920s, only two had been solved. The Outfit, as the Chicago mob was also commonly known, was getting away with murder. Neither Superintendent Wilson nor the state's attorney went after the Outfit in a systematic way. With rare exception, the Cook County's State's Attorneys have avoided investigating the Outfit, which has always had highly placed friends in the machine. At the end of his term Wilson told Life Magazine, "Cosa Nostra in Chicago was so entrenched that he had barely scratched its surface. Nor had he been able to eradicate corruption in Chicago's police force."⁹

Beginning in the 1960s, when the Chicago Outfit was still the nation's second most powerful criminal organization, the CPD and the state's attorney turned their attention away from organized crime to the new street gangs. Street gangs, not the Outfit, began to control the retail distribution of drugs, gambling and prostitution. A "War on Gangs" declared in 1969 by Mayor Richard J. Daley and State's Attorney Edward Hanrahan, took aim at black and Latino gangs. At the same time, Chicago's Outfit sought greater profits from its operations in Las Vegas and Hollywood, and through control of the Teamsters Pension Fund. But while Outfit's vice operations were protected by its still cozy relationship with the Chicago political machine, the

"The 'rotten apple' theory won't work any longer. Corrupt police officers are not natural-born criminals, nor morally wicked men, constitutionally different from their honest colleagues. The task of corruption control is to examine the barrel, not just the apples –the organization, not just the individuals in it—because corrupt police are made, not born."

-NYC Police Commissioner Patrick Murphy

street gangs had to cut their own deals with dirty cops. As the war on drugs progressed, more and more individual police officers were corrupted.

In the 1980s, police corruption again became front-page news. In 1982, ten officers in the Marquette police district were among the first Chicago police officers to be convicted of drug-related corruption charges. "The Marquette 10" arrests were followed by Operation Greylord, a federal investigation into the Cook County court system that swept up several corrupt police officers along with numerous judges, court bailiffs and attorneys. In the 1980s and 1990s, Joseph Miedzianowski, a member of the department's Gang Crimes Unit, ran a drug operation with several gangs.

The conviction of CPD Chief of Detectives and Assistant Police Superintendent William Hanhardt in 2001 for using secret police information to direct a mob-connected jewelry theft ring showed that organized crime could still reach into the CPD even in the 21st Century. The drug/gang connection continued into the current decade. In 2007, the U.S. Attorney's arrested of Keith Herrera and Jerome Finnegan of the Special Operations Squad for corruption and attempted murder.

Human rights violations have long plagued Chicago. At the end of the 1960s in the aftermath of anti-war protests, the Chicago Police Department's Subversive Activities Unit, known as the "Red Squad," spied on legitimate, non-criminal protesters, political activists and community organizations. Originally the "Red Squad" was supposed to provide surveillance of groups such as Communists, or Reds, thought to be plotting to overthrow the United States government. Later, however, the "Red Squad" spied on law-abiding individuals, officials and groups who opposed Mayor Richard J. Daley and the Democratic machine. Like many other secret police units, the Chicago "Red Squad" investigated and infiltrated dissenting political groups but when a group threatened those in power, the "Red Squad" would try to destroy it, directly or indirectly. Allegedly "Red Squad" officers committed criminal acts such as burglary, theft, and destruction of documents and equipment, all blatant violation of the First Amendment, according to the American Civil Liberties Union (ACLU).

Besides the ACLU, some of the groups targeted by the "Red Squad" were the National Association for the Advancement of Colored People, National Lawyers Guild, and Operation PUSH. By the end of the 1960s, the "Red Squad" had collected information on approximately 117,000 Chicagoan, 141,000 out-of-town individuals and 14,000 organizations.

In 1974, the Red Squad reportedly destroyed 105,000 individual and 1,300 organizational files when it learned that the Alliance to End Repression planned to file a lawsuit against the unit

for violating the U.S. Constitution.¹⁰ The ACLU then filed a lawsuit on behalf of 25 organizations and individuals including one of this report's authors, former Chicago Alderman Dick Simpson. After many years of litigation, a 1981 court decree ended the Chicago Police Department's "Red Squad's" unlawful surveillance of political dissenters and their organizations. Then to settle the lawsuit, the City of Chicago agreed to pay a total of \$335,000 to the plaintiffs and nearly \$20,000 in attorneys' fees. And on the last day of 1985, a federal judge ordered the city to pay an additional \$51,000 to two organizations and a civil rights activists who were illegally spied on by the "Red Squad."

The CPD also has a history of violating the human rights of African-Americans and other minorities. State's Attorney Edward Hanrahan orchestrated the infamous 1969 police raid that resulted in the shooting deaths of Fred Hampton and Mark Clark. Jon Burge headed up a team of officers in the 2nd Police District where many young, African-American men were tortured over several decades.

Conviction Analysis

In order to study the extent of police corruption in Chicago, we focused on reports of criminal convictions of police in newspapers, magazines, books and various other sources. Data on corruption that did not result in convictions was not available. Other officers are brought formally to the Police Review Board and some resigned to avoid formal charges. Some police misconduct is handled through a grievance process conducted by the department management and the police union. Generally, such cases are not reported in the news media. As a result, our information, which primarily is based on media reports of criminal convictions, very likely underestimates the breadth and severity of the police corruption problem.

However, the conviction statistics are the most concrete data available to assess and analyze the continuing problem of police corruption in Chicago. In addition, a more detailed look at the conviction cases reveals the strong connections between corruption and the war on drugs, the code of silence and the lack of internal and external oversight.

For each instance of police corruption or misconduct found, the following information was recorded:

- | | |
|---|--|
| <ul style="list-style-type: none"> - Officer's name - Rank, title, position - Date of conviction | <ul style="list-style-type: none"> - Type of incident - Description of the crime and related corruption - Source and citation |
|---|--|

Three hundred cases of police crime were documented. After compiling the database of police crime, all of the cases were collapsed and coded into the following categories with the frequencies with which they occurred:

Civil Right Violations (CRV) – 10 police officers guilty of illegal search and seizures, false arrests, malicious prosecutions and extended detentions.

Off Duty Crime (ODC) – 53 police officers committed crimes while off duty.

General Police Crime (GPC) – 114 officers involved in scams, tax fraud, stealing, extortion, lying, bribery, and theft.

Drugs, Guns and Gangs cases (DGG) -- 95 cases including gang-related illegal drug dealings, weapon sales and gang activity.

Brutality, Torture and Sex Abuse cases (BTX) – 23 cases involving brutal beatings, torture, sexual abuse and excessive force.

The War on Drugs

In studying corruption and in the war on drugs we find David Carter's typology to be useful, distinguishing between what he calls Type 1 and Type 2 acts of drug-related corruption. Type 1 is the drive for private gain, illegitimate acts that misuse the public status of an officer for his/her private gain, and illegitimate goals.

Type 2 corruption has the legitimate goal of prosecuting the bad guys, but uses illegitimate means of falsifying evidence, selling confiscated drugs from one gang to another in order to build a larger case, or lying under oath to get a prosecution.¹¹

Those officers who engage in misconduct and violate citizens' constitutional rights would do so with the perception that their misconduct would go undiscovered or investigated in such a deficient manner or subjected to prolonged delay in adjudication that they would not be held accountable or sanctioned.¹²

Lou Reiter, Police Consultant

TABLE 2
OPPORTUNITY FOR DRUG CORRUPTION BY ASSIGNMENT

<i>Assignment</i>	<i>Drug Exposure</i>	<i>Type 1 Corruption</i>	<i>Type 2 Corruption</i>
Patrol officers	Street dealers Arrests of persons in possession of drugs Response to calls where drugs are involved	Street bribes Street confiscation of drugs Protection money	Perjury with respect to the facts of the arrest Perjury of facts of the drug seizure
Drug and vice officers	Undercover (UC) Operations Generally Drug and money possession for role playing Social interaction with dealers and users in UC role	Suppressing evidence and information learned in UC operations in exchange for bribes/money "Ripoffs" of money and drugs from dealers during drug deals	Overt entrapment of suspected drug offenders Perjury and falsifying evidence and incriminating statements Planting drugs in drug raids

Drug trafficking in Chicago is a multi-million dollar operation and gang members are often more than willing to pay for protection. Police officers can make deals with one gang or drug dealer in order to catch another. This can be both good police work as well as a major temptation for corruption. For example, Joseph Miedzianowksi, although he conspired with multiple gangs to import and sell drugs “took the witness stand in his own defense and claimed that he had never betrayed his oath. He said his seeming friendships with members of the Imperial Gangsters and other street gangs were merely designed to coax out inside information.”¹³ However, Miedzianowksi’s arguments did not resonate with the jurors during his trial as he was convicted and sentenced to life in prison for his crimes.

Both Type 1 and Type 2 corruption cases exist in our database. In addition, the war on drugs produces what the London review of the literature calls the “almost impossible” nature of drug-related policing:

- * It is usually ‘secretive, duplicitous and quasi-legal;
- * The use of informants is widespread;
- * It is extremely difficult to regulate;
- * The ‘war on drugs’ rhetoric often increases pressure for results;

- * Securing sufficient evidence to convict is often difficult ;
- * Officers may be required to buy or, occasionally, use drugs in the course of their work; and
- * Very large sums of money may be available to the corrupt officer. Tim Newman summarizes the problem concisely:

Here, then, is possibly the major problem now faced by those seeking to control police corruption. Those areas of police work that have the strongest link with, or are closest to, the 'invitational edge' are also those which are generally subject to the least managerial scrutiny and, in the specific case of drugs, are increasingly associated with extraordinarily large sums of money and therefore very high levels of (financial) temptation.¹⁴

The Code of Silence

It is clear from previous research that supervision of drug and gang squad officers must have the highest priority. However, even honest police officers have difficulty reporting misconduct, and the lack of oversight on the police drug war is a major problem. Lou Rieter, a consultant to the Chicago Police and former Deputy Chief of Police in Los Angeles, testified that:

The Code of Silence exists to varying degrees in all police agencies in the United States. The failure of the Chicago Police Department to acknowledge its potential and take affirmative steps to eliminate or minimize the influence of the Code of Silence, in my opinion, is a conscious choice various Chicago Police managers and executive officers have taken and, in my opinion, represents a position of deliberate indifference by the Chicago Police Department to this disruptive issue within the agency.¹⁵

In the Joseph Miedzianowski prosecution, Brian Netols, Assistant U.S. Attorney testified that he believed that the Code of Silence was involved in all 18 criminal trials of Chicago police officers that he prosecuted a devastating indictment of CPD oversight, according to Reiter's affidavit,

"Netols testified that he believed the Chicago Police Department was in the RICO conspiracy with Miedzianowski and in the wiretaps of the case which he played in court officers stated that they 'were not concerned about investigations by the Internal Affairs Division.' When the search warrant was served on Miedzianowski's home there were 'thousands of documents were taken from his home...,' which appeared to be from Internal Affairs investigations . . ."¹⁶

In short, police officers do not fear being investigated by the Internal Affairs Department. Reiter concludes:

These deficiencies in the administrative investigations of complaints, employee discipline and the adverse impact of the Code of Silence, has been noted by, documented for and relied upon managers and administrators within the Chicago Police Department. The failure to modify this systemic deficiency in the process by successive Police Superintendents, in my opinion, is indicative of a conscious choice by the Police Department to continue this practice of indifference to allegations of misconduct and police abuse including Constitutional violations.¹⁷

The code of silence obviously played a role in the recent case of Officer Anthony Abbate beating up a female bartender.

It should be clear we do not ascribe to the “bad apple” theory of police misconduct. New York’s famous Knapp Report explains:

According to this theory, which bordered on official Department doctrine, any policeman found to be corrupt must promptly be denounced as a rotten apple in an otherwise clean barrel. It must never be admitted that his individual corruption may be symptomatic of underlying disease... A high command unwilling to acknowledge that the problem of corruption is extensive cannot very well argue that drastic changes are necessary to deal with the problem.¹⁸

Rather than focus on individual police or a wholesale indictment of CPD officers, most of whom are honest public servants, this report targets the “practice of indifference” in CPD leadership and the mayors’ offices in providing effective oversight.

Case Studies

The following cases highlight CPD corruption from the 1970s to the present day. Together, these cases, document the pervasive and persistent nature of corruption and the incapacity or unwillingness of the CPD to provide effective oversight. All of the cases are also subjects of controversy, including charges of entrapment, pious denunciations of “bad apples,” and a failure to seriously address systemic issues. Nonetheless, these cases illustrate the different types of police corruption and abuses and demonstrate the severity and breadth of the problem.

Case Study # 1 “Marquette 10”

The “Marquette 10” case is a prime example of police involved in Drugs, Guns and Gangs. In 1982, U.S. Attorney Dan Webb’s investigation into drug dealers in Chicago’s west side led to the arrest of 10 Marquette District officers for accepting bribes from drug dealers. The 10 officers were convicted for protecting two large drug-dealing networks in exchange for money and goods for more than three years. The officers warned the dealers of police raids and even beat up competing dealers, according to court records. The Marquette 10 officers were Thomas Ambrose, Frank DeRango, Curtis Lowery, John De Simone, Robert Eatman, Joseph Pena, James Ballauer, William Guide, William Hass and Dennis Smentek. They each received prison sentences ranging from 10 to 20 years.¹⁹

Case Study # 2 “Austin 7”

The “Austin 7” case highlights the need for greater police oversight. The seven were Austin District tactical police officers and plainclothes cops assigned to root out gangs and drugs on the West Side. They were indicted on December 20, 1996 by a federal grand jury for allegedly stealing and extorting \$65,000 from undercover FBI agents posing as Chicago drug dealers.

The seven officers indicted and tried were Edward Lee “Pacman” Jackson Jr.; Gregory S. Crittleton; Alex D. Ramos; M.L. Moore; Lennon Shields; James P. Young; and Cornelius Tripp. They were indicted on 21 different counts of extortion, illegal use of firearms and the conspiracy to commit robbery. The investigation of these officers was initiated after authorities received numerous complaints from neighborhood residents. After the officers were indicted, prosecutors had to drop more than 120 narcotics cases against suspects because of the involvement of at least one of these officers.

The “Austin 7” officers were prosecuted and convicted of racketeering for shaking down drug dealers for cash and cocaine, for providing protection for large narcotics deliveries and for robberies, home invasions and extortions of narcotics dealers in 1995 and 1996.²⁰

In addressing the issue of police oversight at the time of the convictions in May 1998, the Mayor’s Commission Report on Police Integrity urged that the CPD better monitor misconduct complaints from individuals and neighborhood groups if it hoped to avert similar patterns of abuse in the future.²¹

Case Study # 3 Miedzianowski

Joseph Miedzianowski, a decorated member of the Gang Crimes Unit, was convicted in 2001 of racketeering and drug conspiracy for running an interstate drug ring between Miami and Chicago, shaking down drug dealers, fixing criminal cases, hiding a wanted murderer and undermining his fellow police officers. In 2003 he was sentenced to life in prison.

Miedzianowski’s criminality continued for more than a decade and involved at least eight different gangs and dozens of gang members. Miedzianowski’s lengthy record of corruption raises questions about the capacity or will of the CPD or any of the oversight bodies to effectively supervise drug and gang related misconduct.²²

Case Study# 4 “SOS”

The brazen behavior of the Special Operations Section of the CPD was well known, and both state and federal authorities investigated the unit. Prompted by evidence that police bosses knew of a pattern of misconduct over at least four years, the U.S. Attorney's office took over the Cook County state's attorney's investigation of the elite Special Operations Section (SOS) in 2007, and began investigating the conduct of department bosses and the Internal Affairs Division.²³

In the previous year, 2006, the Cook County State's Attorney's Office indicted 10 members of the CPD's SOS for aggravated kidnapping, theft, burglary, home invasion, armed violence and false arrest. The officers indicted were: Jerome Finnigan, Keith Herrera, Carl Suchocki, Thomas Sherry, BartMaka, Brian Pratscher, Donovan Markiewicz, Guadalupe Salinas, Stephen DelBosque and Eric Olsen. These indictments were the result of a federal investigation of SOS by the US Attorney's office.²⁴ Charges against Officers Thomas Sherry and Carl

Suchocki were dropped in February 2009, because they could not be placed at the scene of the crime. Officers Stephen DelBosque and Eric Olsen pleaded guilty in April 2011 to conducting illegal searches and lying about it before a grand jury or in court. Officers Bart Maka, Brian Pratscher, and Guadalupe Salinas pleaded guilty to charges of felony theft, and Officer Donovan Markiewicz pleaded guilty to charges of official misconduct in September 2009.²⁵

Officer Keith Herrera told Katie Couric on “60 Minutes” that they “pulled over motorists without cause, grabbed their keys and stormed into their homes, falsified reports, pocketed huge sums of money and even shook each other down for money.” Herrera sought to place the blame on team leader Jerome Finnigan who pleaded guilty in April 2011 to conspiracy to commit murder for hire as he hired a former hit-man to kill former SOS member Herrera.²⁶

The charges allege that Finnigan’s share of the money stolen in 2004 and 2005 was approximately \$200,000, while Herrera allegedly netted approximately \$40,000 in 2005 – all of which came from a larger pool of approximately \$600,000 that allegedly was stolen in five separate episodes in 2004 and 2005. Finnigan was sentenced to 13 years in prison; Herrera is still awaiting sentencing, but could see up to 13 years in prison as well. Officers Bart Maka, Brian Pratscher, Guadalupe Salinas, and Donovan Markiewicz were sentenced to 6 months in jail, and Officers Stephen DelBosque and Eric Olsen pleaded guilty to lying on police reports.²⁷ Moreover, Finnegan named 19 other officers who took part in illegal activities, and said that commanding officers knew about the stealing and condoned civil rights violations. Finnegan said SOS officers’ criminality was an “open secret” and while many officers did not steal, they signed off on false reports.²⁸

Case Study # 5 Guerrero and Martinez

Police corruption related to drugs and gangs continues to surface in Chicago. In 2011, the U.S. Attorney’s office filed indictments against two Chicago police officers for helping a gang steal. The officers Alex Guerrero and Antonio Martinez Jr., were accused of taking orders from gang leaders and using their authority to pull people over or enter houses. The indictment alleges the officers received at least \$10,000 to steal guns, hundreds of pounds of drugs and tens of thousands of dollars. Martinez pleaded guilty in December 2011 to charges of conspiracy and racketeering, and Guerrero pleaded guilty to similar charges in July 2012.²⁹

Case Study # 6 Lewellen

The corruption case of Glen Lewellen highlights both the problems of paid informants and the lack of oversight in the CPD. Lewellen, oversaw a federal informant, Saul Rodriguez, from 1996 to 2001. During that time, Rodriguez was paid \$807,000 by the U.S. Attorney for information on drug dealing with his former gang, La Raza.³⁰

But behind the scenes, Lewellen had hatched a secret, unauthorized deal with Rodriguez, where the drug trafficker would keep breaking the law and the cop would help him, joining Rodriguez's drug organization — which prosecutors contended was behind multiple violent kidnappings and robberies.³¹

According to the indictment filed in November of 2010, Lewellen and Rodriguez founded the “Rodriguez Drug Trafficking Organization” in 1996. The Chicago cop and his paid informant allegedly worked together to rip off other drug dealers, splitting millions of dollars. In addition, Rodriguez was involved with three killings – in 2000, 2001 and 2002 - and Lewellen repeatedly invented excuses to keep his informant out of jail and benefit their drug trafficking organization. ³²

Even after Lewellen retired in 2002, he managed to obstruct a separate Drug Enforcement Administration investigation of Rodriguez, prosecutors said. Rodriguez testified that in 2006, Lewellen warned Rodriguez not to speak to a drug courier whose phone was wiretapped. Prosecutors pointed out that at the time, the DEA was investigating Rodriguez’s ties to a cocaine wholesaler.³³

The prosecutors’ case against the 55-year-old Lewellen included evidence of a 2004 rip-off of 70 kilograms of cocaine from a man who delivered the drugs in a tractor-trailer to Lewellen’s warehouse in south suburban Frankfort. Lewellen allegedly drove up in a fake squad car outfitted with police lights and the man ran away, allowing Lewellen and other crew members to steal the drugs.³⁴

Last year in February, a federal jury convicted Lewellen, a former narcotics officer, of joining Rodriguez's massive drug conspiracy.³⁵

Case Study # 7 Osbourn and Gibson

Since 1970, 36 officers have been convicted on civil rights violations in cases similar to the arrest of Felicia Tolson in 1998. Officer Kevin Osbourn and Sgt. Mark Gibson entered her West Side home when looking for a teenager who had earlier escaped arrest. They disregarded her requests for identification and Officer Osbourn arrested Tolson for aggravated battery after she allegedly pushed him.³⁶

Tolson, at the time a correctional officer at the Cook County Jail, was held in custody for 30 hours and was later acquitted of the aggravated battery charge. She stated that due to the incident she suffered post-traumatic stress and depression, along with humiliation, which lead her to quit her job as a correctional officer at Cook County Jail. In 2001, a federal jury found that the two officers falsely arrested Ms. Tolson and awarded her \$300,000 in damages.³⁷

Case Study # 8 Abbate

On 19 February 2007, off-duty Police Officer Anthony Abbate attacked and punched Karolina Obrycka while she was bartending at Jesse's Shortstop Inn, a bar on the Northwest side of Chicago. The incident was caught on a bar videotape on which Officer Abbate can be seen repeatedly punching and kicking the visibly smaller bartender. He later claimed it was self-defense. Officer Abbate was apparently under the influence of alcohol. He stated that the bartender pushed him first and that the fight started after she refused to serve him more drinks. Abbate was convicted in 2009 in state court of aggravated battery and sentenced to community service, anger management counseling and two years of probation.³⁸

On November 14, 2012, federal jury found both the City of Chicago and Abbate responsible and awarded the bartender, Karolina Obrycka, \$850,000 in damages.³⁹

The jury found that the police culture of impunity was "a moving force" in causing Abbate to attack Obrycka as she worked behind the bar. Abbate attacked Obrycka in part because he believed that, as a police officer, he wouldn't be punished, the jury found.⁴⁰

During the trial, Obrycka's lawyer had argued that police brass have denied for decades that a "code of silence" protecting policemen who commit crimes runs all the way from the street to the top of the police department. They also argued that Abbate acted with impunity. That he was unafraid of consequences was the result of the blue wall of silence as well as department's history of ineffective discipline action against wayward officers.⁴¹

Officers who responded to the bar the night of the attack failed to include Abbate's name, the fact that he was a police officer and that there was a video in their police report. This further solidified arguments supporting the existence of blue wall of silence.⁴²

Case Study # 9 & # 10 Doyle and Hanhardt

The cases of Officer Anthony Doyle and Chief of Detectives William Hanhardt hark back to an earlier time when The Outfit, Chicago's version of the organized crime syndicate or Mob, had its tentacles deep into the Chicago Police Department.

At the end of the federal "Family Secrets" trial in 2007, Doyle, was convicted of racketeering conspiracy for passing sensitive information to the Mob about a bloody glove left at the scene of the murder of mobster John Fecarotta in 1986.⁴³ Doyle was a police officer working in the Evidence Department in 1999 when he pulled up information on evidence that turned out to be a bloody glove.⁴⁴ Doyle was sentenced to 12 years in prison in 2009.⁴⁵

Hanhardt, the highest-ranking Chicago police official to be convicted of corruption, pleaded guilty in October 2001 to running a sophisticated jewelry theft ring that operated in several states and stole more than \$5 million in diamonds and other gems. Hanhardt, who had a 33-year police career, worked directly with Chicago organized crime syndicate from the early 1980s to 1998. Hanhardt used law enforcement computers and other databases to get information on traveling jewelry sales representatives.⁴⁶

History of CPD Oversight

"...police corruption cannot exist unless it is at least tolerated at higher levels in the Department."

Frank Serpico, Undercover New York Police Officer

The Chicago Police Department has a long history of failing to curb police abuse and corruption.

1960 - Summerdale Scandal; Police Board Created; Superintendent Hired,

News exposure of a crew of policemen engaged in burglary of legitimate businesses, which became known as the Summerdale Police Scandal, caused public to question the integrity of the Chicago Police Department. The loud criticism and calls for greater accountability led to the resignation of the Police Commissioner, Timothy O'Connor.

To help select a new police chief, Mayor Richard J. Daley created a commission, which included O.W. Wilson, a former police officer and then Dean of the University of California's criminology school. After a month-long search, the committee selected Wilson.

Wilson was hired, given the title of Police Superintendent and told to reform the department. Mayor Daley promised to keep political influence out of the department. He appointed

a five-member “nonpartisan Police Board, to govern the force.”⁴⁷ The Board was given power to oversee the new superintendent and to enforce the department’s rules. In essence, the board acted as the head of the department.

In 1961, the board’s rules were revised. Its authority “to administer or direct the operations of the police department and superintendent” was not included in the new system. Powers were restored to the superintendent. However, the Police Board acquired the power to hear officer disciplinary cases that were previously handled by the Chicago Civil Service Commission.

1966 - ACLU develops reform plan; Mayor creates Citizens Committee

In 1966, the ACLU presented the police department with a reform plan calling for the Chicago Bar Association to review citizen complaints against the police. In response O. W. Wilson asked Harold Smith, a past president of the Chicago Bar Association, evaluate the work of the Internal Investigation Division (IID). Smith concluded that there was no need for a review of complaints by a Chicago Bar Association committee.⁴⁸

In July of that year, Mayor Daley created a 23-member citizens’ committee to evaluate and study police-community relations and to recommend programs to improve these relations.⁴⁹ The committee concluded that there were no faults with the IID’s operations.⁵⁰

1967 - Superintendent reorganizes IID

In 1967, then Police Superintendent James Conlisk Jr., reorganized IID and combined it with the Inspections Division, the unit responsible for inspecting departmental operations. The new unit, the Internal Inspections Division was expected to detect corruption and not just wait for it to be reported by others.⁵¹ The reorganization of IID came soon after detective Jack Muller went to the Superintendent with information alleging tire theft. Muller said he did not go to the IID with this information due to the lack of action in previous reports he made with the IID.⁵²

1970 - Creation of the Internal Affairs Division (IAD)

A police raid on the Black Panthers’ headquarters in December 1969 resulted in the shooting deaths of two African-American men in their beds. There were newspaper exposures of false police reports, charges from the public that the police used excessive force, and allegations from some that the police murdered the victims. The ACLU renewed its call for civilian involvement in police oversight.⁵³

Superintendent Conlisk nixed the idea of including civilian employees in the IID, and based on a study by the International Association of Chiefs of Police, once again reorganized IID. In 1970, a new Internal Affairs Division (IAD) was created with the task of investigating allegations of police misconduct. A separate Inspections Division was created to execute the inspectional function.⁵⁴

1972 - Commission on Human Relations given a role

Due to increasing community dissatisfactions with how police oversight was handled, in 1972 the Mayor called a conference of civic leaders to discuss the problem of police-community relations. At the conference Superintendent Conlisk said the Chicago Commission of Human Relations would be assigned to review IAD files and if necessary re-investigate certain cases. This is the first time a civilian entity was given the opportunity to review and perform its own investigations of the Chicago Police Department. The Commission was not given direct disciplinary authority, only the power to recommend possible disciplinary actions.⁵⁵

1973 - Knoohuizen Report

In 1973, the Chicago Law Enforcement Study Group analyzed the Police Board and how it was performing its four main functions: 1) Budget adoption; 2) adoption of rules and regulations; 3) nominating superintendent candidates; and 4) police officer discipline. The report, authored by Ralph Knoohuizen found that the Board only effectively handled discipline and that its other duties were mostly for show.⁵⁶

1974 - The Office of Professional Standards created

In 1974 Superintendent James Rochford created the Office of Professional Standards (OPS) again combining investigative and inspectional functions in a single agency. OPS did not have subpoena power, did not hold public hearings, and was not asked to make policy recommendations.⁵⁷

Superintendent Rochford proposed that the handling of police misconduct cases be placed directly under his command, and that OPS hire civilian investigators.⁵⁸ However, the investigators could be ex-police officers as long as they were not from CPD. OPS relied on the police department to notify them when they received complaints. OPS and CPD homicide

detectives collaborated on shooting investigations. Critics claimed that OPS often adopted the homicide detectives' investigative findings as their own.⁵⁹

OPS failed for two decades to bring charges against Jon Burge, although multiple victims and civil rights groups had demanded action.

1992 – Five year statute is implemented

In response to complaints about the charges against Burge, in 1992, the State Legislature passed a five-year statute of limitations for administrative proceedings.⁶⁰

2006 - Futterman documents “Chicago Police Department’s Broken System”

Craig B. Futterman, a professor at the University of Chicago Law School and two colleagues, published a report in 2006 analyzing 10,149 complaints of excessive force, illegal searches, racial abuse, sexual abuse and false arrest filed by civilians between 2002 and 2004. Futterman and his team found that:

- only 19 of the 10,149 complaints led to a suspension of a week or more
- the chance of meaningful discipline for a police brutality complaint was less than 3 in a thousand
- only 1 of 3,837 charges of illegal searches led to meaningful discipline
- over a three-year period, not a single charge of false arrest - planting of drugs, guns, etc.- led to an incident of meaningful discipline.

2007 - Independent Police Review Authority created

Mayor Richard M. Daley in 2007 responded complaints about police misconduct and how the Police Department handled them. He created the Independent Police Review Authority (IPRA) to replace OPS. The IPRA was assigned to investigate allegations against police officers, including excessive force, domestic violence, coercion, and biased-based verbal abuse. It also was given the responsibility to investigate discharges of firearms and Tasers, and extraordinary occurrences involving individuals in police custody, regardless of the existence of a complaint. IPRA was also given the intake responsibility for all complaints, from within the department and from community members.⁶¹

2009 - Value of the Police Board doubted by the Chicago Justice Project

The Chicago Justice Project studied Police Board decision in 310 cases in which the Superintendent sought termination of either sworn officers or civilian employees over a 10-year period from 1999 through 2008. The study was authored by Tracy Siska, the project's executive director, and by research assistant Sherie Arriazola. They found that the Police Board upheld the recommended discipline of the Superintendent in agreement with IAD or IPRA in only 37 percent of the cases of sworn officers. They also found that in 20 percent of the cases involving sworn officers, the policemen were returned to work without any discipline at all.

The authors questioned why police discipline is still the responsibility of the Police Board. "Looking at the numbers generated in our study," they said, "it is hard to see how the board serves the public interest by retaining two thirds of the officers the Superintendent is trying to fire."⁶²

2013 - Police Board still struggling

Today there are still major concerns of accountability and transparency for the Police Board. It still has problems of transparency and difficulty earning a reputation as a fair and just decision maker.⁶³ However, even if the Police Board were effective, efficient, transparent, and accountable, it only addresses one aspect of police oversight, the individual officer. Though this is important and necessary, there is more to police oversight than the specific behavior of an individual officer. Every aspect that influences an officer needs to be addressed, from training to advancement to discipline.

Discussion of Reform Approaches

Ignacio Cano, who researched ways to fight police corruption in Brazil and South Africa, recommends both External Review and Internal Incentives.⁶⁴ He proposed that:

1. Internal affairs units must report to bodies outside the bureaucratic hierarchy of the police.
2. Officers who report misconduct need substantial financial and professional rewards and strict protection from retaliation within the department.
3. The process of making complaints within the department must be strictly confidential.
4. Internal reviews need to be complemented by external bodies with power of subpoena and a process to turn complaints into prosecution.

In South Africa their anti-corruption report stressed three major themes for policing:

1. Enhancing internal accountability by establishing effective systems to receive and deal with public complaints, through dedicated internal capacity to investigate allegations of police abuse and criminality, and improve the management of discipline throughout the organization.

2. Promoting organizational integrity by fostering a culture that adheres to the South African Police Service Code of Conduct and Code of Ethics, that respect the Constitution and that puts service to the people first.

3. Mobilizing community support by encouraging communities to promote professional, honest, corruption-free policing by recognizing and supporting good police conduct and reporting all incidences of poor service or police criminality.⁶⁵

We have incorporated these international experiences in dealing with police corruption in making our recommendations for reform of the Chicago police department.

Summary of the Chicago Problem

The problem of police corruption in Chicago is not simply that there are occasional flawed police officers. Nearly all officers join the police force because they desire to serve and protect not serve and collect. By far, most officers are law-abiding, dedicated public servants.

The real problem is that an embarrassingly large number police officers violate citizens' rights, engage in corruption and commit crimes while escaping detection and avoiding discipline or prosecution for many years. The "code of silence" and "deliberate indifference" have prevented police supervisors and civilian authorities from effectively eliminating police corruption.

Today, the major source of police corruption is the war on drugs. While the public has many different ideas on the solution to the drug issue, the strong demand for drugs means that many people will risk the dangers of trafficking. Violence will continue as a way to settle disputes. The large amounts of money involved mean that police corruption will remain endemic as long as current policies continue.

Police superintendents and mayors typically denounce each new case as another "bad apple," and have failed to establish meaningful internal reforms or effective oversight. Fraternal Order of Police leadership and members of the City Council have repeatedly opposed establishing a powerful independent Police Review Board.

Recommendations for Chicago

Internal Leadership, Reforms and Incentives

1. The Police Superintendent must take the lead in promoting professional behavior through out the police force. He should make curbing police corruption a priority and create rules and procedures that punish corruption and reward integrity.
2. The Police Board should provide greater transparency by explaining its decisions in plain English on its web site. Currently the decisions are on the web site but they are often expressed in legal language that can be difficult for the average person to comprehend. The full legal findings should also be posted on the web site.
3. Independent Police Review Authority should report on the status of its investigations and Bureau of International Affairs should report the cases referred to the state's attorney for prosecution.
4. The Police Department should provide special recognition, accommodations and promotions, to officers for providing information leading to the successful prosecution of police officer corruption. "Meritorious Promotion" currently used within the department should include promotions for officers who report criminal conduct of police officers. Officers who choose to serve in the Bureau of Internal Affairs will be prioritized for promotion and will not be compelled to return to their old units after their service in BIA is complete.
5. CPD must punish officers who do not report police corruption, brutality, and other misconduct they observe. The Police Code of Ethics and Department Rules should be strengthened to require that officers must promptly report any crime or unlawful action committed by a fellow police officer. Article Five, Rule 21 of the Rules and Regulations of the Chicago Police Department should be amended to read: "Failure to report promptly to the Department any information *including violations of the law by police officers.*"
6. The Department should require and provide more extensive ethics training for officers. Training in issues of accountability for sergeants and front-line supervisors should be increased. This training needs to teach sergeants how to quickly recognize ethical problems of officers, particularly in the war on drugs, how to advise them, and how to hold them accountable.

External Review and Oversight

1. The Mayor and City Council should enact legislation to replace the current appointed Police Board with either:
 - A. a democratically elected civilian Police Board, or

B. a new appointed board with such high caliber members as good-government advocates and civil right leaders, former federal prosecutors, inspector generals, or respected former public defenders or eminent retired judges.

In either case, the new board's purview must not be limited to cases referred by the Superintendent or IPRA and appeals from individual officers. It also should have the power hire special inspectors to conduct investigations. And, it must be empowered to refer cases to the State's Attorney and U.S. Attorney.

A call for a democratically elected police board is supported by groups such as the Chicago Alliance Against Racist and Political Repression. (See Appendix VI.)

2. The Cook County State's Attorney must allocate sufficient resources for its public integrity unit to improve its prosecution of police corruption. The State's Attorney should issue an annual report on its efforts to curb police corruption and establish better procedures to encourage residents to confidentially report criminal police misconduct.

3. The Mayor and City Hall should report to the public the cost of police corruption and make information about police corruption cases easy to access. It should report the cost of investigating, defending and settling police corruption cases in its annual city budget and make it available on the city's web site along with a searchable database with all indictments and convictions of police officers.

Appendix I, Database of Convicted Chicago Police Officers, 1960 - 2012

Year	First Name	Last Name	Title/ Position	Event	Code	Notes	Citations
2011	Anthony	Abbate	Police Officer	Convicted	ODC	Found guilty of aggravated battery related to punching and kicking a female bartender	Chicago Tribune, May 25, 2011
1999	Manuel	Acevado	Police Officer	Convicted	BTX	Found guilty of causing paralyzing injury, excessive force, and failure to provide medical care	Chicago Tribune, Oct 26, 1999
2006	Michael	Acosta	Commander	Convicted	GPC	Pleaded guilty to one count of fraud for stealing \$4000 from police award fund.	Chicago Tribune, Jan 18, 2006
2007	Michael	Allegretti	Police Officer	Convicted	BTX	Pleaded guilty to attempted intimidation charges. He asked women whom he pulled over to expose their breasts to avoid traffic tickets	Chicago Sun Times, Sep 7, 2007
1982	Thomas	Ambrose	Police Officer	Convicted	DGG	Found guilty of accepting bribes to allow two heroin rings to operate in the Marquette District	Chicago Tribune Jul 1, 1982
1986	Ramon	Anderson	Sergeant	Convicted	GPC	Pleaded guilty to bribery related to shaking down a tavern owner	Chicago Tribune, July 17, 1986
1987	John	Antonucci	Police Officer	Convicted	GPC	Pleaded guilty to two counts of making false statements	Chicago Tribune, March 24, 1987
1973	Daniel H.	Armstrong	Police Officer	Convicted	GPC	Found guilty of conspiracy and perjury related to shakedown of tavern owners	Chicago Tribune, Oct 6, 1973
2005	Rafael	Balbontin	Police Officer	Convicted	ODC	Found guilty of stabbing his wife to death with a knife while off duty	Chicago Tribune, Oct 6, 2007
2002	Sydney	Barber	Police Officer	Convicted	ODC	Found guilty of first-degree murder while off duty	Chicago Tribune, Sep 26, 2002
1973	Edward J.	Barry	Sergeant	Convicted	GPC	Found guilty of conspiracy related to shakedown of tavern owners	Chicago Tribune, Oct 6, 1973
1973	Thomas D.	Batastini	Police Officer	Convicted	GPC	Found guilty of conspiracy and perjury related to shakedown of tavern owners	Chicago Tribune, Oct 6, 1973
2003	Turan	Beamon	Police Officer	Convicted	DGG	Pleaded guilty to charges that he stole cash and narcotics from a drug dealer	Chicago Tribune, Nov 23, 2003

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 25 of 54

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338

1992	William F	Beck	Police Officer	Convicted	GPC	Pleaded guilty to two counts of income tax fraud related to extorting bribes from truck drivers	Chicago Tribune, April 2, 1992
1997	Gregory	Becker	Police Officer	Convicted	ODC	Found guilty of shooting a homeless man, and leaving him on the street to die	Chicago Tribune, May 12, 1997
1961	Peter	Beeftink	Police Officer	Convicted	GPC	Found guilty of conspiracy to commit burglary and conspiracy to receive stolen property while in uniform and on duty	Chicago Tribune, Aug 24, 1961
1986	Timothy	Belec	Police Officer	Convicted	BTX	Pleaded guilty to aggravated battery and one count of official misconduct for beating a man arrested for loitering	Chicago Tribune, Oct 9, 1986
2003	James	Benson	Police Officer	Convicted	DGG	Pleaded guilty to drug conspiracy and narcotics smuggling	Chicago Tribune, Feb 1, 2003
2009	Christopher	Berlanga	Police Officer	Convicted	ODC	Pleaded guilty to charges of causing death while operating a vehicle while intoxicated	Post Tribune, August 13, 2009
2007	Eural	Black	Police Officer	Convicted	DGG	Found guilty of racketeering and conspiracy related to drug sales committed while armed with a gun	Chicago Tribune, May 12, 2007
1989	Phillip	Blackman	Police Officer	Convicted	DGG	Found guilty of charges related to taking bribes to protect the activities of South Side gamblers and a drug dealer	Chicago Tribune, July 12, 1990
1984	Ira	Blackwood	Police Officer	Convicted	GPC	Found guilty on one count racketeering/bribery and 10 counts of extortion.	Chicago Tribune, Aug 11, 1984
2009	Richard	Bolling	Police Officer	Convicted	ODC	Found guilty of reckless homicide, drunk driving and leaving the scene of the accident that killed a youth	Chicago Tribune, January 12, 2012
1995	Roland	Borelli	Police Officer	Convicted	GPC	Pleaded guilty to 1 count extortion and 2 counts of filing false tax returns	Chicago Tribune, May 10, 1995
1974	Joseph	Bouse	Police Officer	Convicted	GPC	Found guilty of attempted bribery and official misconduct	Chicago Tribune, Sep 10, 1974

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338

PAGE 27 of 34	1973	Clarence	Braasch	Captain	Convicted	GPC	Pleaded guilty to two counts of tax fraud.	Chicago Tribune, Oct 6, 1973
	2002	Corey	Braddock	Police Officer	Convicted	ODC	Found guilty of solicitation of a sex act	People v. Braddock, Case No.1-03-0404, March 24, 2004
	1992	Anthony	Brandys	Police Officer	Convicted	GPC	Pleaded guilty to two counts of tax fraud	Chicago Tribune, March 16, 1992
	1961	Allan	Brinn	Police Officer	Convicted	GPC	Found guilty of conspiracy to commit burglary and conspiracy to receive stolen property	Chicago Tribune, Aug 24, 1961
	1992	Kenneth	Brown	Police Officer	Convicted	GPC	Pleaded guilty to a charge of official misconduct	Chicago Tribune, July 1, 1992
	2011	Victor	Brown	Police Officer	Convicted	GPC	Pleaded guilty to extortion stemming from charges that he accepted \$4500 bribe money from other officers to fix Police Board cases	Chicago Tribune, May 10, 2010
	1988	Philip	Bruno	Detective	Convicted	GPC	Pleaded guilty to accepting bribes from vending machine operators	Chicago Tribune, Oct 1, 1988
	1967	Raymond	Burford	Police Officer	Convicted	ODC	Pleaded guilty to voluntary manslaughter in the shooting of a police informant	Chicago Tribune, June 14, 1967
	2010	Jon	Burge	Lieutenant	Convicted	GPC	Found guilty of perjury and obstruction of justice related to torture of witnesses into giving confessions in the 1970s and 1980s	Chicago Tribune, Dec 29, 2010
	1992	Robert A	Burke	Police Officer	Convicted	GPC	Found guilty of lying to a grand jury when he denied giving a handcuff key to an inmate who killed two officers during an escape attempt	Chicago Tribune, Feb 1, 2003
	2004	Willie C.	Caldwell	Police Officer	Convicted	GPC	Pleaded guilty to attempted extortion for demanding a payoff to return an impounded vehicle to a citizen	Chicago Tribune, Dec 21, 2004
	1973	Natale R.	Cale	Police Officer	Convicted	GPC	Found guilty of conspiracy related to shakedown of tavern owners	Chicago Tribune, Oct 6, 1973
	2010	Gerald	Callahan	Police Officer	Convicted	ODC	Found guilty of battery for punching a 61-year-old man and a 50-year-old while he was off duty.	Chicago Tribune, Feb 12, 2010
	2008	Scott	Campbell	Police Officer	Convicted	ODC	Pleaded guilty to income tax evasion and mail fraud charges stemming from towing scam	Chicago Tribune, April 22, 2009

PAGE 28 of 34	1985	Thomas	Capparelli	Police Officer	Convicted	GPC	Pleaded guilty to accepting bribes to sidetrack investigations of motorists involved in hit-and-run accidents	Chicago Tribune, May 30, 1985
	2006	Kevin	Carey	Police Officer	Convicted	ODC	Pleaded guilty to the DUI charge related to a road rage while off duty	Chicago Sun-Times, Jan 23, 2012
	1989	John	Carpenter	Police Officer	Convicted	DGG	Found guilty of charges related to taking bribes to protect the activities of gamblers and a drug dealer	Chicago Tribune, July 12, 1990
	2004	Rodney	Carriger	Police Officer	Convicted	CRV	Found guilty of home invasion and aggravated unlawful restraint and multiple counts of armed violence, bribery and official misconduct	Chicago Tribune, Sep 15, 2004
	2006	Jason	Casper	Police Officer	Convicted	ODC	Pleaded guilty to charges stemming from reckless homicide and aggravated drunken driving	Chicago Tribune, Jan 18, 2008
	2002	Xavier	Castro	Police Officer	Convicted	DGG	Found guilty of illegally entering the homes of suspected drug dealers and lying under oath to conceal improper searches	Chicago Tribune, July 12, 2002
	1973	John	Catalano	Police Officer	Convicted	GPC	Found guilty of conspiracy related to shakedown of tavern owners	Chicago Tribune, Oct 6, 1973
	2003	Alonzo	Caudillo	Police Officer	Convicted	ODC	Found guilty in the death of a 19 year old female whom he hit and killed while driving his Jeep	Chicago Tribune, Feb 8, 2005
	1992	Gregory	Chambers	Police Officer	Convicted	ODC	Found guilty of shooting and killing his girlfriend while off duty	Chicago Tribune, Nov 15, 1992
	1985	Anthony	Chiavola Sr.	Police Officer	Convicted	ODC	Pleaded guilty to conspiring to carry money skimmed from the gambling receipts	Chicago Tribune, July 30, 1985
	1982	Anthony	Chiavolo Jr.	Police Officer	Convicted	ODC	Pleaded guilty to serving as courier who delivered the skimmed cash from Las Vegas casino to various mob bosses	Chicago Tribune, June 23, 1982
	2009	Michael J	Ciancio	Police Officer	Convicted	GPC	Pleaded guilty to extortion related to soliciting bribes from tow truck drivers	Chicago Sun Times, Feb 12, 2011

ELECTRONICALLY FILED
 7/2/2015 12:12 PM
 2014-CH-15338
 PAGE 29 of 34

1961	Allen	Clements	Police Officer	Convicted	GPC	Found guilty of conspiracy to commit burglary and conspiracy to receive stolen property while in uniform and on duty	Chicago Tribune, Aug 24, 1961
2009	William	Cozzi	Police Officer	Convicted	BTX	Pleaded guilty that he used excessive force related to beating a man who was handcuffed and shackled in a wheelchair	Chicago Sun Times, June 20, 2009
2002	Matthew	Craig	Police Officer	Convicted	CRV	Pleaded guilty to violating a defendant's civil rights by lying about evidence against arrested people	Chicago Sun Times, April 13, 2002
2001	Gregory S.	Crittleton	Police Officer	Convicted	DGG	Pleaded guilty to racketeering and weapons charges related to robbing money from gang members	Chicago Sun Times Oct 19, 2001
1990	Kenneth	Cullen	Police Officer	Convicted	ODC	Found guilty of fatally shooting a man after a traffic altercation while off-duty	Chicago Tribune, March 24, 1995
2012	Sean	Dailey	Police Officer	Convicted	GPC	Pleaded guilty to DUI when his blood alcohol content registered .14	Chicago Sun Times, Feb 29, 2012
1972	Timothy	Danaher	Sergeant	Convicted	GPC	Pleaded guilty to extorting money from taverns and a south side pharmacy	Chicago Tribune July 27, 1972
2007	Aaron	Del Valle	Police Officer	Convicted	GPC	Found guilty of lying to a grand jury in case of patronage hiring at city hall	Chicago Tribune, March 29, 2007
1985	Michael	Delany	Police Officer	Convicted	GPC	Pleaded guilty to committing burglaries while on duty	Chicago Tribune, May 3, 1985
2011	Stephen	DelBosque	Police Officer	Convicted	DGG	Plead guilty to conducting illegal searches and lying about it, in court or before a grand jury	CBS Chicago, April 7, 2011
1972	George	DeMet	Sergeant	Convicted	GPC	Found guilty of extorting money and liquor from tavern operators	Chicago Tribune, Jun 21, 1972
1982	Frank T.	Derango	Police Officer	Convicted	DGG	Found guilty of accepting bribes to allow two heroin rings to operate in the Marquette District.	Chicago Tribune, July 1, 1982
1982	John F.	DeSimone	Police Officer	Convicted	DGG	Found guilty of accepting bribes to allow two heroin rings to operate in the Marquette District.	Chicago Tribune Jul 1, 1982

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338

PAGE 30 of 34	1973	Robert	Devitt	Lieutenant	Convicted	GPC	Found guilty of perjury related to receiving bribes from tavern owners	Chicago Tribune, May 5, 1973
	1995	William	Devoney	Lieutenant	Convicted	ODC	Pleaded guilty to insurance fraud	Chicago Tribune, June 7, 1995
	2008	Richard	Doroniuk	Police Officer	Convicted	DGG	Pleaded guilty to racketeering, admitting he robbed drug dealers of cash , planted drugs on people he arrested and used fake informants to secure search warrants	Chicago Tribune, June 4, 2008
	2003	Anthony	Downing	Police Officer	Convicted	BTX	Found guilty of official misconduct and bribery for engaging in a sex act with a young prostitute	Chicago Tribune, Feb 22, 2003
	2009	Anthony	Doyle	Police Officer	Convicted	GPC	Found guilty of racketeering conspiracy related to passing on confidential information about the federal probe to a mob friend	Chicago Tribune, March 12, 2009
	1972	Brian	Duffy	Police Officer	Convicted	GPC	Pleaded guilty to perjury related to ambulance chasing scheme	Chicago Tribune, Oct 21, 1972
	1964	Thomas	Durso	Police Officer	Convicted	ODC	Found guilty of shooting and killing handcuffed police informant	Chicago Tribune, Oct 30, 1974
	2002	Daniel	Durst	Police Officer	Convicted	BTX	Found guilty of excessive force and failure to stop beating	Chicago Tribune, Oct 23, 2002
	1993	James E.	Dvorak	Detective	Convicted	GPC	Pleaded guilty to bribery and income tax charges	Chicago Sun-Times, Aug 31, 1993
	1979	Patrick A.	Dwyer	Police Officer	Convicted	ODC	Found guilty of attempted robbery of a grocery store	Chicago Tribune, Jul 10, 1979
	1981	Fred	Earullo	Police Officer	Convicted	BTX	Found guilty of fatally beating up a mental patient after he was arrested and in custody. Suspect that was beaten by the officer had massive brain swelling, two broken legs, broken neck and nine broken ribs after his arrest	Chicago Tribune, Jan 26, 1984
	1982	Robert L.	Eatman	Police Officer	Convicted	DGG	Found guilty of accepting bribes to allow two heroin rings to operate in the Marquette District	Chicago Tribune Jul 1, 1982

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 31 OF 34

1989	Elbert	Elfreeze	Police Officer	Convicted	DGG	Pleaded guilty to charges related to taking bribes to protect the activities of gamblers and a drug dealer	Chicago Tribune, Jan 10, 1990
1973	Martin D.	Eshoo	Police Officer	Convicted	GPC	Found guilty of conspiracy and perjury related to shakedown of tavern owners	Chicago Tribune, Oct 6, 1973
1961	Frank	Faraci	Police Officer	Convicted	GPC	Found guilty of conspiracy to commit burglary and conspiracy to receive stolen property while in uniform and on duty	Chicago Tribune, Aug 24, 1961
1973	Edward F.	Finn	Police Officer	Convicted	GPC	Found guilty of conspiracy related to shakedown of tavern owners	Chicago Tribune, Oct 6, 1973
2011	Jerome	Finnegan	Police Officer	Convicted	DGG	Pleaded guilty to the murder-for-hire charge, robbery and a tax-evasion charge related to stealing of cash from drug dealers	Chicago Tribune, May 5, 2012
2006	Corey	Flagg	Police Officer	Convicted	DGG	Pleaded guilty to racketeering for shaking down drug dealers for cash and cocaine and providing protection for large narcotics deliveries	Chicago Tribune, May 9, 2007
1973	Carl	Flagg	Sergeant	Convicted	GPC	Found guilty of conspiracy and perjury related to shakedown of tavern owners	Chicago Tribune, Oct 6, 1973
1998	Tyrone	Francies	Police Officer	Convicted	DGG	Found guilty of robbing undercover agents posing as drug dealers	Chicago Sun Times, June 9, 1998
2012	Joseph	Frugoli	Police Officer	Convicted	ODC	Pleaded guilty to aggravated driving under the influence for crashing into a car and killing two men	Chicago Tribune, Nov 16, 2012
1992	Michael	Gallagher	Police Officer	Convicted	ODC	Found guilty of weapons charges related to illegal possession of silencer	Chicago Tribune, Dec 17, 1992
2002	John	Galligan	Police Officer	Convicted	DGG	Pleaded guilty to extortion, the theft of 2.2 pounds of cocaine from a drug dealer and supplying 3 grams of cocaine to a police informant	Chicago Sun Times Feb 27, 2003
1989	Victor	Garcia	Police Officer	Convicted	GPC	Pleaded guilty to burglarizing a residency of a retired police officer	Chicago Tribune, April 6, 1989

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 32 of 34

1982	Jerome	Garrison	Police Officer	Convicted	ODC	Found guilty of possession of a stolen motor vehicle with an altered vehicle identification numbers	Chicago Tribune, Jan 1, 1982
1973	John M.	Geraghty	Sergeant	Convicted	GPC	Found guilty of conspiracy and perjury related to shakedown of tavern owners	Chicago Tribune, Oct 6, 1973
1999	Aaron	Gibson	Police Officer	Convicted	ODC	Pleaded guilty to identity theft. He used other officer's identity to fraudulently obtain instant credit and make illegal purchases in the amount of \$20,000	Chicago Tribune, July 22, 1999
1989	James	Ginani	Police Officer	Convicted	GPC	Pleaded guilty to extorting bribes from trucking companies to overlook trucks exceeding weight limits	Chicago Tribune, April 2, 1992
2002	Robert	Gloeckler	Police Officer	Convicted	CRV	Pleaded guilty to a misdemeanor civil-rights violation related to lying under oath while testifying in court	Chicago Tribune, March 5, 2002
1985	Willie	Grady	Police Officer	Convicted	DGG	Found guilty of conspiracy, three counts of distribution of cocaine and one count of distribution of heroin	Chicago Tribune, Sep 6, 1985
1985	Ralph G.	Graham	Police Officer	Convicted	ODC	Found guilty of mail fraud for receiving about \$15,000 in checks fraudulently issued, participated in a scheme to receive illicit Blue Cross/Blue Shield insurance benefits	Chicago Tribune, Feb 1, 1985
1973	Philip R.	Grana	Police Officer	Convicted	GPC	Found guilty of conspiracy and perjury related to shakedown of tavern owners	Chicago Tribune, Oct 6, 1973
1985	Ronald J.	Green	Police Officer	Convicted	GPC	Found guilty of accepting bribes to sidetrack investigations of hit-and-run accidents	Chicago Tribune, June 6, 1985
2009	Joseph	Grillo	Police Officer	Convicted	ODC	Pleaded guilty to income tax evasion and mail fraud charges stemming from towing scam	Chicago Tribune, March 04, 2009
1961	Patrick	Groark	Police Officer	Convicted	GPC	Found guilty of conspiracy to commit burglary and conspiracy to receive stolen property	Chicago Tribune, Aug 25, 1961

ELECTRONICALLY FILED
7/2/2015 12:12 PM
PAGE 33 of 34
2014-CH-15338

2011	Alex	Guerrero	Police Officer	Convicted	DGG	Pleaded guilty to racketeering, related to using his law enforcement status to commit armed robberies of drug traffickers for the Latin Kings	Chicago Tribune, Dec 02, 2011
2006	Richard	Guerrero	Lieutenant	Convicted	GPC	Found guilty of misdemeanor telephone harassment for taking a phone number of a police report and harassing a woman	Chicago Sun Times, March 1, 2006
1982	William A.	Guide	Police Officer	Convicted	DGG	Found guilty of accepting bribes to allow two heroin rings to operate in the Marquette District	New York Times Jan 18, 1983
1989	Everett	Gully	Sergeant	Convicted	DGG	Found guilty of charges related to taking bribes to protect the activities of South Side gamblers and a drug dealer	Chicago Tribune, July 12, 1990
2007	Larry	Guy Jr.	Police Officer	Convicted	BTX	Pleaded guilty to misdemeanor battery related to beating a handcuffed shoplifting suspect	Chicago Tribune, Jan 24, 2009
1997	Timothy	Hampton	Police Officer	Convicted	DGG	Found guilty of cocaine possession, armed violence and official misconduct late	Chicago Tribune, Dec 06, 1997
1992	Paul	Hardin	Police Officer	Convicted	GPC	Found guilty of aggravated assault, official misconduct and theft	Chicago Tribune, July 1, 1992
2005	Larry	Hargrove	Sergeant	Convicted	DGG	Found guilty of shaking down drug dealers for cash and narcotics over a period of six years	Chicago Tribune, June 23, 2005
1982	William L.	Hass	Police Officer	Convicted	DGG	Found guilty of accepting bribes to allow two heroin rings to operate in the Marquette District	Chicago Tribune Jul 1, 1982
1995	David	Hayes	Police Officer	Convicted	ODC	Pleaded guilty to leaving the scene of an accident after he crashed a car into another car	Chicago Tribune, March 7, 2008
2005	Darek	Haynes	Police Officer	Convicted	DGG	Pleaded guilty to racketeering for shaking down drug dealers for cash and cocaine and providing protection for large narcotics deliveries	Chicago Tribune, May 12, 2007
1986	James	Hegarty	Police Officer	Convicted	GPC	Pleaded guilty to 1 count of tax fraud	Chicago Sun Times, March 1, 1986
2008	John	Herman	Police Officer	Convicted	BTX	Found guilty of aggravated criminal sexual assault, aggravated kidnapping and misconduct	Chicago Tribune Dec 04, 2007
2011	Marcos	Hernandez	Police Officer	Convicted	GPC	Pleaded guilty to improperly accessing motorists' information and pocketing payoffs from tow truck operators	Chicago Tribune, Aug 16, 2011

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338

2011	Keith	Herrera	Police Officer	Convicted	DGG	Pleaded guilty to civil rights and tax-related charges and admitted he stole cash from suspected drug dealers and other citizens after making illegal traffic stops or home searches	Chicago Tribune, May 5, 2012
1998	Eric	Holder	Police Officer	Convicted	ODC	Found guilty of resisting arrest following a fight while Holder was off duty at the time	Chicago Tribune, March 7, 1998
2009	Margaret	Hopkins	Police Officer	Convicted	DGG	Pleaded guilty to official misconduct related to falsifying a police report after her colleagues illegally searched drug dealers and others for drugs	Chicago Sun-Times, Sep 23, 2009
2012	Edward	Howard Jr.	Sergeant	Convicted	BTX	Found guilty of felony aggravated battery and official misconduct charges for slapping a handcuffed teen in an unprovoked attack	Chicago Tribune, July 20, 2012
1999	Rayshawn	Hudgins	Police Officer	Convicted	BTX	Found guilty of aggravated kidnapping, unlawful restraint related to rape and sexual abuse of teen boys	Chicago Tribune, Jan 15, 1999
2004	Ernest	Hutchinson	Police Officer	Convicted	CRV	Found guilty of home invasion and aggravated unlawful restraint and multiple counts of armed violence, bribery and official misconduct	Chicago Tribune, Sep 15, 2004
1996	Sonia	Irwin	Police Officer	Convicted	DGG	Found guilty of aiding and abetting the Gangster Disciples street gang	Chicago Tribune, Feb 15, 1996
2001	Edward Lee	Jackson Jr	Police Officer	Convicted	DGG	Found guilty of racketeering for shaking down drug dealers for cash and cocaine and providing protection for large narcotics deliveries	Chicago Sun-Times Oct 19, 2001
2002	Eugene	Jennings	Police Officer	Convicted	GPC	Pleaded guilty to bribery, solicitation of sex and official misconduct	Chicago Sun Times, Sep 25, 2002
2005	Erik	Johnson	Police Officer	Convicted	DGG	Pleaded guilty to conspiracy charges related to shaking down drug dealers for cash and cocaine and providing protection for large narcotics deliveries	Chicago Tribune, May 12, 2007

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 33 of 34

1970	Walter	Johnson	Police Officer	Convicted	GPC	Pleaded guilty to theft in the amount of \$3,000	Chicago Tribune, July 8, 1970
2005	Broderick	Jones	Police Officer	Convicted	DGG	Pleaded guilty to racketeering for shaking down drug dealers for cash and cocaine and providing protection for large narcotics deliveries	Chicago Tribune, Jan 28, 2005
1979	Wilton	Jones	Police Officer	Convicted	DGG	Found guilty of conspiracy related to Chicago based heroin distribution ring	Chicago Tribune, March 9, 1979
1971	John J.	Jordan	Police Officer	Convicted	GPC	Found guilty of bribery charges stemming from payoffs the officer took from ambulance drivers for calling them to the accident	Chicago Tribune, April 20, 1971
1961	Alex	Karras	Police Officer	Convicted	GPC	Found guilty of conspiracy to commit burglary and conspiracy to receive stolen property while in uniform and on duty	Chicago Tribune, Aug 24, 1961
1961	Sol	Karras	Police Officer	Convicted	GPC	Found guilty of conspiracy to commit burglary and conspiracy to receive stolen property while in uniform and on duty	Chicago Tribune, Aug 24, 1961
1971	Edward J.	Kavale	Police Officer	Convicted	ODC	Found guilty of reckless conduct related to shooting a 19- year old youth while off duty	Chicago Tribune, May 13, 1971
2010	John	Killackey	Police Officer	Convicted	ODC	Found guilty of stiffing a cabdriver of an \$8 fare and then threatening him at gunpoint	Chicago Tribune, May 28, 2010
1975	Thomas	King	Police Officer	Convicted	GPC	Pleaded guilty to bribery and official misconduct	Chicago Tribune, Oct 15, 1975
2010	Richard	Kleinpass	Police Officer	Convicted	ODC	Pleaded guilty to violation of owner's duties in animal neglect case	Chicago Sun-Times, May 22, 2010
1981	Louis	Klisz	Police Officer	Convicted	BTX	Found guilty of fatally beating up a mental patient after he was arrested and in custody. Suspect that was beaten by the officer had massive brain swelling, two broken legs, broken neck and nine broken ribs after his arrest	Chicago Tribune, Jan 26, 1984
1963	Gregory	Kouvelis	Police Officer	Convicted	ODC	Pleaded guilty to auto theft	Chicago Tribune, Feb 26, 1963

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 36 of 34

2005	John	Krass	Police Officer	Convicted	ODC	Found guilty of aggravated drunken driving and reckless homicide related to a car crash while he was off duty that killed a 20-year-old man	Chicago Sun-Times, April 28, 2005
1992	Anthony	Kreiser	Police Officer	Convicted	DGG	Found guilty of conspiring to distribute cocaine	Chicago Tribune, May 24, 1992
1988	Clarence	Kujawa	Detective	Convicted	GPC	Pleaded guilty: tax charges, accepting payoffs to make sure bar owners received liquor licenses	Chicago Sun Times, Apr 22, 1988
1991	Roy	Kummer	Police Officer	Convicted	ODC	Found guilty of aggravated battery in connection with the fatal beating committed while off duty	Chicago Tribune, April 14, 1991
1988	Leonard	Kurz	Police Officer	Convicted	BTX	Found guilty of charges stemming from robbery and severely beating a businessman who filed a complaint against him for harassment	Chicago Tribune, July 30, 1995
1981	Thomas	Kurz	Police Officer	Convicted	GPC	Found guilty of mail fraud and attempted extortion	Chicago Tribune, Feb 27, 1981
2000	John	Labiak	Police Officer	Convicted	CRV	Found guilty of home invasion and aggravated unlawful restraint and multiple counts of armed violence, bribery and official misconduct	Chicago Tribune, Sep 15, 2004
1992	Edward	LaCourse	Police Officer	Convicted	GPC	Pleaded guilty to extorting bribes from trucking companies to overlook trucks exceeding weight limits	Chicago Tribune, April 2, 1992
1984	James	LaFevour	Police Officer	Convicted	GPC	Pleaded guilty to 3 counts of tax fraud	Chicago Tribune, April 30, 1985
1974	Arthur	LaGace	Police Officer	Convicted	GPC	Found guilty of bribery and shaking down a motorist during a traffic stop	Chicago Tribune, June 14, 1974
1987	Michael	Lambesis	Investigator	Convicted	GPC	Pleaded guilty to corruption charges and admitted he passed \$17,500 in bribe money. On the separate charge he also pleaded guilty to selling two machine guns and two silencers to the undercover FBI agent	Chicago Tribune, Aug 11, 1987

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338

PAGE 37 of 34	1993	Milton	Lancaster	Police Officer	Convicted	BTX	Found guilty of official misconduct and criminal sexual abuse for molesting a woman he pulled over for a traffic stop	Chicago Tribune, Aug 19, 1993
	1991	Patrick	Lawrence	Police Officer	Convicted	ODC	Found guilty of sexual assaulted and abuse of a 15-year-old boy while off duty	Chicago Tribune, Sep 20, 1991
	2007	Edward	Leak	Police Officer	Convicted	ODC	Found guilty of masterminding a plot to have his friend and business associate killed to collect on a \$500,000 insurance policy	Chicago Tribune, Oct 19, 2007
	1994	Reginald	Lee	Police Officer	Convicted	DGG	Found guilty of charges related to possession of a controlled substance and sale of narcotics	Court Case 392 F.3d 909, Docket No. 04-1402
	2012	Glenn	Lewellen	Police Officer	Convicted	DGG	Found guilty of providing members of the drug ring with information concerning ongoing federal investigations into its operations	Chicago Tribune, Feb 1, 2012
	1980	Peter	Lipa	Police Officer	Convicted	ODC	Found guilty of stealing \$100,000 in state toll-way revenue during the armed robbery of a toll-road collection truck while off duty	Chicago Tribune, Oct 6, 1980
	1998	Marvin	Little	Police Officer	Convicted	GPC	Found guilty of theft and official misconduct perpetrated during warrantless search	Chicago Tribune, Jan 13, 1998
	1998	Richard	Lopardo	Police Officer	Convicted	DGG	Pleaded guilty to charges that he pocketed payoffs in return for providing sensitive details about a police investigation of a drug dealer	Chicago Tribune, Oct 23, 1998
	1982	Curtis A.	Lowery	Police Officer	Convicted	DGG	Found guilty of accepting bribes to allow two heroin rings to operate in the Marquette District.	Chicago Tribune Jul 1, 1982
	2003	Kenny	Lunsford	Police Officer	Convicted	CRV	Found guilty of wrongful death of an unarmed man he shot in the back	Chicago Tribune, Aug 08, 2003
	1988	Duane	Lyle	Police Officer	Convicted	CRV	Found guilty of violating the civil rights of a South Side man he shot in the head after a traffic accident	Chicago Tribune, Nov 16, 1988
	1981	Richard	Madeja	Police Officer	Convicted	ODC	Pleaded guilty to possession and manufacture of silencer	Chicago Tribune, Nov 10, 1981
	2009	Bart	Maka	Police Officer	Convicted	DGG	Pleaded guilty to felony theft related to illegal searchers of drug dealers and gang suspects and stealing their money and narcotics	Chicago Sun Times, Sep 18, 2009

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338

1985	Steve	Manning	Police Officer	Convicted	GPC	Found guilty of conspiracy and burglarizing a jewelry store in Pilsner where \$260,000 were stolen in jewels	Chicago Tribune, March 11, 1987
2009	Donovan	Markiewicz	Police Officer	Convicted	DGG	Pleaded guilty to official misconduct related to illegal searchers of drug dealers and gang suspects and stealing their money and narcotics	Chicago Sun Times, Sep 18, 2009
1994	Thomas	Marquez	Police Officer	Convicted	BTX	Pleaded guilty to a charge of extortion	Chicago Tribune, Jan 27, 1994
1985	Louis J	Martin	Police Officer	Convicted	GPC	Found guilty of racketeering and mail fraud related to soliciting bribes from motorists who were under investigation for leaving the scenes of accidents	Chicago Tribune, Oct 3, 1985
2011	Antonio	Martinez Jr	Police Officer	Convicted	DGG	Pleaded guilty to conspiring to participate in racketeering activity, conspiring to possess cocaine and marijuana, interfering with commerce by threat or violence and using a firearm during a crime of violence and drug trafficking	Chicago Tribune, Dec 02, 2011
2000	Pedro	Mataterrazas II	Police Officer	Convicted	DGG	Pleaded guilty to narcotics conspiracy charges	Chicago Tribune, Oct. 7, 2000
2003	Peter L.	Matich	Police Officer	Convicted	DGG	Pleaded guilty to drug charges of stealing 7 kilograms of cocaine from a drug dealer	Chicago Sun-Times, Feb 14, 2003
1984	Arthur W.	McCauslin	Police Officer	Convicted	GPC	Pleaded guilty to income tax fraud	Chicago Tribune, Aug 22, 1985
2001	Brian M.	McCluskey	Police Officer	Convicted	DGG	Pleaded guilty to being part of a network that sold ecstasy to teenagers	Chicago Tribune, Nov 8, 2001
1996	Ralph	McCue	Police Officer	Convicted	GPC	Found guilty of two counts of official misconduct related to robbery of a videocassette and \$12	Chicago Tribune, Feb 8, 1996
1973	Edward	McGee	Police Officer	Convicted	GPC	Found guilty of conspiracy related to shakedown of tavern owners	Chicago Tribune, Oct 6, 1973

PAGE 38 of 34

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 39 OF 34

2009	James	McGovern	Sergeant	Convicted	DGG	Pleaded guilty to misdemeanor charge of attempted obstruction associated with illegal drug sales	Chicago Tribune, Sep 26, 2009
2007	Charlton	McKay	Police Officer	Convicted	ODC	Found guilty of trying to conceal his role in the reckless homicide by filing a false police report	Chicago Tribune, June 20, 2007
1986	Lawrence	McLain	Police Officer	Convicted	GPC	Pleaded guilty to two counts of tax fraud	Chicago Sun Times, May 29, 1986
1989	Edward J.	McMahon	Police Officer	Convicted	ODC	Pleaded guilty to misdemeanor election code violations in connection with the 1986 petition drive for a nonpartisan mayoral election	Chicago Sun-Times, Aug 17, 1989
1998	Gerald	Meachum	Police Officer	Convicted	DGG	Found guilty of robbing undercover agents posing as drug dealers	Chicago Sun-Times, June 9, 1998
1982	Erskine	Melchor	Police Officer	Convicted	DGG	Found guilty of possession and delivery of cocaine	Chicago Tribune, Feb 1, 1984
1995	Christopher	Messino	Police Officer	Convicted	DGG	Found guilty on two tax counts stemming from charges related to narcotics sales	Chicago Tribune, Oct 4, 2000
1995	Clement	Messino	Police Officer	Convicted	DGG	Found guilty of narcotics conspiracy, money laundering and tax charges	Chicago Tribune, April 14, 2000
2003	Joseph	Miedzianowski	Police Officer	Convicted	DGG	Found guilty of RICO conspiracy, distribution of cocaine, extortion, possession with intent to distribute cocaine & illegal possession of a firearm	Chicago Sun Times Feb 27, 2003
1990	Nedrick	Miller	Sergeant	Convicted	DGG	Pleaded guilty to running a million-dollar, round-the-clock drug ring operating out of an apartment building he managed	Chicago Tribune, Dec 20, 1996
2001	Steven G.	Miller	Police Officer	Convicted	GPC	Pleaded guilty to official misconduct related to shaking down immigrants	Chicago Tribune, Aug 14, 2001
1984	Raymond	Mills	Police Officer	Convicted	DGG	Found guilty of sale of a quarter ounce of cocaine	Chicago Tribune, March 29, 1984
1989	Thure	Mills	Police Officer	Convicted	DGG	Pleaded guilty to charges related to taking bribes to protect the activities of South Side gamblers and a drug dealer.	Chicago Tribune, Jan 10, 1990

ELECTRONICALLY FILED
 7/2/2015 12:12 PM
 2014-CH-15338
 PAGE 40 of 54

2012	Kallatt	Mohammed	Police Officer	Convicted	DGG	Pleaded guilty to extorting payoffs from heroin and crack dealers	Chicago Tribune, Nov 2, 2012
2001	M.L	Moore	Police Officer	Convicted	DGG	Found guilty of racketeering for shaking down drug dealers for cash and cocaine and providing protection for large narcotics deliveries	Chicago Sun Times Oct 19, 2001
1996	Martin	Moore	Police Officer	Convicted	GPC	Found guilty of two counts of official misconduct related to robbery of a videocassette and \$12	Chicago Tribune, Feb 8, 1996
1972	Walter	Moore	Police Officer	Convicted	GPC	Found guilty of trying to shake down Austin area tavern owners for \$50 a month	Chicago Tribune, June 20, 1972
2004	Mario	Morales	Police Officer	Convicted	DGG	Pleaded guilty to stealing 220 pounds of marijuana and more than \$10,000 in cash from a drug dealer	Chicago Tribune, Jan 22, 2004
1961	Henry	Mulea	Police Officer	Convicted	GPC	Found guilty of conspiracy to commit burglary and conspiracy to receive stolen property while in uniform and on duty	Chicago Tribune, Aug 24, 1961
1973	Lowell E.	Napier	Police Officer	Convicted	GPC	Pleaded guilty to one count of conspiracy to commit extortion of tavern owners	Chicago Tribune, Jan 24, 1973
1989	Ronald	Nash	Police Officer	Convicted	GPC	Pleaded guilty to charges stemming from taking bribes in an FBI auto-theft sting	Chicago Sun Times, Oct 15, 2012
2002	Thomas P	Nash	Police Officer	Convicted	GPC	Pleaded guilty to a single misdemeanor count of theft related to disability scam	Chicago Sun Times, Oct 15, 2012
1985	John	Novack	Police Officer	Convicted	GPC	Found guilty of mail fraud and racketeering related to accepting bribes from motorists involved in hit and run accidents	Chicago Tribune, May 30, 1985
1969	Richard L.	Nuccio	Police Officer	Convicted	ODC	Found guilty of murder of a 19-year old youth whom he shoot in the back	Chicago Tribune, May 22, 1969
1989	Daniel	O'Connor	Police	Convicted	GPC	Found guilty of taking \$950 in bribes for	Chicago Tribune,

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 41 of 54

			Officer			providing confidential information	Oct 24, 1989
1988	Robert	O'Donnell	Police Officer	Convicted	GPC	Pleaded guilty to income tax evasion related to accepting payoffs to make sure bar owners received liquor licenses	Chicago Sun-Times, Apr. 22, 1988
2003	Ruben	Oliveras	Police Officer	Convicted	DGG	Pleaded guilty to misdemeanor civil rights violation	Chicago Tribune, May 29, 2003
2011	Eric	Olsen	Police Officer	Convicted	DGG	Plead guilty to conducting illegal searches and lying about it, in court or before a grand jury	Chicago Tribune, April 20, 2011
1975	Peter	Orciuoli	Police Officer	Convicted	GPC	Found guilty on charges of theft of \$90,000 worth of cigarettes	Chicago Tribune, Jan 15, 1975
2011	Donald	Owsley	Police Officer	Convicted	ODC	Found guilty of financial exploitation of the elderly and forgery while off duty	Chicago Sun-Times, June 18, 2011
1972	James V.	Pacente	Police Officer	Convicted	GPC	Found guilty of extortion and perjury related to tavern shakedown	Chicago Tribune, Oct 13, 1972
2009	John	Pallohusky	Sergeant	Convicted	GPC	Pleaded guilty to one count of felony theft related to stealing of about \$1 million from the union fund	Chicago Tribune, June 6, 2012
1995	Fred	Pascente	Detective	Convicted	ODC	Pleaded guilty to mail fraud involving a false insurance claim while off duty	Chicago Tribune, Nov. 28, 1995
1992	Robert	Passeri	Police Officer	Convicted	GPC	Pleaded guilty to extorting bribes from trucking companies to overlook trucks exceeding weight limits	Chicago Tribune, April 2, 1992
2002	William M.	Patterson	Sergeant	Convicted	DGG	Found guilty of conspiracy and attempting to possess cocaine with intent to distribute the drugs after stealing \$20,000 and five bricks of fake cocaine planted by government investigators	Chicago Tribune, May 3, 2002
1998	Falandes	Peacock	Police Officer	Convicted	ODC	Found guilty of stealing from a Super K-Mart while off duty	Chicago Tribune, Sep 2, 1998
1992	William	Pedersen	Detective	Convicted	ODC	Pleaded guilty to selling criminal histories and employment and earnings information stolen from federally protected computer files	Chicago Sun Times, January 23, 2011

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338

1982	Joseph R.	Pena	Police Officer	Convicted	DGG	Found guilty of accepting bribes to allow two heroin rings to operate in the Marquette District.	Chicago Tribune, Jul 1, 1982
1998	Gilberto	Perez	Police Officer	Convicted	BTX	Pleaded guilty to aggravated criminal sexual assault and kidnapping	Chicago Tribune, May 10, 1998
1981	Anthony	Pesha	Police Officer	Convicted	GPC	Found guilty of mail fraud and extortion related to police car repair schemes and phony billing to the city of Chicago	Chicago Tribune, Feb 27, 1981
1993	Samuel	Pesoli	Police Officer	Convicted	GPC	Pleaded guilty to 2 counts of perjury	Chicago Sun-Times, May 4, 1993
2002	James	Petrucci	Police Officer	Convicted	GPC	Pleaded guilty to lying to a supervisor related to shaking down immigrants for money	Chicago Tribune, May 10, 2002
1981	Tyrone	Pickens	Police Officer	Convicted	GPC	Found guilty of charges stemming from burglarizing home while in uniform, official misconduct and possession of marijuana	Chicago Tribune, Sep 7, 1981
2003	Edgar I.	Placencio	Police Officer	Convicted	DGG	Pleaded guilty to concealing a civil rights felony	Chicago Tribune, May 29, 2003
2012	Juan	Prado	Police Officer	Convicted	GPC	Pleaded guilty to extortion-related to pocketing money in payoffs from a tow truck operator	Chicago Tribune, July 1, 2010
2009	Brian	Pratscher	Police Officer	Convicted	DGG	Pleaded guilty to felony theft related to illegal searchers of drug dealers and gang suspects and stealing their money and narcotics	Chicago Sun Times, Sept 18, 2009
1991	Robert	Purtill	Lieutenant	Convicted	GPC	Pleaded guilty to three felony tax charges of depriving the government out of in excess of \$100 by not reporting the bribes on his tax returns	Chicago Tribune, Feb 15, 1991
2001	Alex D.	Ramos	Police Officer	Convicted	DGG	Found guilty of racketeering for shaking down drug dealers for cash and cocaine and providing protection for large narcotics deliveries	Chicago Sun Times Oct 19, 2001
1994	Michael	Randy	Police Officer	Convicted	ODC	Found guilty of mail fraud and money laundering related to sale of fraudulent certificates of deposit	Chicago Tribune, Jan 5, 1994

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 43 of 34

1998	Herbert	Redmond	Police Officer	Convicted	GPC	Found guilty of theft and official misconduct perpetrated during warrantless search	Chicago Tribune, Jan 13, 1998
1982	Vincent R.	Rizza	Police Officer	Convicted	DGG	Found guilty of conspiring to sell cocaine valued at \$120,000	Chicago Tribune, May 22, 1982
1992	Nickolas	Rizzato	Police Officer	Convicted	DGG	Pleaded guilty to conspiring to possess and distribute cocaine	Chicago Tribune, Jan 20, 1992
1961	Daniel	Rizzo	Police Officer	Convicted	GPC	Found guilty of accepting a \$10 dollar bribe from a motorist whom he stopped for driving through a stop sign	Chicago Tribune, Jan 18, 1961
1973	Stanley B.	Robinson	Sergeant	Convicted	CRV	Found guilty of depriving two citizens of their rights to life, liberty, and property without due process	Chicago Tribune, Aug 7, 1973
2002	Norberto	Rodriguez	Police Officer	Convicted	DGG	Pleaded guilty to possession of heroin with intent to sell	Chicago Tribune, Nov 23, 2010
1995	Lloyd	Roe	Police Officer	Convicted	DGG	Pleaded guilty to extorting money from a drug dealer	Chicago Tribune, Aug 24, 1995
2000	John	Rose	Police Officer	Convicted	DGG	Pleaded guilty to selling crack cocaine stolen from drug dealers	Chicago Tribune, June 30, 2000
1973	James	Ross	Patrolman	Convicted	GPC	Found guilty of extortion and one count perjury for lying to the court	Chicago Tribune, Jan 12, 1973
1988	Rick	Runnels Sr.	Police Officer	Convicted	BTX	Found guilty of charges related to robbery and beating of a businessman who filed a complaint against him for harassment	Chicago Tribune, July 30, 1995
1973	Edward	Russell	Police Officer	Convicted	GPC	Found guilty of conspiracy and perjury related to shakedown of tavern owners	Chicago Tribune, Oct 6, 1973
1973	Emmons P.	Russell	Police Officer	Convicted	GPC	Found guilty of conspiracy and perjury related to shakedown of tavern owners	Chicago Tribune, Oct 6, 1973
2010	Sean	Ryan	Police Officer	Convicted	DGG	Pleaded guilty to charges that he sold a semi-automatic assault rifle to a gang member who was a convicted drug dealer	Chicago Tribune, Jan 13, 2010
2009	Guadalupe	Salinas	Police Officer	Convicted	DGG	Pleaded guilty to felony theft related to illegal searches of drug dealers and gang suspects and stealing their money and narcotics	Chicago Sun Times, Sep 18, 2009

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338

PAGE 44 of 54	1973	Harry R.	Salvesen	Police Officer	Convicted	GPC	Found guilty of conspiracy related to shakedown of tavern owners	Chicago Tribune, Oct 6, 1973
	1990	Fred	Sanders	Patrolman	Convicted	DGG	Found guilty of charges related to taking bribes to protect the activities of gamblers and a drug dealer	Chicago Sun Times, Jan 10, 1990
	1977	Richard	Scanlon	Sergeant	Convicted	CRV	Pleaded guilty to official misconduct stemming from charges that he lied on a stand when he testified that a defendant shot him while the truth was that the officer shot himself during a struggle.	Chicago Tribune, Aug 17, 1977
	1973	Joseph A.	Schillinger	Sergeant	Convicted	GPC	Found guilty of conspiracy and perjury related to shakedown of tavern owners	Chicago Tribune, Oct 6, 1973
	1972	Thomas	Schmidt	Police Officer	Convicted	BTX	Found guilty of depriving a suspect of civil rights by beating him with a night stick and kicking his teeth out	Chicago Tribune, Nov 27, 1972
	1973	Steve L.	Seno	Police Officer	Convicted	GPC	Found guilty of conspiracy related to shakedown of tavern owners	Chicago Tribune, Oct 6, 1973
	1974	Gerald	Sepka	Police Officer	Convicted	GPC	Found guilty of bribery and shaking down a motorist during a traffic stop	Chicago Tribune, June 14, 1974
	1985	Robert M.	Sepulveda	Police Officer	Convicted	GPC	Pleaded guilty to accepting bribes to sidetrack investigations of motorists involved hit-and-run accidents	Chicago Tribune, May 30, 1985
	1990	Mitchell	Shacter	Lieutenant	Convicted	CRV	Pleaded guilty to a misdemeanor charge of harassment by telephone	Chicago Tribune, Feb 10, 1990
	2009	Mahmoud "Mike"	Shamah	Police Officer	Convicted	DGG	Found guilty of racketeering and conspiracy charges related to stealing of drugs from drug dealers	Chicago Tribune, July 3, 2009
	1960	James	Shannon	Police Officer	Convicted	GPC	Pleaded guilty to aiding robbers in holdups and collecting payoffs from them	Chicago Tribune, May 25, 1960

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 45 OF 54

2001	Lennon	Shields	Police Officer	Convicted	DGG	Found guilty of racketeering for shaking down drug dealers for cash and cocaine and providing protection for large narcotics deliveries	Chicago Sun Times Oct 19, 2001
1998	Alex	Sierra	Police Officer	Convicted	GPC	Pleaded guilty to conspiracy to commit a robbery	Chicago Tribune, Feb 14, 1998
2002	Michael	Simpson	Police Officer	Convicted	GPC	Pleaded guilty to charges of lying to a supervisor related to shaking down immigrants	Chicago Tribune, May 10, 2002
1992	Raymond	Siwek	Detective	Convicted	DGG	Found guilty of possession with intent to deliver more than 500 grams of cocaine	Chicago Tribune, May 5, 1995
1982	Dennis L.	Smentek	Police Officer	Convicted	DGG	Found guilty of accepting bribes to allow two heroin rings to operate in the Marquette District.	Chicago Tribune Jul 1, 1982
1982	Dennis	Smetanka	Police Officer	Convicted	DGG	Found guilty of accepting bribes to allow two heroin rings to operate in the Marquette District.	Chicago Tribune, April 11, 1995
2004	John L.	Smith	Police Officer	Convicted	DGG	Found guilty of narcotics conspiracy, money laundering and three counts each of tax evasion and filing false tax returns	Chicago Tribune, Nov 11, 2004
1989	Willie	Smith	Patrolman	Convicted	DGG	Pleaded guilty to charges related to taking bribes to protect the activities of South Side gamblers and a drug dealer.	Chicago Tribune, Jan 10, 1990
2002	Daryl L.	Smith	Police Officer	Convicted	GPC	Found guilty of theft of government property	Chicago Tribune, May 3, 2002
2000	Richard	Sobotta	Police Officer	Convicted	ODC	Pleaded guilty to contempt of court for helping a superior try to wiggle out of a speeding ticket	Chicago Sun-Times, Oct 24, 2000
1987	William	Sorice	Police Officer	Convicted	GPC	Found guilty of conspiring and burglarizing a jewelry store where \$260,000 were stolen in jewels	Chicago Tribune, March 11, 1987
1992	Gloria	Steele	Police Officer	Convicted	DGG	Found guilty of charges that she aided in her son's large-scale heroin operation	Chicago Tribune, May 9, 1992
1989	Robert	Stephenson	Sergeant	Convicted	DGG	Found guilty of charges related to taking bribes to protect the activities of gamblers and a drug dealer	Chicago Tribune, July 12, 1990
1995	Tyrone	Stevenson	Police Officer	Convicted	DGG	Pleaded guilty to charges of extortion where he extorted \$150,000 from an Indiana drug dealer	Chicago Tribune, Aug 24, 1995

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338

1989	Orville	Stewart	Patrolman	Convicted	DGG	Found guilty of charges related to taking bribes to protect the activities of South Side gamblers and a drug dealer	Chicago Tribune, July 12, 1990
1986	Vito	Stonis	Police Officer	Convicted	BTX	Pleaded guilty to aggravated battery and one count of official misconduct for beating a man arrested for loitering	Chicago Tribune, Oct 9, 1986
1998	Baxter G.	Streets	Police Officer	Convicted	DGG	Found guilty of robbing undercover agents posing as drug dealers	Chicago Sun-Times, June 10, 1998
1966	John	Sullivan	Detective	Convicted	DGG	Found guilty of sale of narcotics	Chicago Tribune, Nov 11, 1966
2003	Vondale	Sullivan	Police Officer	Convicted	ODC	Pleaded guilty to a federal bank robbery charge	Pantagraph, Nov 15, 2003
1995	John	Summerville	Detective	Convicted	BTX	Pleaded guilty to sexually assaulting several women during traffic stops	Chicago Sun Times, July 28, 1995
1973	William D.	Swallow	Police Officer	Convicted	GPC	Found guilty of conspiracy and perjury related to shakedown of tavern owners	Chicago Tribune, Oct 6, 1973
1973	William	Taylor	Police Officer	Convicted	DGG	Found guilty of smuggling narcotics	Chicago Tribune, Aug 5, 1973
1966	Sheldon	Teller	Sergeant	Convicted	DGG	Found guilty of sale of narcotics	Chicago Tribune, Nov 11, 1966
1979	Mary Ann	Terry	Police Officer	Convicted	GPC	Found guilty of welfare fraud and perjury while on active duty	Chicago Tribune, Sep 14, 1980
1974	Mark	Thanasouras	Captain	Convicted	GPC	Pleaded guilty to charges stemming from corruption and shaking down of tavern owners	Chicago Tribune, Feb. 5, 1974
1991	Daniel	Thanos	Police Officer	Convicted	ODC	Found guilty of aggravated battery in connection with the fatal beating committed while off duty	Chicago Tribune, April 6, 1991
1989	Fred	Tilford	Patrolman	Convicted	DGG	Found guilty of charges related to taking bribes to protect the activities of gamblers and a drug dealer	Chicago Tribune, July 12, 1990

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 47 of 54

1975	John	Toner	Sergeant	Convicted	GPC	Found guilty of perjury in connection with shakedown of operators of parking lots	Chicago Tribune, March 14, 1975
2001	William	Tortoriello	Police Officer	Convicted	GPC	Pleaded guilty to official misconduct related to shaking down immigrants	Chicago Tribune, Aug 14, 2001
2001	Cornelius	Tripp	Police Officer	Convicted	DGG	Pleaded guilty to racketeering for shaking down drug dealers for cash and cocaine and providing protection for large narcotics deliveries	Chicago Sun Times, Oct 19, 2001
1984	James	Trunzo	Police Officer	Convicted	GPC	Pleaded guilty to two counts of tax fraud	Chicago Tribune Jan 6, 1986
1984	Joseph	Trunzoi	Police Officer	Convicted	GPC	Pleaded guilty to two counts of tax fraud	Chicago Tribune Jan 6, 1986
1998	Samuel	Turks	Police Officer	Convicted	BTX	Found guilty of official misconduct related to fondling of women while conducting routine traffic stops	Chicago Tribune, June 12, 1998
1991	John A.	Vercillo	Police Officer	Convicted	ODC	Found guilty of RICO charges related to series of illicit trades while off duty	Chicago Tribune, Jan 10, 1991
2000	Costantino	Verre	Lieutenant	Convicted	ODC	Pleaded guilty to contempt of court related to perjury in court over a speeding ticket	Chicago Sun-Times, Oct 24, 2000
2009	Frank	Villareal	Police Officer	Convicted	DGG	Pleaded guilty to a felony theft charge stemming from illegal searchers of drug dealers and gang suspects and stealing their money and narcotics	Chicago Tribune, Sep 26, 2009
1980	Donald	Vogwill	Police Officer	Convicted	DGG	Pleaded guilty to conspiracy related to smuggling of cocaine into US	Chicago Tribune, Sep 5, 1980
1980	James	Vogwill	Police Officer	Convicted	DGG	Found guilty of conspiracy to smuggle cocaine into US	Chicago Tribune, Sep 5, 1980
1984	Carl	Walston	Police Officer	Convicted	DGG	Found guilty of official misconduct for selling fake heroin to a government informant out of his police car	Chicago Tribune, Feb 25, 1984
1981	Stephen	Webster	Police Officer	Convicted	GPC	Found guilty of charges stemming from burglarizing home while in uniform, official	Chicago Tribune, Sep 7, 1981

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338

						misconduct and possession of marijuana	
1986	Walter	Wells	Police Officer	Convicted	BTX	Found guilty of aggravated sexual assault, and sexual abuse of an 11 year old girl	Chicago Tribune, Dec 18, 1986
1973	Thomas D.	West	Sergeant	Convicted	GPC	Found guilty of conspiracy and perjury related to shakedown of tavern owners	Chicago Tribune, Oct 6, 1973
1991	Gerald	Williams	Police Officer	Convicted	ODC	Found guilty of fatally shooting his physically disabled wife while off duty	Chicago Tribune, Sep 18, 1991
1989	Clarence	Wilson	Police Officer	Convicted	DGG	Found guilty of charges related to taking bribes to protect the activities of gamblers and a drug dealer	Chicago Tribune, July 12, 1990
2012	James	Wodnicki	Police Officer	Convicted	GPC	Pleaded guilty to charges stemming from extortion-related to tow scam	Chicago Tribune, June 19, 2012
2003	Jon F.	Woodall	Detective	Convicted	DGG	Pleaded guilty to conspiring to distribute cocaine	Chicago Sun Times Feb 27, 2003
1989	Thomas	York	Police Officer	Convicted	ODC	Found guilty of mail fraud, arson, and conspiracy	Chicago Sun-Times, July 8, 1989
2001	James P.	Young	Police Officer	Convicted	DGG	Found guilty of racketeering for shaking down drug dealers for cash and cocaine and providing protection for large narcotics deliveries	Chicago Sun-Times Oct 19, 2001
1973	Mike	Zakoian	Police Officer	Convicted	GPC	Found guilty of conspiracy related to shakedown of tavern owners	Chicago Tribune, Oct 6, 1973
1990	Dennis	Zancha	Police Officer	Convicted	BTX	Found guilty of aggravated criminal sexual assault for the attack on a 22 year old woman	Chicago Tribune, Feb 27, 1990
1992	Jerry	Zywicki	Police Officer	Convicted	GPC	Pleaded guilty to conspiring with two other officers to rob a tavern owner and two bartenders	Chicago Tribune, Dec 23, 1992

PAGE 48 of 24

Appendix II: Police Reform in South Africa

Policing the police in Chicago is similar in many ways to problems in other international settings. For example, here is an excerpt from the Executive Summary of an anti-corruption report “Protector or Predator: Tackling Police Corruption in South Africa.” In many ways the problems of Chicago’s police are similar to post-Apartheid South Africa. Note the similar use of “bad apples” as a way to deflect more serious inquiry. As the South African reports says: “A rotten barrel breeds rotten apples, not the other way around.”

Despite the positive changes that have occurred within the South African Police Service (SAPS) since the birth of democracy in 1994, police corruption remains a substantial challenge for the organization. While the extent of police corruption cannot be easily or accurately measured, there is evidence that the problem is a widespread and systemic one. This is not to say that most or a majority of police officials engage in corruption. However, the prevalence of the problem is such that it substantially hinders the extent to which the SAPS is able to achieve its constitutional objectives and build public trust. This is not a unique challenge facing the SAPS. Corruption is a challenge throughout the country’s public and private sectors and is a specific occupational hazard of policing agencies worldwide. Given the nexus of power, discretion and inadequate accountability that often arises in policing, this profession is particularly prone to the problem of corruption.

Typically, police management will respond to incidents or allegations of corruption as a problem of a few ‘bad apples’ who must be punished or removed from the organization. Yet, international research and commissions of inquiry into police corruption consistently emphasize that corruption is more a manifestation of organizational weaknesses than a challenge of bad employees. As such, punitive action against individuals who commit acts of corruption, while necessary, will on its own do little to change the factors that allow for police deviance and corruption to occur in the first place. To address corruption effectively a more holistic approach is required that focuses on strengthening the integrity of both the organization and its employees.

Appendix III: Illinois Law on Misconduct in Public Office

The *Illinois Criminal Code of 1961* (ILCS720/33-3) indicates that any public officer or employee commits misconduct when, in her official capacity, she does any of the following:

- § Intentionally or recklessly fails to perform mandatory duty as required by law;
- § Knowingly performs an act the employee is forbidden by law to perform;
- § Performs an act in excess of their lawful authority with intent to obtain a personal advantage for herself or another; or solicit or knowingly accept for the performance of any act a fee or reward which the employee knows is unauthorized by law.

Appendix IV

PETITION FOR A DEMOCRATICALLY ELECTED CIVILIAN POLICE ACCOUNTABILITY COUNCIL

We, residents of Chicago, Illinois, do hereby petition the Chicago City Council and Mayor Rahm Emanuel to enact legislation such as that proposed by the Chicago Alliance Against Racist and Political Repression to establish a democratically elected Civilian Police Accountability Council (CPAC). This Council will be empowered to make policy, hire and fire police, petition for the appointment of a Special Prosecutor to investigate and prosecute police accused of crimes such as battery, unlawful arrest, racial profiling, torture and murder, and the use of force to suppress the democratic rights of the people to organize and protest.

Return petitions to
Chicago Alliance Against Racist and Political Repression
1325 S. Wabash Ave. Suite 105
Chicago IL 60605
For information; contact@naarpr.org, 312-939-2750
www.naarpr.org

ENDNOTES

¹ Janssen, Kim. “ ‘We proved a code of silence’.” Chicago Sun-Times. November 14, 2012.

² Lou Reiter, police consultant in testimony in US District Court, Northern District of Illinois, Eastern Division. Klpfel and Casalis vs City of Chicago. Case No. 94 C 6415. Feb 23, 2007. This case resulted in a \$9.75 million judgement against the City of Chicago. p. 9.

³ Futterman, Craig et al. “The Use of Statistical Evidence to Address Police Supervisory and Disciplinary Practices: The Chicago Police Department’s Broken System.” November 14, 2007.

⁴ “Police Misconduct’s Legal Tab.” Chicago Sun-Times. July 30, 2012.

⁵ Ibid.

⁶ Meyerson, Ben. “Record verdict: Former gang member awarded \$21 million for wrongful conviction.” Chicago Tribune. June 23, 2009,

⁷ Lighty, Todd and Gary Washburn. “City to pay Haggertys \$18 million.” Chicago Tribune. May 8, 2001.

⁸ This was part of the SOS scandal which we will report on below. On Finnegan attempting to hire a 2-6 gang member to “hit” a fellow officer, see Sun-Times, March 20. 2012: “From jail, cop who admitted guilt in murder-for-hire plot proclaims innocence,” by Frank Main.

⁹ Life Vol. 65, No. 23. Dec. 6, 1968

¹⁰ <http://encyclopedia.chicagohistory.org/pages/1049.html>

¹¹ Carter, David A. Journal of Criminal Justice Vol. 18. pp. 85-98 (1990) p 92

¹² Lou Reiter, police consultant in testimony in US District Court, Northern District of Illinois, Eastern Division. Klpfel and Casalis vs City of Chicago. Case No. 94 C 6415. Feb 23, 2007. This case resulted in a \$9.75 million judgement against the City of Chicago.

¹³ Journal Gazette (Mattoon, IL) - Tuesday, April 24, 2001

¹⁴ Newman, Tim. Understanding and Preventing Police Corruption. Lessons from the Literature. Research Development Statistics. London. 1999

¹⁵ Reiter, op cit. p. 9

¹⁶ Reiter, op cit. p 17.

¹⁷ Reiter op cit. p 19-20.

¹⁸ Knapp, 1972:6-7

¹⁹ Hanna, Janan, John O’Brien and Bill Crawford. “ ‘Marquette 10’ cop celebrates freedom with 500 backers.” Chicago Tribune. April 11, 1995.

²⁰ O’Connor. “Austin cops sent to prison; 5 former officers sentenced in ’96 corruption probe.” Chicago Tribune. October 19, 2001.

²¹ Ibid.

²² Lighty, Todd and Matt O’Connor. “Rogue cop gets life.” Chicago Tribune. January 25, 2003.

²³ Heinzmann, David and Annie Sweeney. “Federal prosecutors say 4 Chicago police officers from elite SOS unit will plead guilty.” Chicago Tribune. April 7, 2011.

²⁴ Heinzmann, David Todd Lighty and Jeff Coen. “Feds join in probe of city’s elite police; Stakes get higher for accused officers.” Chicago Tribune. August 16, 2007.

²⁵ Meisner, Jason. “What happened to the elite officers charged.” Chicago Tribune. September 9, 2011.

²⁶ Heinzman, David. “Indicted city cop to be on ’60 Minutes.’” Chicago Tribune. May 30, 2008.

²⁷ Meisner, Jason. “What happened to the elite officers charged.” Chicago Tribune. September 9, 2011.

²⁸ Marin, Carol and Dan Moseley. “Jailed former cop speaks out about murder scandal.” NBC 5 Chicago

News. March 21, 2012.

²⁹ Tompkins, Sarah. "Ex-Chicago cop plead guilty to racketeering in Latin King case." The Times of Northwest Indiana. July 26, 2012.

³⁰ Sweeney, Annie. "Ex-cop convicted of joining conspiracy." Chicago Tribune. February 01, 2012.

³¹ Ibid.

³² Main, Frank. "Drug-dealing killer: Chicago cop stopped DEA investigation." Chicago Sun-Times. October 4, 2011.

³³ Ibid.

³⁴ Main, Frank. "Ex-cop, four others guilty of participating in drug crew." Chicago Sun-Times. January 31, 2012.

³⁵ Sweeney, Annie. "Ex-cop convicted of joining conspiracy." Chicago Tribune. February 01, 2012.

³⁶ O'Connor, Matt. "Police lose false arrest lawsuit." Chicago Tribune. November 18, 2001.

³⁷ Ibid

³⁸ Babwin, Bob and Michael Tarm. "Will Chicago act on verdict in cop beating trial." NBC News. November 14, 2012.

³⁹ Sweeney, Annie and Jason Meisner. "Jury finds in favor of bartender in cop bar beating case, 'Justice was served.'" Chicago Tribune. November 14, 2012.

⁴⁰ Ibid.

⁴¹ Ibid.

⁴² Janssen, Kim. "Bartender beaten by drunken Chicago cop wins \$850,000 verdict." Chicago Sun-Times. November 13, 2012.

⁴³ Coen, Jeff. "Ex-cop testifies of code, bloody glove." Chicago Tribune. August 23, 2007.

⁴⁴ Coen, Jeff. "Ex-cop testifies of code, bloody glove." Chicago Tribune. August 23, 2007.

⁴⁵ Coen, Jeff. "Ex-cop Anthony Doyle gets 12 years for aiding Outfit." Chicago Tribune. March 13, 2009.

⁴⁶ Schlikerman, Becky. "High-ranking crooked cop released to halfway house." Chicago Tribune. July 19, 2011.

⁴⁷ UNITED PRESS INTERNATIONAL. "CHICAGO CHOOSES A CRIMINOLOGIST TO HEAD AND CLEAN UP THE POLICE." THE NEW YORK TIMES. FEBRUARY 23, 1960.

⁴⁸ Knoohuizen, Ralph. Public Access to Police Information: A Report of the Chicago Law Enforcement Study Group. 1974.

⁴⁹ "Chicago names police panel but refuses a review board." New York Times. July 26, 1966.

⁵⁰ Ibid.

⁵¹ Ibid.

⁵² Chicago Tribune December 6th, 1967

⁵³ Ibid.

⁵⁴ Ibid.

⁵⁵ Ibid.

⁵⁶ Knoohuizen, Ralph. Public Access to Police Information: A Report of the Chicago Law Enforcement Study Group. 1974.

⁵⁷ <http://www.columbia.edu/itc/journalism/cases/katrina/Human%20Rights%20Watch/uspohtml/uspo55.htm#TopOfPage>

⁵⁸ Knoohuizen, Ralph. Public Access to Police Information: A Report of the Chicago Law Enforcement Study Group. 1974.

⁵⁹ <http://www.columbia.edu/itc/journalism/cases/katrina/Human%20Rights%20Watch/uspohtml/uspo55.htm#TopOfPage>

⁶⁰ Conroy, John. "Town without pity." Chicago Reader. January 11, 1996.

⁶¹ Independent Police Review Authority. "Annual Report 2007-2008." City of Chicago. September 2008

⁶² Siska, Tracy and Sherie Arriazola. Chicago Police Board: A 10-Year Analysis. 2009. The Chicago Justice Project.

⁶³ Siska, Tracy and Sherie Arriazola. Chicago Police Board: A 10-Year Analysis. 2009. The Chicago Justice Project.

⁶⁴ Cano I. (2005) Police Oversight in Brazil International Conference on Police Accountability and the Quality of Oversight: Global Trends in National Context, The Hague, The Netherlands.

⁶⁵ Gareth Newham and Andrew Faull. Protector or predator? Tackling police corruption in South Africa. ISS Monograph. No 182.

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF ERIE

----- X
In the Matter of, :
 :
NEW YORK CIVIL LIBERTIES UNION, : Index No. I 2014-000206
 :
Petitioner, :
 :
-against- :
 :
ERIE COUNTY SHERIFF'S OFFICE, :
 :
Respondent, :
 :
For a Judgment Pursuant to Article 78 :
of the Civil Practice Law and Rules. :
----- X

AFFIDAVIT OF ROBERT CLIFTON BURNS

Robert Clifton Burns, being duly sworn, deposes and states:

1. I am Counsel at Bryan Cave in Washington, D.C., focusing my practice on export controls, economic sanctions, and customs law. My clients include companies in high-tech industries including lasers, software, medical devices, telecommunications, networking equipment, and military systems and components. My address is 1155 F Street, NW, Washington, DC, 20004. I am also an Adjunct Professor at Georgetown University Law Center, where I teach a class on Global Commerce and Litigation (which includes export controls and economic sanctions).

2. I submit this affidavit in support of the Petitioner's reply to the Respondent's opposition to the above-captioned Article 78 Petition.

3. Attached as Exhibit A is a true and correct copy of my resume as it appears on the Bryan Cave website. I am widely recognized as an expert on export law, including the law and

regulations relating to the International Traffic in Arms Regulations (“ITAR”), and have been quoted on these matters by, among others, the following media outlets: NPR, New York Times, Washington Post, Reuters, and USA Today.

4. Pursuant to the Criminal Justice Act, I have served as an expert in two federal district court cases involving the ITAR: *United States v. Gowadia*, No. 1:05-cr-00486-SOM-KSC-1 (D. Haw. filed Oct. 26, 2005), and *United States v. Komorowski*, No. 3:08-cr-00228-EMK-1 (M.D. Pa. Jun. 4, 2008).

5. I reviewed the following materials in preparing this affidavit:

- a. Petitioner’s Freedom of Information Law Request, dated June 16, 2014;
- b. Affidavit of FBI Agent Bradley S. Morrison, dated December 31, 2014;
- c. Certificate of Incorporation of Petitioner New York Civil Liberties Union and the New York Civil Liberties Union Foundation;
- d. Disclosures made by Respondent (Affirmation of Andrea Schillaci, Ex. E, F).
- e. U.S. Patent Number 7,592,956, available on the website of the U.S. Patent and Trademark Office, including diagrams;¹
- f. U.S. Trademark Status and Document Retrieval Records, available on the website of the U.S. Patent and Trademark Office, including photographs of various Stingray devices;²
- g. Unredacted Harris Corporation marketing materials, product descriptions, purchase orders, and sole source letters regarding Stingrays posted on the City of Miami’s website;³

¹<http://patft.uspto.gov/netahtml/PTO/srchnum.htm>.

²<http://tsdr.uspto.gov/documentviewer?caseId=sn76303503&docId=SPE20130404144554#docIn=&docIndex=2&page=1>;

<http://tsdr.uspto.gov/documentviewer?caseId=sn77316689&docId=SPE20140514151847#docIndex=2&page=1>;

<http://tsdr.uspto.gov/documentviewer?caseId=sn76303814&docId=SPE20140213150610#docIndex=2&page=1>.

- h. Directorate of Defense Trade Controls, Commodity Jurisdiction Final Determination for “Portable SIM Box Investigation Kit with IMSI/IMEI Catcher and Direction Finding Antenna,” U.S. Dep’t of State;⁴
- i. Relevant statutes and regulations as cited in this affidavit.

All Evidence Suggests That Stingrays Are Not On The Munitions List

6. In order to determine whether a device, or technological data related to that device, is controlled by the Arms Export Control Act (“AECA”) and its implementing International Traffic in Arms Regulations (“ITAR”), I execute the following analysis. First, I look to see if the item is specifically enumerated on the United States Munitions List (“USML”), *see* 22 U.S.C. § 2778; 22 C.F.R. § 121.1. I look to see if the Directorate of Defense Trade Controls (“DDTC”), the office within the Department of State with authority to designate items to these lists, has made a specific determination about the item or a similar item.

7. I have been asked to determine whether cell site simulators are regulated by the AECA and the ITAR. Cell site simulators, also called IMSI catchers, are devices that mimic cell phone towers and prompt cell phones to transmit their unique identifying numbers, including International Mobile Subscriber Identity (“IMSI”) or International Mobile Equipment Identity (“IMEI”), and that use directional antennas to locate one or more cell phones. “Stingray” is the name of one model of cell site simulator marketed by the U.S.-based Harris Corporation. Although other models of cell site simulators sold by Harris and other companies have different names, I will use the term “Stingray” throughout this affidavit to mean the whole category of cell site simulator technology.

³ <http://egov.ci.miami.fl.us/Legistarweb/Attachments/34769.pdf>;
<http://egov.ci.miami.fl.us/Legistarweb/Attachments/34771.pdf>;

⁴ [http://egov.ci.miami.fl.us/Legistarweb/Attachments/48003.pdf](https://www.pmddtc.state.gov/commodity_jurisdiction/determinationAll.html).

⁴ https://www.pmddtc.state.gov/commodity_jurisdiction/determinationAll.html.

8. In determining whether Stingrays are regulated by the AECA, I followed the steps described above. I concluded that Stingrays are likely not regulated by the AECA but are rather regulated by the Export Administration Act and the Commerce Control List, 15 C.F.R. § 774, established by the Export Administration Regulations (“EAR”), 15 C.F.R. Ch. VII. I came to this conclusion because, first, Stingrays do not appear anywhere on the USML. *See* 15. C.F.R. § 121.1. Category XI of the USML, which covers “Military Electronics” and which is the Category in which this device would most likely appear were it on the USML, enumerates a number of items with specificity. None of these specific listings include the Stingray, nor is the Stingray described in, or listed in, any other Category of the USML. Second, the description of items covered by Export Control Classification Number (“ECCN”) 5A001 on the Commerce Control List includes specific text describing IMSI catcher/cell site simulator technology that includes Stingrays: “Mobile telecommunications interception or jamming equipment, and monitoring equipment therefor,” including “interception equipment . . . designed for the extraction of client device or subscriber identifiers (e.g., IMSI, TIMSI or IMEI), signaling, or other metadata transmitted of the air interface.” 15 C.F.R. Pt. 774, Supp. 1, Cat. 5 (ECCN 5A001.f, f.2). This description aligns precisely with the Stingrays at issue in this case. Finally, I found on the website of the DDTC that, in a final determination published on April 22, 2013, the DDTC classified an item described as a “Portable SIM Box Investigation Kit with IMSI/IMEI Catcher and Direction Finding Antenna” as covered by ECCN 5A001.⁵ The description of this item in the DDTC determination, while not a Harris model, is similar enough to the Stingrays at issue in this case to further confirm that the controlling regulatory regime for Stingrays is indeed the Commerce Control List, not the AECA.

⁵ See Directorate of Defense Trade Controls Commodity Jurisdiction Final Determination for “Portable SIM Box Investigation Kit with IMSI/IMEI Catcher and Direction Finding Antenna,” U.S. Dep’t of State, https://www.pmddtc.state.gov/commodity_jurisdiction/determinationAll.html.

9. Agent Morrison claims that Stingrays are regulated under USML Category (XI)(b). I note first that he has cited to an outdated version of the list; while he argues that Stingrays are governed by USML Category XI(b) because they are “specifically designed for intelligence, security or military use” (Morrison Aff. ¶ 10), USML Category (XI)(b) has been amended so that it now only applies to equipment “specially designed for intelligence purposes.” 22 C.F.R. § 121.1; compare 22 C.F.R. § 121.1 (effective through Dec. 29, 2014) (prior version of the regulation). While the only way to conclusively determine whether an item was “specially designed for intelligence purposes” would be to obtain a statement from the manufacturer regarding the history of the product’s design or a determination from the DDTC, I see no evidence in Agent Morrison’s affirmation, nor in any of the other materials I have reviewed, showing that Stingrays were so designed. In my view, items that are disclosed in published U.S. Patent applications, as is the case with the Stingray device, are not likely to be “specially designed for intelligence purposes,” since such disclosure is at odds with the covert nature and purpose of items specially designed for intelligence purposes. The classification decision of DDTC cited above, that the above-mentioned “IMSI/IMEI Catcher and Direction Finding Antenna” was not a USML item, also confirms my belief that the Stingray device was not likely to have been specially designed for intelligence purposes. Technology is generally only regulated under one of these regimes, so a classification under the Commerce Control List as ECCN would preclude classification on the USML under the ITAR.

The Implications of Stingrays Being Governed by the Arms Export Control Act and the United States Munitions List Are Significant

10. If the records requested by Petitioner were governed by the AECA and the USML, as asserted by Agent Morrison, Respondent would have to be complying with a stringent set of requirements. Respondent, for example, would be required to severely limit access to all

of the records that it claims to be secret to prevent visual access by non-U.S. persons—anyone working in its own offices who might have access at any point to those records or anyone who might see officers using the equipment.

In Any Case, Disclosure of Responsive Records Are Definitively Not Controlled by the Arms Export Control Act or the Export Administration Act

11. Even if Stingrays were controlled by the AECA and the USML, as claimed by Agent Morrison, the disclosure of the records that are responsive to Petitioner's FOIL requests would not be covered by any export prohibitions.

12. Petitioner does not seek “equipment,” but rather records, and so the only possible export control relevant to Petitioner’s request would be the ITAR restriction on the export of “technical data.” 22 C.F.R. § 120.10(b); 22 C.F.R. § 120.6. With respect to “technical data” as opposed to equipment, ITAR restrictions only apply to “[i]nformation . . . required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles,” and this list does *not* include “basic marketing information on function or purpose or general system descriptions of defense articles” or various information that is already “published and which is generally accessible or available to the public.” 22 C.F.R. §§ 120.6, 120.10, 120.11. Information contained in a published U.S. patent is public domain and, therefore, not technical data controlled by the ITAR. *Id.* at § 120.11(a)(5).

13. Petitioner’s FOIL request does not seek any records that could possibly be categorized as “technical data” subject to ITAR restrictions, as claimed by Agent Morrison. Reports reflecting the number of times Stingrays have been used by Respondent, or Respondent’s internal policies regarding whether to seek warrants for their use, or records of cases in which Stingrays were used, for example, clearly do not constitute “technical data” restricted by ITAR. None of this information would even be useful to anyone seeking merely to

operate the device, much less to design, assemble or manufacture it. And even if the FOIL request resulted in some information about the operation or design of these units, it is unlikely that it would be information not already disclosed in the U.S. Patent application for the Stingray device.

14. In addition, assuming that Stingrays are classified under the Export Administration Act under ECCN 5A001, as I concluded above, the analogous controlled technology for that item—information which cannot be transferred to non-U.S. persons under the Export Administration Act—is classified as ECCN 5E001, which covers technology “for the ‘development’, ‘production’ or ‘use’ (excluding operation) of equipment . . . controlled by 5A001.” 15.C.F.R. Pt. 774, Supp. 1, Cat. 5. “Use,” when excluding “operation,” is limited to information regarding “installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing.” *See* 15 C.F.R. § 772.1 (definition of “use”). None of the information requested by Petitioner in this action could have any bearing on the development, production, installation, maintenance, repair, overhaul or refurbishing of Stingrays. Accordingly, the production of this information would not be prohibited under either regulatory regime.

Disclosure of Responsive Records to the NYCLU Would Not Constitute an “Export” Prohibited by the Arms Export Control Act

15. Similarly, even if Agent Morrison were correct in asserting that Stingrays are governed by the AECA and appear on the USML, which he is not, and even if responding to Petitioner’s requests would constitute “disclosing technical data,” which it would not, the disclosure of records to a U.S. FOIL litigant on United States soil would not be an “export.” *See* 22 C.F.R. § 120.17. The regulation defines “export” in the context of technical data as “disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad” *Id.* The NYCLU is not a foreign person because it is a

"U.S. person" as defined by the regulation. 22 C.F.R. § 120.15 (defining "U.S. person" to include "any corporation, business association, partnership, society, trust, or any other entity, organization or group that is incorporated to do business in the United States"); Certificates of Incorporation of New York Civil Liberties Union and New York Civil Liberties Foundation (incorporating in New York State and Delaware, respectively).

16. Agent Morrison suggests that the release of information to an American person who may, at some point in the future, possibly make it available to a foreign person in the context of a public disclosure, would be a constructive violation of ITAR. This does not appear to be based in any legal or practical application of ITAR of which I am aware.

Dated: Washington, D.C.
February 4, 2015

District of Columbia : 55

Robert Clifton Burns
Robert Clifton Burns

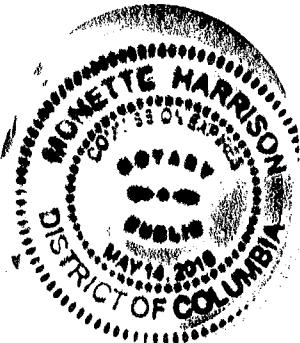
Signed and sworn to before me on 4th day of February
by Robert Clifton Burns.

Monette Harrison

Notary Public

My Commission Expires on 5/14/16

My Commission Expires
May 14, 2016



**CERTIFICATE OF CONFORMITY
PURSUANT TO CPLR 2309(c)
(OUT OF STATE NOTARIZATION)**

The undersigned does hereby certify that he is an attorney at law duly admitted to practice in the District of Columbia and is a resident of the District of Columbia; that he makes this affidavit in accordance with the requirements of the Clerk of the County of Erie pertaining to the acknowledgement of the proof of the Affidavit of Robert Clifton Burns, to be filed in Supreme Court, Erie County; that the foregoing acknowledgment of Robert Clifton Burns, named in the foregoing instrument taken before Monette Harrison, a Notary in the District of Columbia, being the place in which it was taken, and based upon my review thereof, appears to conform with the law of the District of Columbia as to the purpose for which it is submitted and filed.

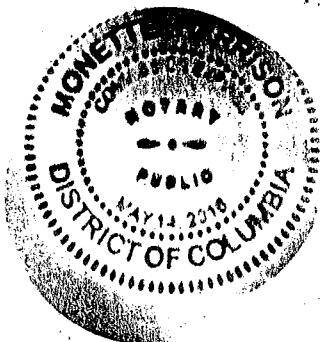


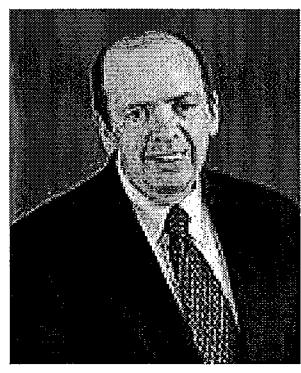
District of Columbia, SS

Sworn to before me this 4th day of February, 2015,

Monette Harrison
Notary Public

My Commission Expires: May 14, 2016





Robert Clifton Burns

*Counsel
Washington*

1155 F Street, N.W.
Suite 500
Washington, District of Columbia
20004-1357

Phone: 1 202 508 6067
Fax: 1 202 220 7367
email: clif.burns@bryancave.com

Clif Burns focuses his practice on international business transactions, export controls, economic sanctions, customs and international intellectual property matters. These transactions principally involve clients in high-tech industries including lasers, software, medical devices, telecommunications, B2B and B2C e-commerce and military equipment. In handling international business transactions, Mr. Burns advises clients on international sales of goods and services, cross-border distributorship agreements, licenses, joint ventures and mergers and acquisitions, along with required notifications under Exxon-Florio and Hart-Scott-Rodino. In addition, Mr. Burns represents a number of clients in international arbitration proceedings arising under the arbitration clauses commonly found in cross-border business agreements.

Mr. Burns' export control work encompasses a broad range of areas and includes matters involving the Export Administration Regulations (EAR) administered by the Department of Commerce, the International Traffic in Arms Regulations (ITAR) administered by the State Department and the country-based economic sanctions program administered by the Office of Foreign Assets Control of the Treasury Department. Mr. Burns also has broad experience in developing compliance programs for each of these three regulatory schemes, conducting due diligence for compliance with these schemes, and submitting voluntary disclosures of prior unlicensed exports. Customs matters have included registration and enforcement of intellectual property rights with the Customs Service and release of seized merchandise.

Companies represented by Mr. Burns are located in France, Germany, the Netherlands, Australia and the United States.

Mr. Burns speaks French fluently. Mr. Burns is currently an Adjunct Professor of Law at the Georgetown University Law Center. He was Editor-in-Chief of the Northwestern University Law Review and a law clerk for the Hon. Robert A.



Sprecher on the United States Court of Appeals for the Seventh Circuit.

Bar and Court Admissions

District of Columbia

United States Courts of Appeals for the Seventh and Federal Circuits
Court of Appeals, District of Columbia

Education

Northwestern University, J.D., *cum laude*, 1978

Northwestern University, B.A., with honors, 1975

Publications

- Export Law Blog
- "Weatherford Woes," *The Deal*, published, September 2007
- "Recent Developments Regarding DDTC's Rules on Brokering," *The International Lawyer*, Summer 2007
- "Going Bananas: Chiquita Tried to Protect Its Workers and Got Mashed by Prosecutors," *Legal Times*, published, April 2007
- "Turning Yourself In: Export Enforcement Trends," *Industry Week*, March 2007
- "Voluntary Disclosures of Export Violations," *The Corporate Counselor*, February 2007
- "Enforcement of ITAR Part 130 Adds Problems for Brokers," *The Export Practitioner*, December 2006
- "Expansion of Brokering Rules Gives Headaches to Exporters," *The Export Practitioner*, August 2006
- "Proof or Consequences: False Advertising and the Doctrine of Commercial Free Speech," 56, University of Cincinnati Law Review, 1988



Speeches and Seminars

- "Don't Get Left Behind: Implementing Export Control Reform," webinar, April 9, 2013 [Link to Webinar](#)
- Society for International Affairs, "Compliance Insiders: Industry Best Practices and Effective Tools," April 3, 2008.
- Journal of International Law Annual Symposium, "International Trade Sanctions," University of Pennsylvania Law School, February 29, 2008
- TRACE International, "ITAR Part 129 Compliance Issues," September 2005 and September 2006
- National Defense Industries Association, "Arbitration and Government Contracts," November 2005

Professional Affiliations

- District of Columbia Bar Association

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 12 of 12



ELECTRONICALLY FILED
7/2/2015 12:12 PM
UNITED STATES DEPARTMENT OF COMMERCE
Bureau of Industry and Security
Washington, D.C. 20230
CALENDAR: 11
PAGE 1 of 2
CIRCUIT COURT OF
COOK COUNTY, ILLINOIS
CHANCERY DIVISION
CLERK DOROTHY BROWN

MAR 27 2015

Mr. Matthew Topic
Loevy & Loevy
312 N. May Street, Suite 100
Chicago, IL 60607

Via electronic mail: matt@loevy.com

Subject: Freedom Of Information Act (FOIA) Request Re: BIS 15-031

Dear Mr. Topic:

This is in response to your February 9, 2015 amended Freedom of Information Act (FOIA), 5 U.S.C. § 552, request to the Department of Commerce's Bureau of Industry and Security (BIS) for aggregate data on "cell site simulators" or the Export Control Classification Numbers (ECCNs) that the product may fall under.

BIS has completed its review of your request. Without knowing specific technical details, it was determined that ECCN 5A001.f "Intercepting systems and equipment, communications" would be the most appropriate category where a cell site simulator may be filed. Our record shows that there were 14 responsive documents under this ECCN from 1/1/2007 to 12/31/2014. Specific information related to the 14 documents is exempt from disclosure under FOIA exemption (b)(3), specifically Section 12(c) of the Export Administration Act.

Exemption (b)(3) protects information "specifically exempted from disclosure by statute." The statutory provision that specifically exempts this information from disclosure by establishing particular criteria for withholding is Section 12(c) of the Export Administration Act of 1979, as amended (the "Act").¹ Section 12(c)(1) states, in pertinent part, that "information obtained for the purpose of, consideration of, or concerning, license applications under this Act shall be withheld from public disclosure unless the release of such information is determined by the Secretary to be in the national interest." This Section does not merely authorize maintaining the confidentiality of information obtained under the Act, but requires such information not be disclosed unless its release is determined to be in the national interest. In the absence of a national interest determination authorizing release of information responsive to your request and consistent with the criteria of Section 12(c), any such information cannot be released.

¹ Since August 21, 2001, the Act has been in lapse and the President, through Executive Order 13222 of August 17, 2001 (3 C.F.R. 2001 Comp. p. 783 (2002)), which has been extended by successive Presidential Notices, the most recent being that of August 7, 2014 (79 Fed. Reg. 46959 (Aug. 11, 2014)), continues the Regulations in effect under the International Emergency Economic Powers Act (50 U.S.C. §1701 et seq. (2000)).



Exhibit 1-AT

You have the right to appeal this denial of the FOIA request. An appeal must be received within 30 calendar days of the date of this response letter by the Assistant General Counsel for Administration (Office), Room 5898-C, U.S. Department of Commerce, 14th and Constitution Avenue, N.W., Washington, D.C. 20230. An appeal may also be sent by e-mail to FOIAAppeals@doc.gov, by facsimile (fax) to 202-482-2552, or by FOIAonline, if you have an account in FOIAonline, at: <https://foiaonline.regulations.gov/foia/action/public/home#>.

The appeal must include the following:

- A copy of the original FOIA request
- A copy of the agency response to the FOIA request
- A statement of the reason why the withheld records should be made available and why denial of the records was in error

The submission (including e-mail, fax, and FOIAonline submissions) is not complete without the required attachments. The appeal letter, the envelope, the e-mail subject line, and the fax cover sheet should be clearly marked "Freedom of Information Act Appeal."

The e-mail, fax machine, FOIAonline, and Office are monitored only on working days during normal business hours (8:30 a.m. to 5:00 p.m., Eastern Time, Monday through Friday). FOIA appeals posted to the e-mail box, fax machine, FOIAonline, or Office after normal business hours will be deemed received on the next normal business day. If the 30th calendar day for submitting an appeal falls on a Saturday, Sunday or legal public holiday, an appeal received by 5:00 p.m., Eastern Time, the next business day will be deemed timely.

If you have questions regarding this request, please contact Jennifer Kuo at (202) 482-0953 or via e-mail at jennifer.kuo@bis.doc.gov.

Sincerely,



Daniel O. Hill
Deputy Under Secretary
for Industry and Security

ELECTRONICALLY FILED
7/22/2015 12:12 PM
2014-CH-15338
PAGE 2 of 2

Law Offices

191 N. Wacker Drive
Suite 3700
Chicago, IL
60606-1698

(312) 569-1000
(312) 569-3000 fax
www.drinkerbiddle.com

CALIFORNIA
DELAWARE
ILLINOIS
NEW JERSEY
NEW YORK
PENNSYLVANIA
WASHINGTON D.C.
WISCONSIN

VIA E-MAIL

Matthew Topic
Loevy & Loevy
312 N. May Street
Suite 100
Chicago, Illinois 60607
matt@loevy.com

Re: NOTICE OF RESPONSE
REQUEST RECEIVED: December 31, 2014
FOIA FILE NO.: 15-0003

Dear Mr. Topic:

The City of Chicago has retained Drinker Biddle & Reath LLP to assist in responding to your Illinois Freedom of Information Act (“FOIA”) request received by the Chicago Police Department (“CPD”) on December 31, 2014, a copy of which is attached. During a January 13, 2015, telephone conversation, you agreed to extend CPD’s response date to January 22, 2015.

Your request has been reviewed by CPD and Drinker Biddle & Reath LLP, and documents responsive to your request have been searched for and/or produced by CPD, including by the Organized Crime Division, General Support Services Division, and Internal Affairs Division. Upon review, CPD hereby responds to your requests as follows:

1. *All attorney invoices and billing records for Martinez v. Chicago Police Department 2014 CH 15338 or the FOIA requests described therein.*

CPD does not have any documents responsive to this request.

2. *An inventory of everything kept and maintained by the Tech Lab for the past 10 years.*

CPD has been unable to locate a document that provides an inventory of everything kept and maintained by the Tech Lab for the past 10 years. Please note that while FOIA requires a public body, such as CPD, to produce documents, (*See 5 ILCS 140/3(a)* “Each public body shall make available to any person for inspection or copying all public records, except as otherwise provided in section 7 of this Act.”), FOIA does not require a public body to provide answers to questions or create documents. *See Chicago Tribune*

January 22, 2015

Matthew Topic

January 22, 2015

Page 2

Co. v. Dep't of Fin. & Prof'l Regulation, 2014 IL App. (4th) 130427, ¶ 33 (4th Dist. 2014); *Kenyon v. Garrels*, 184 Ill.App.3d 28, 32 (4th Dist. 1989).

Full or partial inventories for two individual years were located by CPD, but CPD does not understand these documents to be responsive to your request for an inventory of everything kept and maintained by the Tech Lab for the preceding ten years. If CPD has misinterpreted the scope of your request, please contact me to discuss.

3. *All logs or other such records showing the date and time any cell site simulator equipment was removed from and returned to the Tech Lab, by whom, the rank and assignment (bureau, division, section etc.) of the people checking out the equipment, and what equipment was checked out.*

CPD has been unable to locate any documents responsive to this request.

4. *The summary digests of all CRs involving Jack Costa.*

CPD has located records responsive to this request. However, the responsive records are exempt from disclosure pursuant to 5 ILCS 140/7(1)(a), which exempts from production "information specifically prohibited from disclosure by . . . State law." Attached are two orders issued by Judge Peter Flynn in *Fraternal Order of Police, Chicago Lodge No. 7, et al. v. City of Chicago, et al.*, No. 14 CH 17454, that prohibit CPD from producing summary digests of CRs more than four years old. The records responsive to this request are exempt from production pursuant to these orders because the records solely contain information that is more than four years in age.

5. *All records referencing both ITAR and cell site simulators or known alternative terms for those things (for example, IMSI catchers).*

The enclosed documents are responsive to this request.

Section 7(1) of FOIA provides that "[w]hen a request is made to inspect or copy a public record that contains information that is exempt from disclosure under this Section, but also contains information that is not exempt from disclosure, the public body may elect to redact the information that is exempt. The public body shall make the remaining information available for inspection and copying." Portions of the enclosed documents have been redacted under the following exemptions:

Section 7(1)(g) of FOIA exempts "[t]rade secrets and commercial or financial information obtained from a person or business where the trade secrets or commercial or financial information are furnished under a claim that they are proprietary, privileged or confidential, and that disclosure of the trade secrets or commercial or financial information would cause competitive harm to the person or business, and only insofar as the claim directly applies to the records requested." 5 ILCS 140/7(1)(g). The enclosed

documents contain third-party commercial and financial information obtained from a business under a claim that the information is confidential and proprietary. Accordingly, that commercial and financial information has been redacted.

Additionally, CPD has identified several documents that are potentially responsive to this request, including two Harris Corporation (“Harris”) operator manuals for cell site simulator equipment and Harris product descriptions (collectively, “the Harris documents”). However, the Harris documents are being withheld under the following exemptions:

Section 7(1)(a) of FOIA provides that “information specifically prohibited from disclosure by federal or State law or rules and regulations implementing federal or State law” is exempt from release under the Act. 5 ILCS 104/7(1)(a). The requested information is prohibited by the following federal law:

22 U.S.C. § 2778. The Arms Export Control Act and implementing regulations restrict the dissemination of technical information relating to regulated defense articles, which includes the equipment that is the subject of your request. Specifically, technical information for cell site simulator equipment is subject to the non-disclosure provisions of the International Traffic in Arms Regulations (ITAR), 22 C.F.R. Parts 120-130.

Technical information need not leave the borders of the United States to be deemed an export. Providing technical information without a license to anyone intending to publicize the information would constitute a violation of the Arms Export Control Act. The Harris documents contain technical information regarding the capabilities, operation, and use of cell site simulator technology. Accordingly, disclosure of the Harris documents is prohibited by ITAR.

Section 7(1)(d)(v) of FOIA exempts documents that “disclose unique or specialized investigation techniques other than those generally used and known. . . .” 5 ILCS 140/7(1)(d)(v). The Harris documents disclose information regarding a unique and specialized investigative technique not otherwise known to members of the public, namely, the specific capabilities, settings, limitations, and deployment of cell site simulator equipment.

Section 7(1)(g) of the Illinois FOIA exempts “[t]rade secrets and commercial or financial information obtained from a person or business where the trade secrets or commercial or financial information are furnished under a claim that they are proprietary, privileged or confidential, and that disclosure of the trade secrets or commercial or financial information would cause competitive harm to the person or business, and only insofar as the claim directly applies to the records requested.” 5 ILCS 140/7(1)(g). The Harris documents responsive to this portion of your FOIA request are being withheld as they contain trade secrets and commercial information obtained from Harris under a claim that

Matthew Topic

January 22, 2015

Page 4

they are proprietary information, the disclosure of which would cause competitive harm. Attached please find an affidavit from Harris explaining its position regarding the documents it provided to CPD that are responsive to your FOIA request.

Section 7(1)(i) of the Illinois FOIA exempts “[v]aluable formulae, computer geographic systems, designs, drawings and research data obtained or produced by any public body when disclosure could reasonably be expected to produce private gain or public loss. . . .” 5 ILCS 140/7(1)(i). The Harris documents, which include information regarding the specific capabilities, settings, limitations, and deployment of cell site simulator equipment, contain information exempt under this provision.

Section 7(1)(v) of the Illinois FOIA exempts “[v]ulnerability assessments, security measures, and response policies or plans that are designed to identify, prevent, or respond to potential attacks upon a community’s population or systems, facilities, or installations, the destruction or contamination of which would constitute a clear and present danger to the health or safety of the community. . . .” 5 ILCS 140/7(1)(v). The Harris documents describe the specific capabilities, settings, limitations, and deployment of cell site simulator equipment, all of which may reveal security measures used by law enforcement in the detection, prevention and response to acts and potential acts of violence and terrorism. Thus, the documents contain information exempt under this provision.

Very truly yours,


Jeff Perconte

JP/das
Enclosure

You have the right of review of this denial by the Illinois Attorney General’s Public Access Counselor (PAC). You can file a request for review by writing to:

Public Access Counselor
Office of the Attorney General
500 2nd Street
Springfield, Illinois 62706

You may also seek judicial review of a denial under 5 ILCS 140/11 by filing a lawsuit in the State Circuit Court.

FOIA request

Matt Topic [matt@loevy.com]

Sent: Wednesday, December 31, 2014 3:54 PM

To: FOIA

Cc: Collins, Daniel J. [Daniel.Collins@dbr.com]; Freddy M [freddyinchicago@gmail.com]

My client, Freddy Martinez, requests PDF copies of the following records to be delivered to me by email to this address, or if that is not feasible, by a mutually agreeable alternative mechanism of delivery (please contact me to discuss if needed):

1. All attorney invoices and billing records for Martinez v. Chicago Police Department 2014 CH 15338 or the FOIA requests described therein.
2. An inventory of everything kept and maintained by the Tech Lab for the past 10 years.
3. All logs or other such records showing the date and time any cell site simulator equipment was removed from and returned to the Tech Lab, by whom, the rank and assignment (bureau, division, section etc.) of the people checking out the equipment, and what equipment was checked out.
4. The summary digests of all CRs involving Jack Costa.
5. All records referencing both ITAR and cell site simulators or known alternative terms for those things (for example, IMSI catchers).

This is not a commercial request. Please do not communicate with me through any means other than by email to this email address.

Matthew Topic
Loevy & Loevy

312 N. May Street, Suite 100
Chicago, IL 60607
312-789-4973 (office)
773-368-8812 (cell)
matt@loevy.com

FREDDY MARTINEZ,)
)
Plaintiff,) 2014 CH 15338
)
v.) Hon. Kathleen Kennedy
)
CHICAGO POLICE DEPARTMENT,)
)
Defendant.)

DECLARATION OF BRIAN L. OWSLEY

1. My name is Brian L. Owsley.
2. In 1988, I graduated from the University of Notre Dame with honors earning a Bachelor's of Arts. In 1993, I graduated from Columbia University School of Law with a Juris Doctorate where I was a Harlan Fiske Stone Scholar. A copy of my curriculum vitae is attached as Exhibit A.
3. From May 2005 through May 2013, I served as a United States Magistrate Judge in the Corpus Christi Division of the United States District Court for the Southern District of Texas. As part of my duties, I received applications and issued orders concerning all manner of requests for electronic surveillance, including applications for pen registers as well as cell site simulators.
4. Since leaving the bench, I have taught law. First, I served as a Visiting Assistant Professor of Law at the Texas Tech University School of Law for the 2013-2014 academic year. Then, I taught as an Assistant Professor of Law in a tenure track position at the Indiana Tech Law School for the 2014-2015 academic year. Finally, I will begin a new tenure-track position as an Assistant Professor of Law at the University of North Texas – Dallas College of Law for the 2015-2016 academic year.
5. In my legal scholarship, I research and write about a number of topics related to electronic surveillance, most notably issues about cell site simulators and greater transparency in the process of electronic surveillance applications and orders. For example, I have published *TriggerFish, StingRays and Fourth Amendment Fishing Expeditions*, 66 Hastings L.J. 183 (2014), which was the first law review article to focus on the growing use of cell site simulators. I also wrote *Spies in the Skies: Dirtboxes and Airplane Electronic Surveillance*, 113 Mich. L. Rev. First Impressions 75 (2015), which concerns about the use of cell site simulators mounted on aircraft. Additionally, I published *To Unseal or Not to Unseal: The Judiciary's Role in Preventing Transparency in Electronic Surveillance Applications and Orders*, 5 Calif. L. Rev. Circuit 259 (2014), which raised concerns about the need to unseal these files. Copies of these articles are attaches as Exhibits B-D hereto and incorporated by reference into my declaration.

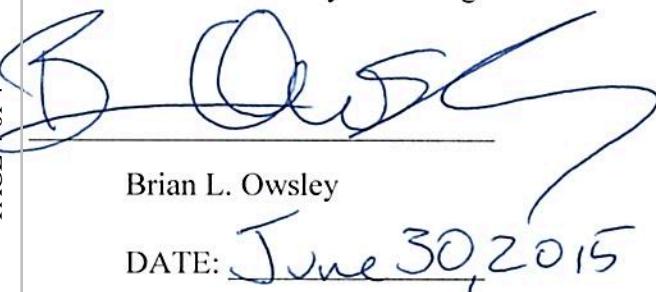
6. Since entering legal academia, I have also been quoted extensively in numerous media outlets regarding cell site simulators. Moreover, I testified about cell site simulators before the Oversight Committee of the Michigan House of Representatives.
7. There is no federal statute addressing the use of cell site simulators. Similarly, there are very few state statutes authorizing the use of cell site simulators, including no Illinois statute of which I am aware.
8. A pen register is a specific device that enables law enforcement officials to receive the outgoing dialed telephone numbers from a known telephone number. In other words, the law enforcement official must provide the judicial officer with a specific telephone number in order to obtain a pen register for that telephone number. In turn, the law enforcement official must take the court order to the telecommunications provider to obtain the list of the outgoing dialed telephone numbers.
9. A cell site simulator is a device that operates much differently than a pen register. Cell phones operate by connecting with the nearest cell phone tower in the cell phone user's telecommunications network. That cell phone tower in turn relays any telephone call along a series of towers and equipment in order to complete the telephone call. When a cell phone is on, it periodically seeks out the nearest cell phone tower with the strongest signal to register with the tower so that the phone can signal its capability to receive any telephone calls, text messages, emails, or other data.
10. A cell site simulator functions by mimicking a cell tower for the cell phones surrounding it and forcing those phones to connect with the simulator instead of the legitimate towers. As these cell phones connect with the cell site simulator, the device captures the data, including the cell phone's geographical location, its telephone number, and its International Mobile Subscriber Identity, which is a unique identification number. This capture of data occurs very quickly and once completed the cell site simulator releases the cell phone, which in turn connects with the nearest cell phone tower with the strongest signal.
11. Certain cell site simulators can also capture the content of calls, text messages, numbers dialed, and web pages visited.
12. Unlike pen registers, cell site simulators are used without the phone carrier's knowledge or assistance.
13. State court judges in Tacoma, Washington learned in 2014 that the pen register applications presented to them by Tacoma detectives, which contained no mention of cell site simulator technology, were used for cell site simulators. The court ultimately changed its procedures to require greater disclosure in applications for use of cell site simulators.
14. Law enforcement officials have let accused criminals go free or plead to reduced sentences rather than disclose details about the role that cell site simulators played in an investigation.
15. Law enforcement typically uses cell site simulators in three different ways. Each way has a different level of invasiveness.
16. First, law enforcement officials may use the cell site simulator with the known cell phone number of a targeted individual in order to determine that individual's location. For

- example, officials are searching for a fugitive and have a cell phone number that they believe the individual is using. They may operate a cell site simulator near areas where they suspect the individual may be such as a relative's residence.
17. Second, law enforcement officials may use the cell site simulator to target a specific individual who is using a cell phone, but these officials do not know the cell phone number. They follow the targeted individual from a residence to various other locations over a day or longer time period. At each new location, they activate the cell site simulator and capture the cell phone data for all of the nearby cell phones. After they have captured the data at a number of sites, they can analyze the data in hopes of determining the cell phone or cell phones used by the targeted individual. This approach captures the data of all nearby cell phones, including countless cell phones of individuals unrelated to the criminal investigation.
 18. Third, anecdotal evidence suggests that law enforcement have used cell site simulators at large gatherings, such as political rallies and protests. Using the devices at these types of events would allow law enforcement to capture the cell phone data of everyone who has attended the event and create databases of political activists.
 19. In the latter two examples, law enforcement officials do not know the cell phone number of the targeted cell phones, but instead are seeking to obtain cell phone numbers. In the first example, while the officials may know the targeted individual's cell phone number, they are not seeking a list of outgoing dialed telephone numbers, but the targeted individual's cell phone number. Each of these three examples of typical usage of a cell site simulator fall outside the scope of a pen register, and thus in my opinion the use of a pen register statute to obtain authorization for usage of a cell site simulator is improper.
 20. Given the inapplicability of a pen register statute to authorizing a cell site simulator, a basis must be determined for authorizing such usage. In the absence of any specific statutory authority, in my opinion, the proper basis should be the Fourth Amendment of the United States Constitution based on a probable cause standard.
 21. In my opinion, the lack of transparency regarding the applications and orders for electronic surveillance, including cell site simulators, is a significant problem in a free society.
 22. In espousing this opinion, I fully recognize the need to initially seal such applications and orders. This sealing is often necessary to protect ongoing criminal investigations as well as innocent individuals. However, the continued sealing of these documents without any consideration of when to unseal them is a large problem that does not need to exist.
 23. Fortunately, there are many solutions and approaches to handle this problem. First, as a general rule, the documents should be unsealed after the statute of limitations for the crime that is being investigated has lapsed.
 24. Second, as a general rule, the documents should be unsealed after the targeted individual has been convicted and exhausted all of his criminal appeals.
 25. Third, even when unsealing a document fully may not be appropriate because of the timing or the nature of the targeted individual, the appropriate course is not to continue sealing the documents, but instead to redact the problematic name or other information. This redaction should be as minimally applied as necessary to achieve the goal of

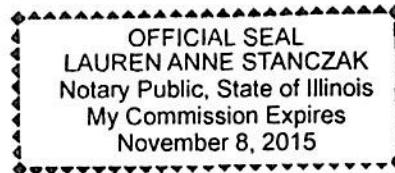
safeguarding the sensitive information. The rest of the document should be unsealed and available to the public.

26. This transparency is important because the public needs to be certain that electronic surveillance is being done in a manner in which individual privacy is not being sacrificed at the expense of the significant goal of criminal prosecutions. In order to ensure that the public has this critical information, courts must refrain from routinely sealing these documents so that the public has access to this information.
27. Technology already exists that allows a cell phone user to determine whether his or her cellular phone is connected to a cell site simulator.
28. To develop countermeasures to counteract the efficacy of a cell site simulator, one would need more information than is typically disclosed in a pen register application or order. The general capabilities of cell site simulators are already common knowledge, and criminals inclined to take countermeasures already have access to information making clear that law enforcement is capable of tracking them through their cellular phones.

Under penalty of perjury, I affirm that the statements in this declaration are true and correct to the best of my knowledge.



Brian L. Owsley
DATE: June 30, 2015



Brian L. Owsley

1901 Main Street
 University of North Texas-Dallas College of Law
 Dallas, Texas 75201
 214-243-1774
 brian.owsley@untsystem.edu

ACADEMIC EXPERIENCE

University of North Texas – Dallas College of Law	Dallas, TX
Assistant Professor	July 2015—present
I will teach Torts and Constitutional Law in the spring and fall semesters.	
 Indiana Tech Law School	 Fort Wayne, IN
Assistant Professor	July 2014—July 2015
I taught Criminal Law and Professional Responsibility in the fall semester as well as Torts and Legal Ethics in the spring semester.	
 Texas Tech University School of Law	 Lubbock, TX
Visiting Assistant Professor	August 2013—May 2014
I taught Torts and Professional Responsibility in the fall semester and taught Professional Responsibility and Employment Law in the spring semester.	
 Columbia University School of International and Public Affairs	 New York, NY
Teaching Assistant	Fall 1993
I served as a Teaching Assistant for Professor Louis Henkin's International Law course. I conducted a weekly review session to address the week's lectures and I graded the final examinations.	

EDUCATION

Columbia University School of International and Public Affairs	New York, NY
M.I.A., received May 1994	GPA: 3.25/4.0
 Columbia University School of Law	
J.D., received May 1993	Harlan Fiske Stone Scholar
Certificate with honors - Parker School of Foreign and Comparative Law	
Columbia Human Rights Law Review	1991-1993
Executive Editor	1992-1993
Black Law Students Association	
Columbia Society of International Law	
Columbia Journal of Gender and Law	1991-1993
 UNIVERSITY OF NOTRE DAME	
B.A., received with honors, May 1988	GPA: 3.42/4.0
Majors: Program of Liberal Studies & Government	

LEGAL EXPERIENCE

United States District Court for the Southern District of Texas	Corpus Christi, TX
United States Magistrate Judge	May 2005—May 2013
Presided over civil consent trials and criminal misdemeanor trials; conducted initial appearances, preliminary hearings, detention hearings, arraignments, suppression hearings and other criminal proceedings; took guilty pleas and sentenced criminal misdemeanor defendants; issued orders and memoranda and recommendations; resolved discovery disputes; and conducted mediation proceedings.	

United States Department of Justice Trial Attorney	Washington, DC September 2001—May 2005
Served as lead attorney in complex litigation cases; supervised teams of trial attorneys, paralegals, consultants and experts; argued motions in the Court of Federal Claims and appeals in the Federal Circuit; took and defended expert and fact witness depositions; examined and cross-examined trial witnesses; supervised and conducted discovery; researched and drafted motions, pleadings, and briefs on behalf of the Commercial Litigation Branch in the Civil Division.	
Ross, Dixon & Bell, L.L.P. Associate	Washington, DC November 1999—August 2001
Researched and drafted legal memoranda, complaints, motions, and briefs regarding civil claims and insurance matters; engaged in and prepared discovery; deposed witnesses; attended trial court hearings; attended settlement negotiations; analyzed insurance claims; determined coverage positions for insurer clients; monitored insurance defense counsel.	
United States Equal Employment Opportunity Commission General Attorney	Washington, DC September 1997—November 1999
Researched and drafted legal memoranda, motions and briefs on behalf of the Office of the General Counsel, primarily in federal appellate courts; argued appeals; negotiated settlement agreements.	
Southern Poverty Law Center Law Fellow	Montgomery, AL September 1996—August 1997
Researched and drafted legal memorandum, met and discussed matters with clients, and drafted complaints.	
United States Court of Appeals for the Sixth Circuit Law Clerk for the Honorable Martha Craig Daughtrey	Nashville, TN September 1995—August 1996
Human Rights Watch Leonard H. Sandler Fellow	New York, NY September 1994—September 1995
Middle East Division, focusing primarily on Iraq and Iran. Established a network of contacts, monitored daily human rights situation, engaged in advocacy, and wrote and edited reports, press releases, and letters; participated in a human rights mission to Sudan to examine human rights abuses, including the effects of the civil war; interviewed victims of human rights violations and government officials; and planned and conducted a mission in Amman, Jordan focusing on human rights violations in Iraq, especially freedom of expression.	
United States District Court for the Southern District of Texas Law Clerk for the Honorable Janis Graham Jack	Corpus Christi, TX May 1994—August 1994
Simpson Thacher & Bartlett Summer Associate	New York, NY Summer 1993
Rogers & Wells Summer Associate	New York, NY Summer 1992
Kituo Cha Sheria Human Rights Legal Intern	Nairobi, Kenya Summer 1991

LAW REVIEW PUBLICATIONS

Supreme Court Jurisprudence of the Personal in City of Los Angeles v. Patel, 114 Mich. L. Rev. First Impressions _ (forthcoming 2015).

Cell Site Simulators and the Fourth Amendment, 43 Search & Seizure L. Rep. _ (forthcoming 2015).

Spies in the Skies: Dirtboxes and Airplane Electronic Surveillance, 113 Mich. L. Rev. First Impressions 75 (2015).

Beware of Government Agents Bearing Trojan Horses, 48 Akron L. Rev. __ (forthcoming 2015).

Drug Sniffing Dogs and the Fourth Amendment, 42 Search & Seizure L. Rep. 37 (2015).

TriggerFish, StingRays and Fourth Amendment Fishing Expeditions, 66 Hastings L.J. 183 (2014).

Distinguishing Immigration Violations from Criminal Violations: A Discussion Raised by Justice Sonia Sotomayor, 163 U. Pa. L. Rev. Online 1 (2014).

To Unseal or Not to Unseal: The Judiciary's Role in Preventing Transparency in Electronic Surveillance Applications and Orders, 5 Calif. L. Rev. Circuit 259 (2014).

The Supreme Court Goes to the Dogs: Reconciling Florida v. Harris and Florida v. Jardines, 77 Alb. L. Rev. 349 (2014).

The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance, 16 U. Pa. J. Const. L. 1 (2013).

Cops and Robbers: The Use of Cell Tower Dumps to Investigate Bank Robberies, Am. Crim. L. Rev. (Jan. 26, 2013), <http://www.americancriminallawreview.com/aclr-online/cops-and-robbers-use-cell-tower-dumps-investigate-bank-robberies/>

Issues Concerning Charges for Driving While Intoxicated in Texas Federal Courts, 42 St. Mary's L.J. 411 (2011).

Survivorship Claims Under Employment Discrimination Statutes, 69 Miss. L.J. 423 (1999).

Black Ivy: An African-American Perspective on Law School, 28 Colum. Hum. Rts. L. Rev. 501 (1997).

Ethnic Vietnamese in Cambodia: A Case Study of the Tension Between Foreign Policy and Human Rights, 6 Touro Int'l L. Rev. 377 (1995).

Landmines and Human Rights: Holding Producers Accountable, 21 Syracuse J. Int'l L. & Com. 101 (1995).

Racist Speech and 'Reasonable' People, 24 Colum. Hum. Rts. L. Rev. 323 (1993).

OTHER PUBLICATIONS

Written Statement, "Hearing on Hailstorm/Stingray type surveillance devices" Michigan House of Representatives, Oversight Committee Meeting (Lansing, Michigan, May 13, 2014), available at <http://house.mi.gov/sessiondocs/2013-2014/testimony/Committee237-5-13-2014.pdf>.

Iraq Chapter of *Human Rights Watch World Report 1996* (New York: Human Rights Watch, December 1995).

Human Rights Watch/Middle East, *Iraq's Brutal Decrees: Amputation, Branding and the Death Penalty* (New York: Human Rights Watch, June 1995).

Iraq Chapter of *Human Rights Watch World Report 1995* (New York: Human Rights Watch, December 1994).

WORKS IN PROGRESS

Facebook, the Judiciary, and Ethical Considerations.

Cell Phones Tracking in the Era of United States v. Jones and Riley v. California.

PRESENTATIONS

Commentator, “Surveillance Discretion: Automated Suspicion and the Fourth Amendment” by Elizabeth Joh, Privacy Law Scholars Conference, (Berkeley, California, June 4, 2015)

“What is (should be) the scope and limitation of police power to track suspects?” Texas Tech University School of Law Criminal Law Symposium, “The 4th Amendment in the 21st Century” (Lubbock, Texas, April 17, 2015).

“Criminal: Hot Topics in E-Surveillance,” United States District Court for the Northern District of California 2015 Judicial Conference (Napa, California, March 28, 2015).

“Ethical Considerations Regarding Social Media,” 2014 Annual Hot Topics for Indiana Lawyers, Allen County Indiana Bar Association (Fort Wayne, Indiana, October 29, 2014).

“Ethical Considerations Regarding Contacts with Unrepresented Persons,” Ninth Annual Faculty Update for Legal Services Attorneys, Public Interest Practitioners & *Pro Bono* Attorneys, Texas Tech University School of Law (Lubbock, Texas, October 24, 2014).

“Facebook, the Judiciary, and Ethical Considerations,” University of Missouri School of Law, Judicial Education and the Art of Judging, Works-in-Progress Conference, (Columbia, Missouri, Oct. 9, 2014).

Panel Discussant, “Transparency in the Open Government Era,” Southeastern Association of Law Schools, 2014 Annual Conference (Amelie Island, Florida, August 7, 2014).

Moderator, “Alumni and Former Law Clerk Panel,” Second Annual Judicial Clerkship and Internship Training Academy, Texas Tech University School of Law (Lubbock, Texas, April 5, 2014).

“Ethics of Witness Preparation,” Eighth Annual Faculty Update for Legal Services Attorneys, Public Interest Practitioners & *Pro Bono* Attorneys, Texas Tech University School of Law (Lubbock, Texas, October 25, 2013).

“Catching a TriggerFish or a StingRay: The Government’s Secretive Electronic Surveillance Technique,” Southeastern Law Scholars Conference, Charleston School of Law (Charleston, South Carolina, October 5, 2013).

Panelist, “Ethics for Law Clerks,” Judicial Clerkship and Internship Training Academy, Texas Tech University School of Law (Lubbock, Texas, April 20, 2013).

Panelist, “Cellular phones and mobile privacy: Direct government surveillance (Stingrays),” Yale Information Society Project: Location Tracking and Biometrics Conference (New Haven, Connecticut, March 3, 2013).

Panelist, “Baseball with the Bench” (discussing practice in federal courts), Corpus Christi Young Lawyers Association (Corpus Christi, Texas, June 16, 2011).

Panelist, “Baseball with the Bench” (discussing practice in federal courts), Corpus Christi Young Lawyers Association (Corpus Christi, Texas, May 28, 2009).

“DWI in the Federal Venue” Corpus Christi Bar Association (Corpus Christi, Texas, April 17, 2009).

Panelist, “Baseball with the Bench” (discussing practice in federal courts), Corpus Christi Young Lawyers Association (Corpus Christi, Texas, June 5, 2008).

Panelist, “Baseball with the Bench” (discussing practice in federal courts), Corpus Christi Young Lawyers Association (Corpus Christi, Texas, June 21, 2007).

“Criminal Practice in Federal Magistrate Court” Corpus Christi Bar Association (Corpus Christi, Texas, May 18, 2007).

ACADEMIC SERVICE

Indiana Tech Law School

Appointments Committee
Diversity Committee
Library Committee
Faculty Advisor: Black Law Students Association

Texas Tech University School of Law

Judicial Clerkship Committee

MEDIA COMMENTARY

Eric Markowitz & Jeff Stone, “This New Tech Is Making Prison Inmates Flush Their Smuggled Cell Phones Down Toilets,” International Business Times, June 26, 2015, available at <http://www.ibtimes.com/new-tech-making-prison-inmates-flush-their-smuggled-cell-phones-down-toilets-1985511> (quoted).

Larry Greenemeier, “What is the Big Secret Surrounding Stingray Surveillance,” Scientific American, June 25, 2015, available at <http://www.scientificamerican.com/article/what-is-the-big-secret-surrounding-stingray-surveillance/> (interview).

Ross Todd, “Koh Takes Up Hot Topic in Cell Phone Surveillance,” The Recorder, June 4, 2015, available at <http://www.therecorder.com/id=1202728446200/Koh-Takes-Up-Hot-Topic-in-Cell-Phone-Surveillance?slreturn=20150516154008> (quoted).

Cyrus Farivar, “County sheriff has used stingray over 300 times with no warrant,” Ars Technica, May 24, 2015, available at <http://arstechnica.com/tech-policy/2015/05/county-sheriff-has-used-stingray-over-300-times-with-no-warrant/> (quoted).

Cyrus Farivar, “In rare move Silicon Valley county gov’t kills stingray acquisition,” Ars Technica, May 7, 2015, available at <http://arstechnica.com/tech-policy/2015/05/in-rare-move-silicon-valley-county-govt-kills-stingray-acquisition/> (quoted).

Cyrus Farivar, “DEA, US Army bought \$1.2M worth of hacking tools in recent years,” Ars Technica, Apr. 16, 2015, available at <http://arstechnica.com/tech-policy/2015/04/dea-us-army-bought-1-2m-worth-of-hacking-tools-in-recent-years/> (quoted).

Jessica Glenza & Nicky Woolf, “Stingray spying: FBI’s secret deal with police hides phone dragnet from courts,” The Guardian, April 10, 2015, available at <http://www.theguardian.com/us-news/2015/apr/10/stingray-spying-fbi-phone-dragnet-police> (quoted).

Justin Fenton, “Baltimore Police used secret technology to track cellphones in thousands of cases,” The Baltimore Sun, April 9, 2015, available at <http://www.baltimoresun.com/news/maryland/baltimore-city/bsmd-ci-stingray-case-20150408-story.html#page=1> (quoted).

Cyrus Farivar, “To explain stingrays, local cops cribbed letter pre-written by FBI,” Ars Technica, Mar. 24, 2015, available at <http://arstechnica.com/tech-policy/2015/03/to-explain-stingrays-local-cops-cribbed-letter-likely-pre-written-by-feds/> (quoted).

Karen Chen, “ACLU and others want to know more about cell phone technology HPD is using,” Houston Chronicle, Feb. 27, 2015, available at <http://www.houstonchronicle.com/news/houston-texas/houston/article/ACLU-and-others-want-to-know-more-about-cell-6106414.php?t=d980ceb3eaec4584b7&cmpid=twitter-premium> (quoted).

Cyrus Farivar, “Cops get handheld radar that can ‘detect people breathing’ through walls,” Ars Technica, Jan. 21, 2015, available at <http://arstechnica.com/tech-policy/2015/01/cops-get-handheld-radar-that-can-detect-people-breathing-through-walls/> (quoted).

Fred Clasen-Kelly, “Charlotte-Mecklenburg police cellphone surveillance records sought,” The Charlotte Observer, Nov. 2, 2014, available at <http://www.charlotteobserver.com/news/local/article9226817.html> (quoted).

Cyrus Farivar, “Florida court: Come back with a warrant to track suspects via mobile phone,” Ars Technica, Oct. 20, 2014, available at <http://arstechnica.com/tech-policy/2014/10/florida-court-come-back-with-a-warrant-to-track-suspects-via-mobile-phone/> (quoted).

Michael Siconolfi, “Long-Term Secrecy Surrounds Electronic Monitoring,” The Wall Street Journal, Sept. 30, 2014, available at <http://online.wsj.com/articles/long-term-secrecy-surrounds-electronic-monitoring-1412118727?KEYWORDS=secrecy> (quoted).

Cyrus Farivar, “NSA built ‘Google-like’ interface to scan 850+ billion metadata records,” Ars Technica, Aug. 25, 2014, available at <http://arstechnica.com/tech-policy/2014/08/nsa-built-google-like-interface-to-scan-850-billion-metadata-records/> (quoted).

Ryan Gallagher, “The Surveillance Engine: How the NSA Built Its Own Secret Google,” The Intercept, Aug. 25, 2014, available at <https://firstlook.org/theintercept/article/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/> (quoted).

Cyrus Farivar, “Rare cop-owned drone could fly over California in Bay Area soon,” Ars Technica, July 30, 2014, available at <http://arstechnica.com/tech-policy/2014/07/rare-cop-owned-drone-in-california-could-fly-over-bay-area-soon/> (quoted).

Cyrus Farivar, “Courts may hear challenges to secret cell tracking devices after new ruling,” Ars Technica, June 25, 2014, available at <http://arstechnica.com/tech-policy/2014/06/courts-may-hear-challenges-to-secret-cell-tracking-devices-after-new-scotus-ruling/> (quoted).

Craig Timberg, “Supreme Court cellphone ruling hints at broader curbs on surveillance,” The Washington Post, June 25, 2014, available at http://www.washingtonpost.com/business/technology/supreme-court-cellphone-ruling-hints-at-broader-curbs-on-surveillance/2014/06/25/2732b532-fc9b-11e3-8176-f2c941cf35f1_story.html (quoted).

Cyrus Farivar, “Illinois buys cell-tracking gear complete with NDAs, no bid process,” Ars Technica, June 21, 2014, available at <http://arstechnica.com/tech-policy/2014/06/illinois-spent-over-250000-on-covert-cellular-tracking-equipment/> (quoted).

Cyrus Farivar, “Legal experts: Cops lying about cell tracking ‘is a stupid thing to do,’” Ars Technica, June 20, 2014, available at <http://arstechnica.com/tech-policy/2014/06/legal-experts-cops-lying-about-cell-tracking-is-a-stupid-thing-to-do/> (quoted).

Tim Cushing, “Michigan State Politicians Looking Into Sheriff Department’s Use Of A Cell Tower Spoof,” Techdirt, June 9, 2014, *available at* <https://www.techdirt.com/articles/20140517/07153627270/michigan-state-politicians-looking-into-sheriff-departments-use-cell-tower-spoof.shtml> (quoted).

Jennifer Valentino-Devries, “Sealed Court Files Obscure Rise in Electronic Surveillance,” The Wall Street Journal, June 3, 2014, at 1, *available at* <http://online.wsj.com/articles/sealed-court-files-obscure-rise-in-electronic-surveillance-1401761770> (quoted).

Cyrus Farivar, “Dow Jones asks court to unseal long-completed digital surveillance cases,” Ars Technica, June 3, 2014, *available at* <http://arstechnica.com/tech-policy/2014/06/dow-jones-asks-court-to-unseal-long-completed-digital-surveillance-cases/>.

Brian Fung, “How hard should it be for cops to track your location? A new lawsuit revives the debate,” The Washington Post, June 3, 2014, *available at* <http://www.washingtonpost.com/blogs/the-switch/wp/2014/06/03/how-hard-should-it-be-for-cops-to-track-your-location-a-new-lawsuit-revives-the-debate/> (quoted).

John Turk, “Experts question transparency of cell phone tracking device owned by Sheriff’s Office at legislative hearing,” Macomb Daily News, May 16, 2014, *available at* <http://www.macombdaily.com/general-news/20140516/experts-question-transparency-of-cell-phone-tracking-device-owned-by-sheriffs-office-at-legislative-hearing> (quoted).

Lauren Abdel-Razzaq, “Cellphone tracker use lacks oversight, Michigan lawmakers told,” The Detroit News, May 13, 2014, *available at* <http://www.detroitnews.com/article/20140513/POLITICS02/305130093/Cellphone-tracker-use-lacks-oversight-Michigan-lawmakers-told> (quoted).

Paul Cicchini, “Spying on the Bad Guys or Invading Your Privacy?” Fox 17, May 13, 2014, *available at* <http://www.fox17online.com/2014/05/13/spying-on-the-bad-guys-or-invading-your-privacy/#axzz3lugASWlr> (quoted).

Ellen Nakashima, “FBI wants easier process to hack suspects’ computers,” The Washington Post, May 9, 2014, *available at* http://www.washingtonpost.com/world/national-security/fbi-wants-easier-process-to-hack-suspects-computers/2014/05/09/f30c37b0-d78d-11e3-8a78-8fe50322a72c_story.html (quoted).

Ann E. Marimow & Craig Timberg, “Low-level federal judges balking at law enforcement requests for electronic evidence,” The Washington Post, Apr. 24, 2014, *available at* http://www.washingtonpost.com/local/crime/low-level-federal-judges-balking-at-law-enforcement-requests-for-electronic-evidence/2014/04/24/eec81748-c01b-11e3-b195-dd0c1174052c_story.html (quoted).

Ellen Nakashima, “Agencies collected data on Americans’ cellphone use in thousands of ‘tower dumps,’” Washington Post, Dec. 8, 2013, *available at* http://www.washingtonpost.com/world/national-security/agencies-collected-data-on-americans-cellphone-use-in-thousands-of-tower-dumps/2013/12/08/20549190-5e80-11e3-be07-006c776266ed_story.html (quoted).

John Kelly, “Cellphone data spying: It’s not just the NSA,” USA Today, Dec. 8, 2013, *available at* <http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/> (quoted).

Craig Timberg & Ellen Nakashima, “FBI’s search for ‘Mo,’ suspect in bomb threats, highlights use of malware for surveillance,” The Washington Post, Dec. 5, 2013, *available at* http://www.washingtonpost.com/business/technology/fbis-search-for-mo-suspect-in-bomb-threats-highlights-use-of-malware-for-surveillance/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html (quoted).

Channel 9 (Denver NBC Affiliate), “Ridgeway case highlight data collection,” Nov. 20, 2013, available at <http://www.9news.com/video/default.aspx?bctid=2854882216001> (quoted).

Nate Anderson, “How ‘Cell Tower Dumps’ caught the High Country Bandits—and why it matters,” Ars Technica, Aug. 29, 2013, available at <http://arstechnica.com/tech-policy/2013/08/how-cell-tower-dumps-caught-the-high-country-bandits-and-why-it-matters/> (quoted).

Ellen Nakashima, “Little-known surveillance tool raises concerns by judge, privacy activists,” The Washington Post, Mar. 27, 2013, available at http://articles.washingtonpost.com/2013-03-27/world/38070419_1_magistrate-judge-federal-agents-stingrays (quoted).

Jennifer Valentino Devries, “Judge Questions Tools That Grab Cellphone Data on Innocent People,” The Wall Street Journal Law Blog, Oct. 22, 2012, available at <http://blogs.wsj.com/digits/2012/10/22/judge-questions-tools-that-grab-cellphone-data-on-innocent-people/> (quoted).

Ellen Nakashima, “Cellphone Tracking Powers on Request,” The Washington Post, Nov. 23, 2007, available at <http://www.washingtonpost.com/wp-dyn/content/article/2007/11/22/AR2007112201444.html> (quoted).

TESTIMONY

“Hearing on Hailstorm/Stingray type surveillance devices” Michigan House of Representatives, Oversight Committee Meeting (Lansing, Michigan, May 13, 2014), available at <http://www.house.mi.gov/MHRPublic/videoarchive.aspx>.

SELECTED PUBLISHED OPINIONS

In re Search of Cellular Telephones, 945 F. Supp. 2d 769 (S.D. Tex. 2013).

In re Application of United States for an Order Pursuant to 18 U.S.C. Section 2703(d), 964 F. Supp. 2d 674 (S.D. Tex. 2013).

In re United States ex rel. for an Order Pursuant to 18 U.S.C. Section 2703(d), 930 F. Supp. 2d 698 (S.D. Tex. 2012).

In re the Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747 (S.D. Tex. 2012).

Wilbert v. Quarterman, 647 F. Supp. 2d 760 (S.D. Tex. 2009).

Kemppainen v. Aransas County Detention Center, 626 F. Supp. 2d 672 (S.D. Tex. 2009).

Quintanilla v. Astrue, 619 F. Supp. 2d 306 (S.D. Tex. 2008) (memorandum and recommendation adopted).

Garner v. Morales, 237 F.R.D. 399 (S.D. Tex. 2006).

Brown v. Carr, 236 F.R.D. 311 (S.D. Tex. 2006).

United States v. Zamora, 408 F. Supp. 2d 295 (S.D. Tex. 2006).

HONORS

Commendation by the Senate of the State of Texas in Senate Resolution Number 849 for service as a United States Magistrate Judge on May 8, 2013.

Special Commendation for Outstanding Service in the Civil Division of the United States Department of Justice awarded on December 7, 2004.

BAR ADMISSIONS

State of New York, October 31, 1994
District of Columbia, June 4, 2000

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 9 of 9

66 Hastings L.J. 183
Hastings Law Journal
 December, 2014

Articles

TRIGGERFISH, STINGRAYS, AND FOURTH AMENDMENT FISHING EXPEDITIONS

Brian L. Owsley^{a1}

Copyright (c) 2014 UC Hastings College of the Law; Brian L. Owsley

Cell site simulators are an electronic surveillance device that mimics a cell tower causing all nearby cell phones to register their data and information with the cell site simulator. Law enforcement increasingly relies on these devices during the course of routine criminal investigations.

The use of cell site simulators raises several concerns. First, the federal government seeks judicial authorization to use such devices via a pen register application. This approach is problematic because a cell site simulator is different than a pen register. Moreover, the standard for issuance of a pen register is very low. Instead, this Article proposes that the applicable standard for granting a request to use a cell site simulator should be based on the Fourth Amendment probable cause standard.

Second, cell site simulators sweep up the data and information of innocent third-parties. The government fails to account for this problem. This Article proposes that the granting of an application for a cell site simulator should require a protocol for dealing with the third-party information that is captured.

***184 TABLE OF CONTENTS**

INTRODUCTION	185
I. CELL SITE SIMULATORS UTILIZE BASIC EXISTING CELLULAR TELEPHONE TECHNOLOGY	187
II. CELL SITE SIMULATORS CAPITALIZE ON EXISTING CELLULAR TECHNOLOGY TO RETRIEVE A CELL PHONE USER'S INFORMATION	191
A. BASIC OPERATIONS OF CELL SITE SIMULATORS	191
B. THE MANNER IN WHICH LAW ENFORCEMENT OFFICIALS USE CELL SITE SIMULATORS	192
III. THE DEVELOPMENT OF THE PEN REGISTER STATUTE	194
IV. FEW AVAILABLE EXAMPLES OF EITHER MOTIONS OR COURT ORDERS ADDRESS CELL SITE SIMULATORS & SIMILAR DEVICES	200
A. COURT ORDERS ADDRESSING APPLICATIONS FOR DIGITAL ANALYZERS AND CELL SITE SIMULATORS	201
1. <i>The Central District of California</i>	201
2. <i>The Southern District of Texas</i>	203
a. <i>The Use of a Cell Site Simulator in a Prison Setting</i>	203
b. <i>The Use of a Cell Site Simulator to Target a Drug Dealer</i>	204
3. <i>The Northern District of Texas</i>	205
4. <i>The District of Maryland</i>	206
5. <i>The District of New Jersey</i>	207
6. <i>The District of Arizona</i>	208
7. <i>Other Magistrate Judges Have Acknowledged Handling Cell Site Simulator Applications</i>	210
B. FORM APPLICATIONS AND ORDERS DRAFTED BY LAW ENFORCEMENT AGENCIES	211
1. <i>The United States Attorneys' Bulletin</i>	211

Exhibit 2-B

2. <i>The Department of Justice Electronic Surveillance Manual</i>	212
3. <i>The District of Arizona Form</i>	213
4. <i>The Los Angeles Police Department Form</i>	215
V. THE DEVELOPMENT OF FOURTH AMENDMENT JURISPRUDENCE	218
A. HISTORICALLY, THE FOURTH AMENDMENT WAS PROPERTY-CENTRIC	218
B. IN KATZ, the Supreme Court Established the Reasonable Expectation of Privacy Analysis	220
C. PEOPLE HAVE A REASONABLE EXPECTATION OF PRIVACY IN THEIR CELL PHONES, INCLUDING THE NUMBERS THEY DIAL	227
CONCLUSION	230

*185 INTRODUCTION

In recent years, traditional and online media have raised concerns about a means of electronic surveillance employed by the government that has various colorful and ominous names: TriggerFish, StingRay, AmberJack, KingFish, LoggerHead, Gossamer, Harpoon, Hailstorm, International Mobile Subscriber Identifier (“IMSI”)¹ catcher, Electronic Serial Number (“ESN”)² reader, cell site simulator, or digital analyzer.³ The first eight names are essentially brand names of similar devices manufactured and sold by the Harris Corporation.⁴ In the course of various criminal investigations, the government seeks to utilize an electronic device known as a StingRay that acts as a cell site simulator.⁵ In other words, the device deceives nearby cell phones into believing that the device is a cell tower so that the cell phone's information is then downloaded into the cell site simulator.⁶

Imagine if you will, a federal agent sitting inside an unmarked van in a parking lot monitoring the activities of some subject of a criminal investigation. Inside the van the agent has an electronic surveillance device about the size of a bankers box connected to a laptop computer. With this device, the agent is targeting the subject's cell phone in a manner that the cell phone's number and other data, including, potentially, voice communications, can be downloaded. This is a great device for apprehending the bad guys. Unfortunately, this device is *186 capturing similar information from all the cell phones in the surrounding area. So the person who lives nearby, the couple who are sitting in the coffee shop on the corner, and you as you drive by in your car--all of you are also having your cell phone information captured and downloaded into the agent's computer. Let us assume that the agent obtained some kind of judicial authorization for this electronic surveillance. Would you want your information captured and saved in a government computer forever based only on the most minimal of standards? That is what the federal government is doing through its current use of cell site simulators.

Whatever these devices are called, they have proliferated in recent years, being used by state and federal law enforcement officials as well as by American and foreign intelligence agencies.⁷ Not only are large law enforcement agencies like the Los Angeles Police Department using them,⁸ but small cities like Gilbert, Arizona have also acquired them.⁹ This technology, which has been patented since at least 2002,¹⁰ has often been purchased with funds from the Department of Homeland Security to assist in regional terrorism investigations.¹¹ However, these devices have also come to be used for routine criminal investigations, including such offenses as burglary and murder.¹²

This Article addresses the use of cell site simulators and makes three principal points. First, the government's current approach of relying on the pen register statute to justify its requests for court orders fails because cell site simulators are not pen registers and thus are not covered by the pen register statute. Second, the use of cell site simulators constitutes a Fourth Amendment search, which requires probable cause. *187 Consequently, the proper approach is for the government to establish probable cause in order to obtain a search warrant consistent with the Fourth Amendment. Third, the use of the cell site simulators raises privacy concerns for third parties.

This Article raises the issue of cell site simulators in two ways that have not been addressed in current scholarship. First, I provide examples of court orders that address the use of these devices that have not been probed in previous legal scholarship. Second, I analyze the statutory and constitutional framework in which the government seeks to use cell site simulators. This Article

provides a brief description of cellular telephone and cell site technology that concerns devices such as cell site simulators in Part I. Next, Part II provides a detailed description of how these types of devices operate. In Part III, the discussion documents the historical development of pen registers, including their statutory history. Part IV provides the various few examples of the government's applications for cell site simulators, as well as orders addressing such applications. Part V analyzes the development of Fourth Amendment jurisprudence and discusses the use of cell site simulators in light of people's reasonable expectations of privacy. In assessing these expectations, courts have, to a certain extent, relied on decisions that shape the third party doctrine --*Smith v. Maryland*¹³ and *United States v. Miller*¹⁴--that no longer adequately address the realities of today's cell phone technology or people's expectations of privacy. Finally, in Part VI, I conclude by making some proposals as to how to address the privacy concerns.

I. CELL SITE SIMULATORS UTILIZE BASIC EXISTING CELLULAR TELEPHONE TECHNOLOGY

To fully appreciate the significance of a cell site simulator, it is important to understand the basics of how cellular telephones work. In enacting the Electronic Communications Privacy Act ("ECPA"), Congress addressed cellular telephones, which at that time were based on radio transmission.¹⁵ In building a network, telecommunications providers created "large service areas [[that] are divided into honeycomb-shaped segments or 'cells'--each of which is equipped with a low-power *188 transmitter or base station which can receive and radiate messages within its parameters" from cellular phones within the providers' networks.¹⁶ Each "cell," in turn, collects "a number of pieces of data 'regarding the strength, angle, and timing of the caller's signal measured at two or more cell sites, as well as other system information such as a listing of all cell towers in the market area, switching technology, protocols, and network architecture.'"¹⁷ Consequently, each cell site "detects the radio signal from the handset, and connects it to the local telephone network, the Internet, or another wireless network."¹⁸ Typically, cell sites are physically located atop towers, but the equipment can also be placed on trees, roofs, flagpoles, and buildings.¹⁹

Within this framework of cell tower networks, the origination of a cellular telephone call initiates a series of relays along the cell site network:

When a caller dials a number on a cellular telephone, a transceiver sends signals over the air on a radio frequency to a cell site. From there the signal travels over phone lines or a microwave to a computerized mobile telephone switching office ("MTSO") or station. The MTSO automatically and inaudibly switches the conversation from one base station and one frequency to another as the portable telephone . . . moves from cell to cell.²⁰

Whenever any cellular phone is turned on, it sends out a signal seeking the closest cell site, which in turn will register that telephone with that cell site.²¹ "This process, called 'registration,' occurs approximately every *189 seven seconds,"²² enabling "cellular providers to obtain a plethora of information about the telephones contacting their cell-sites."²³

The Department of Justice ("DOJ") has explained that "to provide service to cellular telephones, providers have the technical capability to collect information such as the cell tower nearest to a particular cell phone, the portion of that tower facing the phone, and often the signal strength of the phone."²⁴ For example, in 1997, the Federal Communications Commission ("FCC") issued rules "requir[ing] cellular service providers to upgrade their systems to identify more precisely the longitude and latitude of mobile units making emergency 911 calls."²⁵ Telecommunications providers "generally keep detailed historical records of this information for billing and other business purposes."²⁶

This network of cell towers was designed to further communication among a subscriber's cell phone with other cell phones or landline telephones. It is necessary for efficient operation of the network. It is unlikely to change in any significant manner

because the complete overhaul of the technology would be expensive. It is this system of cell tower networks that government officials seek to utilize when employing cell site simulators.

*190 Most cellular telephones around the world operate through the Global System for Mobile Communications (“GSM”).²⁷ Within this system, a cell phone initiating a call connects through its unique International Module Equipment Identity (“IMEI”)²⁸ to a base station, which is essentially the hardware of a cell tower.²⁹ A base station potentially can operate with signal strength as low as fifty watts.³⁰ Of course, the number of base stations in an area hinges on the volume of demand for cellular service in that area:

The size of the cell depends basically on the geographic features of the area and consequently on the range of the stations. But also the number of possible calls, that have to be handled simultaneously, has to be considered, since it is limited by the number of available channels. Hence, in densely populated areas, the cells often have a diameter of only a few hundred meters, whereas in sparsely populated areas several kilometers are usual.³¹

A base station is “not only responsible for the connectivity [of the cell phone call, but is] also needed for encryption and decryption of communication data.”³² From the base station, a cell phone call is routed to a base station controller, which in turn will move the call to another base station to prevent the call from being terminated.³³ If this handoff has to be done beyond a base station controller’s range, then the transfer is handled by a mobile switching center.³⁴ This transfer represents the final stage of the call as the mobile switching center “is responsible for the authentication, routing, handoffs over different Base Station Controllers, connection to the landline, etc.”³⁵

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 4 of 41

***191 II. CELL SITE SIMULATORS CAPITALIZE ON EXISTING CELLULAR TECHNOLOGY TO RETRIEVE A CELL PHONE USER’S INFORMATION**

Understanding how cell phone technology works, it is next important to appreciate how cell site simulators exploit cell phone technology in order to gather electronic information.

A. BASIC OPERATIONS OF CELL SITE SIMULATORS

Cell site simulators are being used more and more by intelligence agencies around the world, not just in the United States.³⁶ Although the Harris Corporation is one of the major producers of these devices, these days, a reasonably bright computer whiz with \$1,500 can buy the raw components to make one.³⁷ The names TriggerFish and StingRay are trade names manufactured by the Harris Corporation, which sells those devices to American law enforcement and intelligence agencies.³⁸ Essentially, a TriggerFish is an older piece of technology that is a digital analyzer for passive interception of analog cell phone service.³⁹ In other words, while it can intercept a cell phone call’s verbal content, a digital analyzer (because it is a passive surveillance technique) can intercept only cell phones that are actually transmitting.

On the other hand, a StingRay is an IMSI catcher that captures digital cell phone information through an active interception process.⁴⁰ In 1996, Rohde & Schwarz, a German electronics company specializing in wireless communications, first invented an IMSI catcher that was able “to identify a subscriber by forcing it to transmit the IMSI.”⁴¹ One year later, the next model created by Rohde & Schwarz enabled the user “not *192 only to identify, but also to tap outgoing calls.”⁴² Thus, as early as 1997, an IMSI catcher could be used to capture audio content.

Within the GSM, there is a vulnerability in the authentication process that enables cell site simulators, like an IMSI catcher, to breach the system.⁴³ Specifically, “it is not necessary to authenticate a Base Station to a Mobile Station.”⁴⁴ In other words, the cell site simulator tricks the nearby cell phone into transmitting information to it as it would the nearest cell tower. “An IMSI catcher exploits this weakness and masquerades to a Mobile Station as a Base Station.”⁴⁵ Through this masquerade, the cell site simulator “causes every mobile phone of the simulated network operator within a defined radius to log in” or register with it as it would a cell tower.⁴⁶

Cell phones are designed to optimize reception by seeking the strongest signal among nearby base stations.⁴⁷ A base station can operate effectively with signal strength as low as twenty-five watts.⁴⁸ Thus, for a cell site simulator to be effective, it need only be marginally stronger than the signal of the nearest cell towers.

B. THE MANNER IN WHICH LAW ENFORCEMENT OFFICIALS USE CELL SITE SIMULATORS

Law enforcement officials will often use a cell site simulator inside a vehicle in conjunction with a computer that has mapping software.⁴⁹ Normally when a cellular phone is turned on, it seeks a connection to its telecommunications network system by using the nearest cell tower within its network.⁵⁰ This registration process enables the cell phone to communicate with its network, transmitting information and data, including audio content. Capitalizing on this registration, after the cell *193 site simulator mimics a cell tower, nearby cellular phones will connect to it. This connection enables the device to download telephone numbers and other information related to the cellular phones, such as signal strength, because it typically emits the strongest signal in the nearby area.⁵¹ For example, this technology would enable the user of a cell site simulator to detect the electronic serial number of the phone, the number for the cellular telephone, as well as any telephone numbers called from the cell phone.⁵² The surveillance vehicle can then move to several different locations, collecting the phone's signal strength, thus enabling the officers to triangulate and map the phone's location.⁵³

In addition to downloading information from all the cellular phones located within the area, a cell site simulator can be used to locate a specific cellular phone when the number is already known, but the location is unknown.⁵⁴ Law enforcement officials “can drive around until they get a signal from the target phone while pinging it.”⁵⁵ After the target phone is located, the signal strength is measured in order to triangulate and map the location again.⁵⁶ In a hearing addressing electronic surveillance issues, an FBI agent “testified that he was able to determine the approximate distance from the originating cell tower where the cell phone and Stingray switched from the originating cell tower to another cell tower.”⁵⁷ He further explained “that this method allows him to determine, with a reasonable degree of certainty, a fairly narrow geographical location where an individual is located while a cell call is being placed.”⁵⁸

Similarly, in a warrantless search by the Tallahassee Police Department, officers used a handheld device, as well as one mounted on *194 a police vehicle.⁵⁹ Testimony from an unsealed hearing transcript revealed how the cell site simulators were employed:

Police drove through the area using the vehicle-based device until they found the apartment complex in which the target phone was located, and then they walked around with the handheld device and stood ‘at every door and every window in that complex’ until they figured out which apartment the phone was located in. In other words, police were lurking outside people's windows and sending powerful electronic signals into their private homes in order to collect information from within.⁶⁰ Consistent with the testimony in *United States v. Allums*, it is apparent that some law enforcement officials are personally using this technology, as opposed to relying on any third-party telecommunications providers.

Any signals sent by law enforcement officials using a cell site simulator are signals that would not otherwise have been sent during the normal operations of a telecommunication provider's operation of its cell towers.⁶¹ Moreover, the use of this device causes a brief disruption in the telecommunication provider's service to the cell phone.⁶²

Some law enforcement officials are utilizing cell site simulators without court authorization.⁶³ Moreover, the federal officials who do seek a court order routinely file such applications pursuant to the pen register statute.⁶⁴ This approach is highly advantageous for the government, as the standard for a pen register application is much lower than the standard for a warrant because it does not require probable cause.⁶⁵

III. THE DEVELOPMENT OF THE PEN REGISTER STATUTE

In order to analyze the inapplicability of the pen register statute to cell site simulators, one must know the function of a pen register. When the government seeks to ascertain the telephone numbers of incoming and outgoing calls, it files an application seeking a court order *195 authorizing a pen register and a trap and trace device, respectively.⁶⁶ Historically, the Supreme Court defined a pen register as a device recording the outgoing numbers dialed from a specific telephone.⁶⁷ In *United States v. New York Telephone Company*,⁶⁸ the Court similarly defined a pen register: "A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed."⁶⁹ In other words, the Court reiterated the position from *United States v. Giordano*, that a pen register concerns the telephone numbers of outgoing calls from a specific telephone.

**ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 6 of 41**

In *New York Telephone*, the Supreme Court held that Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Wiretap Act") did not apply to pen registers.⁷⁰ Instead, the Court held that the statute concerned only "orders 'authorizing or approving the *interception* of a wire or oral communication.'"⁷¹ Because pen registers do not intercept any communications, the Wiretap Act did not authorize pen registers. Nonetheless, the Court concluded that district courts have the authority to authorize the installation of a pen register.⁷² The basis for this authority was [Rule 41 of the Federal Rules of Criminal Procedure](#), which requires a showing of probable cause.⁷³ Specifically, the Court reasoned "that [Rule 41](#) is sufficiently broad to include seizures of intangible items such as dial impulses recorded by pen registers."⁷⁴

In 1986, Congress enacted the ECPA, which amended the Wiretap Act to explicitly address pen registers.⁷⁵ The ECPA defined a pen *196 register as a "device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted . . . on the telephone line to which such device is attached."⁷⁶ This definition essentially follows the definition enunciated in *New York Telephone*.

In the Communications Assistance for Law Enforcement Act of 1994, Congress mandated that both telecommunications and Internet service providers permit authorized law enforcement officers access to their networks in order for them to engage in electronic surveillance.⁷⁷ Regarding pen registers, however, the statute required that use of such technology "shall not include any information that may disclose the physical location of the subscriber."⁷⁸ Through this revision, Congress sought to capture transmitted e-mail data as well as the outgoing number dialed on cell phones, but not the location of the cell phone itself. In testifying before Congress in support of the statute, then-FBI Director Louis Freeh attempted to assuage legislators' concerns the statute would be used to authorize the tracking of individuals.⁷⁹

In 2001, Congress amended the definition of the term "pen register" in the USA Patriot Act.⁸⁰ The Patriot Act defines a "pen register" as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by

an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any *197 communication.”⁸¹ An order authorizing a pen register pursuant to the Patriot Act must specify:

- (A) the identity, *if known*, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;
- (B) the identity, *if known*, of the person who is the subject of the criminal investigation;
- (C) the attributes of the communications to which the order applies, including the number or other identifier and, *if known*, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied.⁸²

Analysis of §3123(b)(1) reveals that, in each subsection, Congress inserted the language “if known” to specify that the order need only contain the aforementioned information if known at the time authorization is requested. For example, in subsection (A), the order need not contain the name of the person to whom the cell phone is leased unless that person's name is known. Similarly, in subsection (B), the court order does not have to provide the name of the target of the investigation unless that person's name is known. However, in subsection (C), Congress did not modify the language “the attributes of the communications to which the order applies, including the number or other identifier” to add “if known.” Indeed, the word “and” in that subsection makes clear that “the location of the telephone line or other facility” must be included in the order only “if known.” Consequently, the rest of “the attributes of communications,” including “the number or other identifier,” must be specified within any order authorizing any pen register application.

Moreover, the inclusion of the word “facility” within the text of § 3123(b)(1), in addition to “telephone line,” as covered by the pen register statute, does not permit law enforcement to obtain subscriber information without providing the cell phone number. The DOJ acknowledged that “facility” would include “a cellular telephone number” or “a specific cellular telephone identified by its electronic *198 serial number.”⁸³ Pursuant to § 3123(b)(1), pen register applicants can make requests when they know the cell phone number or the electronic serial number.⁸⁴ Indeed, the DOJ's *Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidences* suggests that a pen register is not appropriate when the targeted cell phone number or electronic serial number is unknown. Much of the significance of the amending language is attributable to the fact that Congress sought to ensure that the use of pen registers extended to new technologies, such as cell phones and computers.⁸⁵

Accordingly, this revision in the USA Patriot Act broadened the definition of a pen register. Some judges have interpreted the Patriot Act to expand the definition to include electronic communications in addition to dialing information, but not to the capture of cell site information.⁸⁶ Others have rejected this approach, concluding that the Patriot Act applies to all communications to and from the targeted cell phone.⁸⁷ Regardless of the debate over the scope of a pen register following the Patriot Act, courts have routinely determined that law enforcement submit an application to use a pen register when seeking information about a particular telephone.⁸⁸ Indeed, the purpose of a pen register is to track telephone numbers, not people.

*199 In *New York Telephone*, the Supreme Court's conclusion that the Wiretap Act did not apply to pen registers did not also mean that the government could obtain pen registers without any judicial intervention.⁸⁹ To the contrary, the Court determined that the government could only obtain a pen register by establishing probable cause, consistent with the seizure standard enunciated in Rule 41 of the Federal Rules of Criminal Procedure, which is based on the Fourth Amendment.⁹⁰ Even if cell site simulators are not covered by the current iteration of the pen register statute, that does not grant the government carte blanche to use these devices without any judicial authorization. Instead, the appropriate approach is for the government to seek authorization for the use of a cell site simulator consistent with the requirements of Rule 41 and the Fourth Amendment.

Congress has limited judicial review of pen register applications to the “ministerial” task of confirming that the government has properly identified the attorney and agency seeking the order as well as providing a certification that the information sought through the device is relevant to an ongoing investigation.⁹¹ When reviewing these applications, courts inquire neither into the veracity of the facts asserted by the government, nor into the reasonableness of its judgment concerning likelihood or relevance.⁹² One scholar notes that “the ECPA’s vague definition of a pen register, in combination with innovations in communications technologies and judicial permissiveness, allows law enforcement to acquire much communication attribute information by satisfying, at most, the minimal pen register procedures.”⁹³ Consequently, the government is typically able to provide the proper identifications and certification to satisfy this low bar.⁹⁴ That low standard may be *200 appropriate in applications in which law enforcement officials are truly seeking a traditional pen register to ascertain the numbers called from a specific cell phone. However, as the few known examples of requests for authorization to employ a cell site simulator demonstrate, the use of the pen register statute to support seeking materials with a cell site simulator is more troubling.

IV. FEW AVAILABLE EXAMPLES OF EITHER MOTIONS OR COURT ORDERS ADDRESS CELL SITE SIMULATORS & SIMILAR DEVICES

Very few judicial decisions address the use of these tools of electronic surveillance. One possible reason for the lack of decisions is that the government has attempted to keep its use of cell site simulator technology a secret.⁹⁵ For example, law enforcement officials often file their applications as requests for pen registers without much, if any, reference to the fact that the device to be used is a different type of electronic surveillance than the traditional pen register.⁹⁶ Moreover, when courts ask the government to provide legal authority for such electronic surveillance, pursuant to the pen register statute, the government is less than candid.⁹⁷ Finally, various government agencies, both federal and state alike, have taken measures to keep their use of cell site simulators secret. The FBI has gone so far as to require its employees to sign nondisclosure agreements to prevent them from disclosing any information about the government’s use of cell site simulators.⁹⁸ There *201 are also allegations that the Sarasota Police Department distorted its response to the court regarding its use of a StingRay.⁹⁹

Indeed, in one case that I heard as a federal magistrate judge, the Assistant United States Attorney (“AUSA”) who appeared before me repeatedly indicated that a legal memorandum would be forthcoming, but instead filed a motion to withdraw after a month. In another case the federal prosecutor indicated that he would provide legal authority the next day, but ultimately did not provide any such support.¹⁰⁰ The magistrate judge hearing the case informed the AUSA that there were some problems with the application.¹⁰¹ Despite providing feedback and guidance, the magistrate judge never heard from the applicant.¹⁰²

Existing decisions reveal that the government filed such applications pursuant to the pen register statute. With the exception of one published decision, they all address the standard after the amendments in the USA Patriot Act. Additionally, few, if any, form motions and orders created by law enforcement officials exist.

A. COURT ORDERS ADDRESSING APPLICATIONS FOR DIGITAL ANALYZERS AND CELL SITE SIMULATORS

1. The Central District of California

One of the first known decisions discussing law enforcement’s use of this technology involves an application by the government for authorization to use a digital analyzer.¹⁰³ This is the only published decision addressing such electronic surveillance devices prior to the USA Patriot Act.

In this application, the government could not identify the cell phones of any of the five subjects of its narcotics investigation, but instead sought to analyze the signals from these subjects' cell phones.¹⁰⁴ Specifically, the applicant indicated that the investigators would "conduct surveillance of the subjects of the investigation, and when they *202 observe[d] a subject using a cellular telephone, they [would] turn on the digital analyzer."¹⁰⁵ At that time they would obtain the information related to the specific cellular telephone that the subject was using.

Although the application sought a court order for the digital analyzer pursuant to 18 U.S.C. §3123, the government maintained that a court order was not necessary.¹⁰⁶ The trial court agreed, reasoning that the Fourth Amendment did not afford the subjects of a criminal investigation a reasonable expectation of privacy regarding their telephone numbers.¹⁰⁷ The court further explained that the pen register statute did not apply to the government's application because the statute contemplated investigation of a specific phone, whereas in this instance, law enforcement was targeting the individuals using the phones.¹⁰⁸

Although the pen register statute did not apply per se, the court found that the spirit of the statute covered the intended activity. Applying the requirements of the statute, the court found the proposed order deficient. First, because the telephone numbers of the subjects of the investigation were unknown, it would be impossible to comply with the statute.¹⁰⁹ The court concluded that in passing the pen register statute, Congress had two principal concerns: "(1) the abusive interception of communications and (2) the accountability of law enforcement officers using advanced technology that might threaten privacy rights."¹¹⁰ The trial court specifically expressed concern about the digital analyzer intercepting the "telephone numbers and calls made by others than the subjects of the investigation."¹¹¹ Additionally, because the proposed court order did not list the specific telephone numbers to be targeted by the digital analyzer, the order should have included "a requirement that the investigative agency maintain a time log identifying each target cellular telephone analyzed (by ESN and telephone number), together with all intercepted telephone numbers dialed or pulsed from each such *203 telephone."¹¹² Because the application did not include the numbers or this requirement, the court denied the application without prejudice.¹¹³

2. The Southern District of Texas

a. The Use of a Cell Site Simulator in a Prison Setting

Since the enactment of the USA Patriot Act in 2001, there have been a few examples of applications for cell site simulators in federal court. In April of 2011, for example, the government filed an application for a pen register in the Southern District of Texas.¹¹⁴ Specifically, the AUSA indicated that the government suspected that federal prison inmates were using cellular phones to perpetrate various federal offenses.¹¹⁵ The government knew the names of the suspects, their location, and the location where they typically used their cell phones;¹¹⁶ however, it did not know the phone numbers or in whose names the phones were purchased or leased.¹¹⁷ To advance its investigation, federal law enforcement agents sought an order authorizing the installation of a pen register and a trap and trace device.¹¹⁸ In the application, the government requested authority to use a device that could ascertain the number of any cell phones operating within a particular area, including the prison facilities.¹¹⁹ According to the AUSA's statements during *ex parte* discussions, the device functioned by impersonating a cell tower, thereby receiving all of the signals sent from any nearby cellular phones.¹²⁰

The government acknowledged that the device would capture the phone numbers of other phones that happened to be in the vicinity, but was confident in its ability to quickly winnow those numbers out and target the phones being used by the suspects.¹²¹ The AUSA did not indicate how this winnowing process would be done. When asked about legal authority supporting the government's application, the Court was advised that a brief with legal support would be filed.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 9 OF 41

Instead of filing this legal brief, about a month after the application was filed, the government filed a motion to withdraw the application *204 because prison officials had discovered and confiscated the cellular telephones that the government was trying to locate.¹²² Because the application was moot, the motion to withdraw was granted.¹²³

b. The Use of a Cell Site Simulator to Target a Drug Dealer

In another application before the Southern District of Texas, the government sought a pen register and a trap and trace regarding a Drug Enforcement Administration (“DEA”) investigation.¹²⁴ The underlying investigation focused on an individual who was allegedly engaged in narcotics trafficking, based on an investigation of a number of years.¹²⁵ In its application, the government acknowledged that it did not know the telephone number of the cell phone used by the subject of the investigation.¹²⁶ During an *ex parte* hearing, the federal agent in charge of the investigation acknowledged that the application sought to use a StingRay device “to detect radio signals emitted from wireless cellular telephones in the vicinity of the [Subject] that identify the telephones.”¹²⁷ Specifically, he explained that if the application were granted, the device would be employed from a vehicle that would be driven near the home of the subject of the investigation; that same vehicle would also follow the subject when he went other places during the period of surveillance.¹²⁸ In this manner, the agents hoped that a common cell phone number would materialize from the numbers obtained at the various surveillance-gathering locations.

The AUSA indicated “that the application was based on a standard application model and proposed order approved by the United States Department of Justice” for use by federal prosecutors.¹²⁹ During the hearing, the AUSA was unfamiliar with some case law raised during the discussion, but represented to the court that he would file a legal *205 memorandum in support of his application the next day.¹³⁰ However, that legal support was never provided to the court.¹³¹

In its analysis of the application, the court first discussed the historical view of pen registers.¹³² Next, it discussed the revised definition of a pen register based on the USA Patriot Act.¹³³ Notwithstanding the broader definition of a pen register in the Patriot Act, the court found that the statute and case law required that the pen register applicant be targeting a known telephone number.¹³⁴ According to the judge, “the plain language of the statute mandates that this Court have a telephone number or some similar identifier before issuing an order authorizing a pen register.”¹³⁵ In other words, given the absence of a known cell phone number target, neither case law nor statutory language supported the applicability of the pen register statute to an application for a cell site simulator.

3. The Northern District of Texas

In an application filed in the Northern District of Texas in 2012, the government sought an order authorizing a pen register regarding the cellular phones used by the subject of an ongoing narcotics trafficking investigation. The alleged violations were possession with intent to distribute cocaine, marijuana, and methamphetamine in violation of 21 U.S.C. §841 and for conspiracy to possess with intent to distribute cocaine, marijuana, and methamphetamine in violation of 21 U.S.C. §846.¹³⁶ The ASUA represented that the subject of the investigation was using one or more unidentified cellular phones.¹³⁷ The government knew that this subject lived at one specific location and frequented another where he worked.¹³⁸ However, the government did not know the cell phone subscriber information of the persons leasing the cell phones that the subject was using.¹³⁹

*206 In its application, the government explained that it sought to use the pen register to simply identify the subject's telephone number, as opposed to tracking the cell phone or attempting to determine its location.¹⁴⁰ Consequently, the use of surveillance equipment was to be limited: “Once the identifying registration data and the number of the *Subject Telephone* is identified, utilization of the pen register . . . shall cease.”¹⁴¹

The court granted the government's application; however, the judge did impose some limits on the government's use of these devices.¹⁴² The judge mandated that the order applied only to the cell phone used by the subject, and that the cell site simulator was to be used only in the subject's vicinity to ascertain his cell phone number.¹⁴³ Additionally, the judge specifically barred the use of the cell site simulator "when the *Subject* [was] in a location in which he would have a reasonable expectation of privacy; including but not limited to: a private residence, a vehicle, or a private office."¹⁴⁴ Once the subject's cell phone number was determined, the government was ordered to cease using the cell site simulator.¹⁴⁵ The government was apparently displeased with the court's conditions and ultimately did not use a cell site simulator.¹⁴⁶ Indeed, the AUSA informed the magistrate judge that the restrictions were too onerous.¹⁴⁷

4. The District of Maryland

In an application filed in the District of Maryland in 2012, the government sought an order relating to the cellular phones used by the subject of an ongoing narcotics trafficking investigation for alleged violations of conspiracy to distribute controlled substances.¹⁴⁸ Specifically, the government sought to use a device to obtain "certain unknown mobile telephone(s) presently with unknown call number(s); unknown subscriber(s); and unknown service provider(s)" used by the subject of the ongoing investigation.¹⁴⁹ The AUSA elaborated that "[t]he *207 purpose of this requested order is to identify this unknown information by deploying the device to the Target Telephone(s)."¹⁵⁰

The AUSA indicated that the cell site simulator would "detect radio signals emitted from wireless cellular telephones in the vicinity of the target, including the Target Telephone(s)."¹⁵¹ The AUSA further explained that "[b]y determining the identifying registration data at various locations in which the subject telephone is reasonably believed to be operating, the telephone number(s) and/or subscriber identities corresponding to the Target Telephone(s) can be identified."¹⁵² The government acknowledged that, by using the device, it would invariably capture the telephone numbers of innocent third parties.¹⁵³

The application requested the court to order that, when the federal agents obtained information from the search, they were "to log the identity of each cellphone analyzed, together with the intercepted subscriber identities for each device."¹⁵⁴ Moreover, it sought an order requiring that the government "avoid the collection of data from individuals other than that of the target."¹⁵⁵

Interestingly, the government asserted that the 1995 Central District of California opinion provided support for its application.¹⁵⁶ Although the application acknowledged that the 1995 decision was not favorable to the government, the decision provided guidance as to what any subsequent applications should contain.¹⁵⁷ Finally, the AUSA maintained that the application and the attached proposed order pending before the Maryland district court adhered to the dictates from the 1995 decision.¹⁵⁸

5. The District of New Jersey

In an application filed in the District of New Jersey in 2012, the government sought an order authorizing a pen register and trap and trace device as well as subscriber information, pursuant to 18 U.S.C. §2703.¹⁵⁹ The government knew the targeted cell phone number and that it was issued by Simple Mobile through its relationship with T-Mobile.¹⁶⁰ *208 Because the location of the targeted cell phone was unknown, the application also sought authorization for "the FBI to deploy mobile pen register and trap and trace equipment to determine the general location of the cellular telephone facility assigned [to the specific] telephone

number.”¹⁶¹ The court authorized the use of this “mobile pen register equipment” “in order to determine the general location” of the cell phone.¹⁶² However, the court limited the FBI from “us[ing] the mobile equipment, absent other authority, to locate the Target Facility once it leads them to believe that they have identified a single residence or private space within which the Target Facility may be located.”¹⁶³

6. The District of Arizona

In a criminal prosecution in the District of Arizona, the government sought the defendant, a fugitive indicted on 74 counts of mail and wire fraud, aggravated identity theft, and conspiracy.¹⁶⁴ “The government located and arrested Defendant, in part, by tracking the location of an aircard connected to a laptop computer that allegedly was used to perpetuate the fraudulent scheme.”¹⁶⁵

After the defendant's arrest, he filed a motion for disclosure of evidence, as well as additional discovery. Specifically, he sought extremely detailed information regarding the aircard, as well as the identities and training of the FBI agents capable of using this technology.¹⁶⁶ In support of the defendant's motion, the American Civil Liberties Union (“ACLU”) filed an *amicus* brief arguing that because the AUSA seeking the original order authorizing the use of the StingRay failed “to apprise the magistrate that it intended to use a stingray, what the device is, and how it works, it prevented the judge from exercising his constitutional function of ensuring that warrants are not overly intrusive and all aspects of the search are supported by probable cause.”¹⁶⁷

The government stipulated to a number of facts related to the motion for discovery, as well as the motion to suppress. It agreed that “[t]he mobile tracking device used by the FBI to locate the aircard function[ed] as a cell-site simulator. The mobile tracking device *209 mimicked a Verizon Wireless cell tower and sent signals to, and received signals from, the aircard.”¹⁶⁸ Additionally, the government acknowledged that “[t]he FBI used the mobile tracking device in multiple locations,” taking readings and then moving to another location to take more readings.¹⁶⁹

In locating the defendant with the use of the cell site simulator device, the government indicated that “[t]he FBI never used more than a single piece of equipment at any given time.”¹⁷⁰ Moreover, the agents using the device were on foot near the defendant's apartment.¹⁷¹ During that surveillance, these agents made telephone calls to the aircard.¹⁷² The government indicated that “[t]he mobile tracking device used to simulate a Verizon cell tower [was] physically separate from the pen register trap and trace device used to collect information from Verizon.”¹⁷³ Finally, for purposes of the defendant's pending motion, the government stipulated that “[t]he tracking operation was a Fourth Amendment search and seizure.”¹⁷⁴

In July 2008, the government obtained a warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure from a magistrate judge in the Northern District of California authorizing the use of the StingRay device to locate the aircard.¹⁷⁵ In finding probable cause, the magistrate judge identified the aircard by both its specific assigned telephone number as well as its ESN.¹⁷⁶ In the motion to suppress, the defendant argued that the government's use of the device to track the aircard violated his Fourth Amendment rights.¹⁷⁷ Specifically, he argued “that the warrant is not supported by probable cause, that it lacks particularity, that the government's searches and seizures exceeded the warrant's scope, and that agents executed the warrant unreasonably because they failed to comply with inventory and return requirements.”¹⁷⁸

The district court judge found that the agent's affidavit in support of the warrant clearly linked locating the aircard with a high likelihood that it would lead to evidence of criminal activity.¹⁷⁹ Furthermore, the court noted that the agent's affidavit specifically indicated that the authorized device was used to locate the aircard.¹⁸⁰ Next, the court concluded that *210 the warrant was sufficiently particular based on the use of the specific telephone number and the ESN identifying the aircard.¹⁸¹

Regarding any argument for privacy by the defendant, the judge concluded that the defendant did not have a legitimate expectation of privacy in light of the fact that he obtained his residence and the computers through identity theft and other fraudulent means.¹⁸²

Regarding the scope of the warrant, defendant argued that Verizon, rather than the FBI, was authorized to search for the aircard.¹⁸³ Again, the court rejected this argument, noting that while the warrant was “not a model of clarity,” it satisfied the standard mandated by Rule 41.¹⁸⁴ Ultimately, the court denied the motion to suppress the evidence related to the aircard in part because the defendant did not have a legitimate expectation of privacy in his aircard.¹⁸⁵

7. Other Magistrate Judges Have Acknowledged Handling Cell Site Simulator Applications

Of course, the above discussion is not exhaustive, as other magistrate judges may have received applications using the pen register application and not realized that they were authorizing or denying use of a cell site simulator.¹⁸⁶ One magistrate judge in the Western District of Washington explained that he received a request for a TriggerFish in 2011, which he denied.¹⁸⁷ Similarly, a magistrate judge in the Eastern District of Texas was faced with a pen register application for a cell site simulator.¹⁸⁸ He indicated some concerns that he had with the request and sought some revisions, or in the alternative, some authority in support of the requested application.¹⁸⁹ Ultimately, the AUSA withdrew the application.¹⁹⁰

Another magistrate judge indicated that he and his colleagues in the Southern District of California routinely grant requests for cell site simulators because people do not have any expectation of privacy in their telephone numbers.¹⁹¹ He did note that an authorization covered *211 only the recording of the ESN and MIN numbers transmitted to the telecommunication providers by cell phone.¹⁹²

B. FORM APPLICATIONS AND ORDERS DRAFTED BY LAW ENFORCEMENT AGENCIES

In addition to these judicial examples addressing government applications to use cell site simulators, law enforcement officials have provided other examples in their training manuals.

1. The United States Attorneys' Bulletin

In a September 1997 *United States Attorneys' Bulletin*, the Electronic Surveillance Unit of the Officer of Enforcement Operations within the Criminal Division of the DOJ issued guidance regarding certain electronic surveillance techniques, including digital analyzers and cell site simulators.¹⁹³ This Bulletin explained that “[i]t is now possible for agents to capture electronically the unknown [ESN] or telephone number of a cellular telephone through the use of a device known as a *digital analyzer*.¹⁹⁴ It further explained that a digital analyzer “can be programmed to identify the telephone number assigned to the subject cellular telephone and telephone numbers dialed from this phone, as well as its ESN; i.e. a number assigned by the cellular telephone manufacturer and programmed into the telephone.”¹⁹⁵ The Bulletin explicitly acknowledged that, because a digital analyzer is capable of intercepting communications as well as telephone numbers, the device “is programmed so it will not intercept cellular conversations or dialed numbers when it is used for the limited purpose of seizing ESNs and/or the cellular telephone's number.”¹⁹⁶

The Bulletin also discussed cell site simulators, explaining that they “can provide agents with a cellular telephone's ESN and mobile identification number ('MIN,' which contains the cellular telephone number and other information related to the operation of the phone).”¹⁹⁷ Next, it elaborated that cell site simulators:

[S]imulate[] some of the activities of a cellular service provider's cell site transmitter, albeit in a much smaller area, and allow[] agents to query cellular phones for their ESNs and MINs through "autonomous *212 registration," an activity a cell site transmitter normally conducts to identify cellular phones operating within its cell or area.¹⁹⁸

Finally, the Bulletin discussed that as with "a real cell site transmitter, the [cell site simulator] can determine ESNs and MINs of cellular phones that are 'powered up' or turned on. (The phone need *not* be in a 'use' mode; the information can be obtained unbeknownst to the cellular phone user.)"¹⁹⁹

The Bulletin discussed that both digital analyzers and cell site simulators:

[C]an capture the cell site codes identifying the cell location and geographical sub-sector from which the cellular telephone is transmitting; the call's incoming or outgoing status; the telephone numbers dialed (pen register order required); and the date, time, and duration of the call. This cell site data is transmitted continuously from a cellular telephone (not by the user) as a necessary part of call direction and processing.²⁰⁰

Each telecommunications provider "uses this information to connect with the account in order to direct calls, and constantly reports to the customer's telephone a readout regarding the signal power, status, and mode of the telephone."²⁰¹

2. The Department of Justice Electronic Surveillance Manual

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338 PAGE 4 of 44

In 2005, the DOJ published an *Electronic Surveillance Manual* to provide guidance to its attorneys throughout the country. Specifically, the *Electronic Surveillance Manual* "sets forth the procedures established by the Criminal Division of the Department of Justice to obtain authorization to conduct electronic surveillance."²⁰² The manual, last revised in 2005, discusses digital analyzers in a section concerning pen registers and trap and trace devices.²⁰³ It explicitly cautions the need for a court order prior to using a cell site simulator:

Because section 3127 of Title 18 defines pen registers and trap and trace devices in terms of recording, decoding or capturing dialing, routing, addressing, or signaling information, a pen register/trap and trace order must be obtained by the government before it can use its own device to capture the ESN or MIN of a cellular telephone, even though there will be no involvement by the service provider.²⁰⁴

*213 This determination by the DOJ, that a device used only to obtain a MIN requires a court order, indicates that a device used to ascertain the telephone number would also require a court order.

In the *Electronic Surveillance Manual*, the DOJ explained that "[l]aw enforcement possesses electronic devices that allow agents to determine the location of certain cellular phones by the electronic signals that they broadcast."²⁰⁵ Specifically, a cell site simulator's "equipment includes an antenna, an electronic device that processes the signals transmitted on cell phone frequencies, and a laptop computer that analyzes the signals and allows the agent to configure the collection of information."²⁰⁶

The DOJ does not describe a device used to ascertain a phone number as a pen register. However, it demonstrates a belief that the same legal standards apply to such devices. The point is made explicit in the model form application and proposed order for a TriggerFish, a digital analyzer.²⁰⁷ The caption for the application reads "In the Matter of the United States of America for an Order Authorizing the Installation and Use of a Pen Register."²⁰⁸ Moreover, the caption on the proposed order reads similarly.²⁰⁹

3. The District of Arizona Form

In 2012, the Acting United States Attorney for the District of Arizona created a form application to guide attorneys in that office in requesting ESN identification numbers.²¹⁰ In the form application, the AUSA sought a court order “pursuant to 18 U.S.C. §§3122 and 3123, authorizing law enforcement to use an electronic serial number identifier to collect non-content wireless signaling information.”²¹¹ The caption on the application reads, “In the Matter of the Application of the United States of America for an Order Authorizing the Use of a Mobile Number Recorder to Collect Non-Content Signaling Information from Cellular Telephones.”²¹² Although the form anticipates that the requesting *214 officials have the name of a subject of the investigation, it does not anticipate them having the cellular telephone numbers used by the subject or his drug trafficking organization, assuming the case pertains to drug trafficking.²¹³ The application explains that a “Mobile Number Recorder . . . is an instrument that will decode and/or record non-content signaling information transmitted by a cellular telephone within a limited radius to determine the unique numeric identifiers of the telephone or telephones.”²¹⁴ The form indicates that agents seek to use the Mobile Number Recorder in conjunction with traditional physical surveillance on the subject, such as by tracking the subject in an unmarked van, to obtain telephone numbers.²¹⁵

In support of the application, the government must certify the relevance of the telephone numbers sought.²¹⁶ The form acknowledges that the mobile number recorder will gather telephone numbers unrelated to the subject, but asserts that these unrelated numbers will not be used by the investigating agents.²¹⁷ Additionally, it acknowledges that the device might also gather dialed digit information and posits that such information will be usable by the government pursuant to the pen register statute.²¹⁸ Next, the application contains blanks in which the government is to provide the specific criminal offenses that the subject allegedly committed, as well as specific facts in support of the application.²¹⁹ The government notes that it does not need to provide “specific and articulable facts” in support of its application because it will simply be using the pen register statute to obtain the subject's cell phone numbers with the mobile number recorder.²²⁰

The government also included, in this package to attorneys, a memorandum in support of its position. In the memorandum, the government argues that the mobile number recorder falls within the pen register statute as it is a recording of signaling information.²²¹ The memorandum also discusses the difference in the pen register definition in the ECPA with the amendment in the USA Patriot Act.²²² The government also argues that the Fourth Amendment does not apply to the use of a mobile number recorder.²²³

*215 The memorandum also provides an argument against the pen register statute's applicability to the mobile number recorder.²²⁴ Specifically, it notes that any court order must “include[] the number or other identifier.”²²⁵ The government acknowledges that, since the 2001 amendment, “no court has held that a device like the one in this case falls within the statutory definition of a pen register.”²²⁶ Instead, it addresses the fact that at least one court viewing the 2001 amendments simply focused on applying the pen register statute to e-mails.²²⁷ Consequently, that court determined that a “pen register must still be tied to an actual number or attempted phone call.”²²⁸

The government also provided a proposed order to grant its application.²²⁹ The proposed order follows the rationale provided by the application.²³⁰

4. The Los Angeles Police Department Form

At least one city has also developed form materials for use by its law enforcement officers. On September 29, 2012, Donal Brown, an editor at the First Amendment Coalition, filed a California Public Records Act Request with the Los Angeles Police Department (“LAPD”) for information regarding the use of devices to track and identify a cellular phone’s IMSI.²³¹ Among the various requests, Brown sought “[a] copy of any LAPD internal policies, guidelines or standards for police use of an IMSI device” or in lieu of such records “all other records sufficient to show the policies, guidelines or standards in effect for LAPD use of an IMSI device.”²³² Next, he requested “[r]ecords sufficient to show whether judicial authorization is obtained for LAPD deployment and use of an IMSI device and the type of judicial authorization obtained.”²³³ He also asked for “[r]ecords sufficient to show, for the time period June 1 [to] Sept. 30, 2012, the frequency of LAPD’s deployment and use of an IMSI device,” as well as, for the same time period, “[r]ecords sufficient to show . . . all LAPD uses of an IMSI device in which LAPD personnel *216 eavesdropped on conversation.”²³⁴ Finally, he requested “[r]ecords sufficient to identify all prosecutions or other judicial proceedings initiated by the LAPD or LA District Attorney during 2011 in which information was filed in, or furnished to, the Superior Court (LA County) derived from LAPD’s use of an IMSI device.”²³⁵ Brown asked that a response be provided within ten days.²³⁶

On December 14, 2012, Officer Martin Bland, the Officer-in-Charge of the Discovery Section within the Legal Affairs Division of the LAPD, responded to Brown’s records request.²³⁷ With respect to the first three requests, Bland indicated that he would make documents available after Brown paid the duplicating fee.²³⁸ Bland then acknowledged that, “[d]uring the time period in your request, 21 cell phone numbers were subjected to the deployment of an IMSI,” but “there were no uses of an IMSI device that involved the eavesdropping of conversations.”²³⁹ Finally, Bland declined to provide any information in response to the request regarding prosecutions involving an IMSI device because “there is no centralized repository for records (or information) responsive to [the] request,” which made the request “significantly and unduly burdensome.”²⁴⁰

On December 28, 2012, Bland provided Brown with thirty-one pages of records responsive to his request.²⁴¹ Notably, there was an October 16, 2012 memorandum to all Commanding Officers explaining that “[t]he law regarding the use of cellular and GPS tracking is evolving. Protocols governing cellphone tracking requests are necessary to ensure Department personnel are abiding by the most current case law.”²⁴² Consequently, the memorandum mandated that “[a]ll requests for cellular tracking, made concurrent with an investigation (whether by use *217 of a court order or under an exigent circumstances process), shall be directed through [the Real-Time Analysis and Critical Division].”²⁴³

In the December 28, 2012 letter from Bland to Brown, Bland provided an explanation of the statutory basis and procedures for requesting applications and court orders that use a “cell phone tracking system for identifying” a cell phone’s IMSI, as well as forms for applications and orders.²⁴⁴ Notably, in response to Brown’s request, Bland turned over an LAPD form application addressing requests for authorization of an IMSI device in the Superior Court for the County of Los Angeles.²⁴⁵ The caption reads, “In the Matter of the Application of the People of the State of California for an Order Authorizing the Use of a Pen Register and a Trap-and-Trace Device on Telephone Line Currently Designated by Telephone Number,” with a blank space to fill in the specific telephone number.²⁴⁶ The application sought to distinguish between a telephone number and a telephone line because it maintained that the pen register statute was “defined with respect to telephone lines” as opposed to telephone numbers.²⁴⁷ The application contained a section to be filled in by the police officer indicating the probable cause that supported the request.²⁴⁸

With this form application, the LAPD also provided a proposed order.²⁴⁹ In support of its recommendation, the LAPD proposed citing 18 U.S.C. § 2703(d)²⁵⁰ as the statutory authority for the order, notwithstanding the fact that the form application is characterized as a pen register request.²⁵¹

*218 V. THE DEVELOPMENT OF FOURTH AMENDMENT JURISPRUDENCE

In order to understand the applicability of the Fourth Amendment to the government's applications seeking authorization of cell site simulators, one must understand the history of the Fourth Amendment. Fourth Amendment jurisprudence developed from a fairly narrow property-centric interpretation to a more flexible standard based on reasonable expectations. This more flexible standard should be reassessed in order to ensure that cell phone users have privacy from governmental intrusions into their cell phones.

A. HISTORICALLY, THE FOURTH AMENDMENT WAS PROPERTY-CENTRIC

To better understand the current state of Fourth Amendment jurisprudence, it is important to understand a little about where we started. In light of disputes with the British authorities, the founding fathers sought to ensure that people in the newly formed country would be secure from discretionary governmental intrusions in their lives.²⁵² The Fourth Amendment provides that it is “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”²⁵³ It further mandates that “no Warrants shall issue, but upon probable cause.”²⁵⁴ Consequently, the threshold matter in Fourth Amendment jurisprudence “is whether a specific action or intrusion by the government constitutes a ‘search’ within the meaning of the Amendment.”²⁵⁵

Historically, the Fourth Amendment was viewed to safeguard citizens against search of their homes, persons, and papers based on a right of property. Many scholars have posited that Fourth Amendment jurisprudence was based on a theory of trespass.²⁵⁶ One scholar further explained that this trespass theory is rooted in the landmark pre-constitution decision of *Entick v. Carrington*.²⁵⁷ However, Orin Kerr *219 recently asserted that he and others had it wrong in viewing Fourth Amendment theory as having its historical foundation in trespass.²⁵⁸

In one of the first Supreme Court decisions to address the Fourth Amendment, the defendant challenged the use of his records, seized without a warrant, to convict him for failure to pay customs duties.²⁵⁹ In *Boyd*, the Court addressed the question of “compulsory production of a man's private papers, to be used against him in a proceeding to forfeit his property for alleged fraud against the revenue laws . . . [and whether that constituted] an ‘unreasonable search and seizure’ within the meaning of the Fourth Amendment.”²⁶⁰ In concluding that the trial court erred in requiring the production of the defendant's papers, the Court looked to early colonial history as well as English history, including the decision in *Entick*, finding that the entering and searching of the home constituted a trespass.²⁶¹

In *Olmstead v. United States*,²⁶² the Supreme Court considered a challenge to information that federal agents obtained from wiretapping the telephones within the homes of targets of a criminal investigation. Chief Justice Howard Taft made clear that the wiretapping was “made without *trespass* upon any property of the defendants” because the line that was tapped was “made in the basement of the large office building.”²⁶³ Nonetheless, he stressed that “[t]he well-known historical purpose of the Fourth Amendment, directed against general warrants and writs of assistance, was to prevent the use of governmental force to search a man's house, his person, his papers, and his effects, and to prevent their seizure against his will.”²⁶⁴ In many regards, the applied approach was a plain language interpretation of the amendment. Indeed, Chief Justice Taft distinguished *Hester v. United States*,²⁶⁵ in which he acknowledged that there was a trespass on defendant's property, but *220 ultimately “no search of person, house, papers, or effects.”²⁶⁶ In dissent, however, Justice Louis Brandeis famously cautioned that the Fourth Amendment protected citizens against “invasion of ‘the sanctities of a man's home and the privacies of life.’”²⁶⁷

In *Goldman v. United States*,²⁶⁸ the Supreme Court considered federal agents' use of a detectaphone against a wall to listen and assist in the recording of defendants' conversation within one defendant's office on the other side of the wall. The Court specifically held "what was heard by the use of the detectaphone was not made illegal by trespass or unlawful entry."²⁶⁹ Instead, the only trespass occurred when agents actually entered the defendant's office to install another device that ultimately did not function properly and provided no information.²⁷⁰ As in *Olmstead*, the dissents argued for individual privacy interests. For example, Chief Justice Harlan Fiske Stone and Justice Felix Frankfurter wrote simply:

Had a majority of the Court been willing to overrule the *Olmstead* case, we should have been happy to join them. But as they have declined to do so, and as we think this case is indistinguishable from *Olmstead*'s, we have no occasion to repeat here the dissenting views in that case with which we agree.²⁷¹

Similarly, Justice Frank Murphy dissented, noting an individual's "right of personal privacy guaranteed by the Fourth Amendment."²⁷²

B. IN KATZ, THE SUPREME COURT ESTABLISHED THE REASONABLE EXPECTATION OF PRIVACY ANALYSIS

Regardless of whether one views the development of Fourth Amendment jurisprudence through the prism of property rights, a trespass theory, or a literalist construction, after *Katz v. United States*,²⁷³ the paradigm shifted. In *Katz*, the Supreme Court held that a listening device that recorded the defendant's conversation while he talked in a public telephone booth violated the Fourth Amendment. Justice Stewart Potter explained that Katz, by entering the telephone booth and closing the door before engaging in his telephone call, evidenced an attempt and a belief that his conversation would be private.²⁷⁴ Justice Potter then elaborated that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."²⁷⁵ Finally, he determined that "[t]he Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."²⁷⁶ Interestingly, the phrase "reasonable expectation of privacy," which has been the lasting impact of *Katz*, is not from Justice Stewart's majority opinion, but instead from a concurring opinion by Justice Harlan.²⁷⁷

This "reasonable expectation of privacy" standard was reiterated and adopted by a majority of the Supreme Court in *Terry v. Ohio*.²⁷⁸ In elaborating on this standard, the Court explained, in *United States v. Jacobsen*,²⁷⁹ that "[a] 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed."²⁸⁰ In the post-*Katz* world we are left to ponder what reasonable expectation of privacy, if any, cell phone users have as it relates to the government's use of cell site simulators.

Orin Kerr has posited that while "the phrase 'reasonable expectation of privacy' is notoriously murky, much of the Supreme Court's case law on the reasonable expectation of privacy test can be understood as distinguishing between inside and outside surveillance."²⁸¹ In an earlier article he echoed this theme: "Although the phrase 'reasonable expectation of privacy' sounds mystical, in most (though not all) cases, an expectation of privacy becomes 'reasonable' only when it is backed by a right to exclude borrowed from real property law."²⁸² He distinguished between inside and outside by elaborating that governmental conduct breaches a reasonable expectation of privacy *222 when the surveillance exposes private, enclosed spaces, such as homes, cars, or packages.²⁸³ On the other hand, Patricia Bellia has maintained:

The main constitutional question is whether one retains a reasonable expectation of privacy in communications stored with a third party, such that acquisition of these communications constitutes a

'search' within the meaning of the Fourth Amendment. I call into question the prevailing assumption that an expectation of privacy is lacking when a service provider holds communications on a user's behalf.²⁸⁴

In *Smith v. Maryland*, the Supreme Court considered whether there were any privacy rights in the information that a pen register captures from a landline telephone.²⁸⁵ The Court held that the use of a pen register to obtain the telephone numbers dialed was not a Fourth Amendment search because the telephone user had "no actual expectation of privacy in the phone numbers he dialed."²⁸⁶ However, the Court's decision is a very narrow one and addresses pen register technology from the 1960s. Most importantly, the pen register at issue simply recorded a list of telephone numbers that were dialed from a *landline* telephone.²⁸⁷ Indeed, the decision was issued a decade before the cell phone became ubiquitous. The *Smith* Court did not address the vast amount of information that the government routinely seeks these days in pen register applications for cellular telephones, including the time, date, and duration of any cell phone call as well as the physical location from which the call was made.²⁸⁸ In other words, the analysis of *Smith v. Maryland*, predicated on the information obtained on a landline telephone, does not apply to the information that is obtainable through a pen register for a cell phone today.²⁸⁹ The typical consumer does not expect that all of this data is widely available to the government any time that it simply asks for it.²⁹⁰ The uproar and outrage over the breaches by the National Security Agency ("NSA") further demonstrate that there is no reasonable expectation that this information is anything but private.²⁹¹

*223 In *Georgia v. Randolph*,²⁹² the Supreme Court addressed a Fourth Amendment challenge in which the defendant sought to suppress cocaine obtained during a search of his home that resulted in this conviction for possession of cocaine. Specifically, when police officers responded to a call about a domestic dispute at the residence, the defendant's estranged wife indicated to them that her husband had narcotics in their home.²⁹³ Although the defendant expressly refused to consent to the search of his home when officers asked, they then obtained consent from his wife.²⁹⁴ In the majority opinion written by Justice David Souter, the Court held that the warrantless search was unreasonable in light of the defendant's express refusal to consent to the search.²⁹⁵

In a dissenting opinion joined by Justice Antonin Scalia, Chief Justice John Roberts took issue with the notion that defendant had a reasonable expectation of privacy in his home once he shared that home with another person, in this case his wife.²⁹⁶ Chief Justice Roberts continued by explaining that there are a large number of situations that might lead to various and different social expectations.²⁹⁷ Ultimately, he asserted that custom and "widely shared social expectation" were not a basis for evaluating a search pursuant to the Fourth Amendment.²⁹⁸

Chief Justice Roberts' visceral reaction to social expectation in *Georgia v. Randolph* is interesting when compared to his response to the Government's oral argument in *United States v. Jones*. In *Jones*, the Court dealt with whether the government could place a GPS tracking device on the vehicle of a subject of a criminal investigation without a warrant. During oral argument, Chief Justice Roberts had this exchange with the Deputy Solicitor General:

*224 CHIEF JUSTICE ROBERTS: You think there would also not be a search if you put a GPS device on all of our cars, monitored our movements for a month? You think you're entitled to do that under your theory?

MR. DREEBEN: The Justices of this Court?

CHIEF JUSTICE ROBERTS: Yes.

(Laughter.)

MR. DREEBEN: Under our theory and under this Court's cases, the Justices of this Court when driving on public roadways have no greater expectation of --

CHIEF JUSTICE ROBERTS: So, your answer is yes, you could tomorrow decide that you put a GPS device on every one of our cars, follow us for a month; no problem under the Constitution?

MR. DREEBEN: Well, equally, Mr. Chief Justice, if the FBI wanted to, it could put a team of surveillance agents around the clock on any individual and follow that individual's movements as they went around on the public streets. ²⁹⁹

Put simply, Chief Justice Roberts appeared to address the reasonable expectations of privacy as it personally relates to him and the other members of the Court. Roberts was seemingly concerned about the real possibility that someone could legally engage in this type of surveillance of his vehicle without judicial authorization. ³⁰⁰ While the majority decision, which he joined, focused on a Fourth Amendment violation based on a trespass theory, he implied that the Supreme Court Justices (and others) had an expectation of some privacy. ³⁰¹ The reason for this expectation could arguably be based on the personal nature of one's vehicle and daily travels. Still, he argued there was no expectation of privacy if law enforcement officials arrived at his residence and sought to search his home over his objections if his wife gave them express authority. ³⁰² Possibly, he was more certain that he and his wife are of one mind regarding such a potential intrusion than the possibility that a tracking device could be placed on his vehicle.

In *Jones*, Justice Sonia Sotomayor discussed both *Smith* and *Miller* in arguing that the third-party doctrine needs to be reconsidered: "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." ³⁰³ She continued by asserting that the approach established *225 in *Miller* and *Smith* "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks" including revealing information based on their cell phone usage. ³⁰⁴ In criticizing Justice Scalia's opinion in *Jones*, Justice Samuel Alito noted that the issue was not the physical trespass, but the lengthy and intrusive nature of the electronic surveillance. ³⁰⁵ He continued by positing that the old method of Fourth Amendment analysis may be inapplicable to the new issues raised by electronic surveillance. ³⁰⁶ Similarly, the Court in *Kyllo v. United States* ³⁰⁷ cautioned that "[w]hile the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development." ³⁰⁸

Since the Supreme Court decided *Jones*, one federal appellate court has addressed the issue of whether the use of warrantless cell site location information violates the Fourth Amendment. The Eleventh Circuit concluded that "it cannot be denied that the Fourth Amendment protection against unreasonable searches and seizures shields the people from the warrantless interception of electronic data or sound waves carrying communications." ³⁰⁹ The court continued with an analysis of the three decisions in *Jones* and noted that the *Katz* privacy test is still applicable. ³¹⁰ Ultimately, the Eleventh Circuit held "that cell site location information is within the subscriber's reasonable expectation of privacy" and that "obtaining of that data without a warrant is a Fourth Amendment violation." ³¹¹

Most recently, in *Riley v. California*, the Supreme Court addressed whether evidence obtained by police from a defendant's cell phone during a warrantless search subsequent arrest violated the Fourth Amendment. ³¹² In the first of the consolidated cases, David Riley was stopped by police officers for a routine traffic stop and then subsequently arrested after his car was impounded and a search revealed firearms. ³¹³ During his arrest, the officers seized his smart phone from his pants pocket and searched it, thereafter concluding that he was a member of a *226 street gang. ³¹⁴ The prosecution charged him with a number

of offenses, some of which carried sentencing enhancements based on his gang affiliation.³¹⁵ Riley challenged the denial of his motion to suppress this information.³¹⁶

In the second case, Brima Wurie was arrested for selling drugs. While under arrest, police officers noticed that his flip phone was receiving several calls from a number labeled “my house.”³¹⁷ After searching this cell phone's call log, the officers traced the number to his apartment.³¹⁸ The police then went to Wurie's residence and confirmed that it was in fact his home, in part because the woman pictured in his flip phone was found at the apartment.³¹⁹ A subsequent search of the apartment revealed drugs and firearms, resulting in multiple federal charges against him.³²⁰ The district court denied his motion to suppress, but the Court of Appeals for the First Circuit reversed and vacated Wurie's three convictions.³²¹

In analyzing these two cases, the Court first discussed the history of Fourth Amendment in the context of searches incident to arrest, and ultimately held “that officers must generally secure a warrant before conducting such a search” of a cell phone.³²² The Court continued its analysis by noting that “[d]igital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. Once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one.”³²³

The Court focused next on privacy concerns raised by cell phones, explaining that these devices were essentially small computers that stored immense amounts of data and information.³²⁴ The opinion focused on several reasons that cell phones implicate significant privacy concerns:

First, a cell phone collects in one place many types of information--an address, a note, a prescription, a bank statement, a video--that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a *227 photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all of his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.³²⁵

Finally, the Court emphasized the pervasiveness of cell phones and the fact that people carry them, with all their sensitive information, with them all of the time.³²⁶ Thus, all nine justices held that police must get a search warrant prior to searching a seized cell phone.³²⁷

C. PEOPLE HAVE A REASONABLE EXPECTATION OF PRIVACY IN THEIR CELL PHONES, INCLUDING THE NUMBERS THEY DIAL

While *Katz* established the principle of an individual's reasonable expectation of privacy, *Smith v. Maryland* and *United States v. Miller*³²⁸ are the Supreme Court decisions that are relied upon for the third-party doctrine, which in some ways undercuts *Katz*. In *Miller*, federal agents served grand jury subpoenas issued by the United States Attorney on the defendant's banks seeking records to support a criminal investigation.³²⁹ In a motion to suppress, the defendant challenged the subpoenas because they were not issued by a court.³³⁰ Because the defendant had provided his information to the bank in the regular course of his various banking transactions, the Supreme Court determined that he no longer had a reasonable expectation of privacy.³³¹ Consequently, the Court held “that there was no intrusion into any area in which respondent had a protected Fourth Amendment

interest and that the District Court therefore correctly denied respondent's motion to suppress.”³³² Of course, in this day and age of online banking, people may have a different expectation of privacy than they used to.

Generally, there is not much in the way of empirical research regarding people's reasonable expectations of privacy.³³³ Moreover, there does not appear to be any research questioning people's reasonable expectations of privacy regarding the telephone numbers that they dial with their cell phones. The limited data reflects that individuals, when *228 surveyed, “overwhelmingly expressed agreement with precedent limiting invasions of communications privacy.”³³⁴ In one survey, 63.1% of participants agreed with the decision in *Katz* requiring a warrant to record a phone conversation.³³⁵ That rate went up to 91.7% if the phone in question was the participant's cell phone.³³⁶

Some scholars have asserted that the Supreme Court's determinations of what constitutes “reasonable expectations of privacy” “are often not in tune with commonly held values.”³³⁷ The limited existing quantitative research supports this claim. For example, 85.5% of respondents in one survey disagreed with *United States v. Knott*,³³⁸ in which the Supreme Court upheld the warrantless installation of a tracking device on a vehicle.³³⁹ Similarly, in a poll of Californians, 73 percent “favor a law that required the police to convince a judge that a crime has been committed before obtaining location information from the cell phone company.”³⁴⁰ Moreover, in a question based on *United States v. Miller*, 85.4% of those surveyed disagreed with the Court's ruling that there is no reasonable expectation of privacy in one's bank records.³⁴¹ These results demonstrate a significant disconnect between the Supreme Court's interpretation of what constitutes a reasonable expectation of privacy in various contexts and individual's actual expectations.

Specifically, several state courts have rejected the applicability of *Miller* pursuant to state constitutions.³⁴² Similarly, various state courts have rejected the reasoning and ruling in *Smith v. Maryland*.³⁴³ In light of numerous state court decisions addressing pen registers, the *229 government's use of a pen register to obtain authorization for cell site simulators is troubling from the perspective of a reasonable expectation of privacy standard. A number of state courts have concluded, based on state constitutions and statutes, that their citizens have such a privacy expectation and that probable cause and a warrant are necessary for a pen register.³⁴⁴ Interestingly, these various state court decisions regarding privacy rights, pen registers, and one's reasonable expectations of privacy were all decided in the 1980s, before the cell phone became ubiquitous in American life. These expectations have not disappeared as pen registers have grown more sophisticated and most people rely exclusively on their cell phones to communicate with others. For example, in *State v. Branigh*,³⁴⁵ the Court of Appeals of Idaho concluded that the defendant “had a reasonable expectation of privacy in the telephone log records that the State obtained from Sprint and that the State's acquisition of those logs was subject to the restraints of [the Idaho Constitution].”³⁴⁶ Moreover, this protection extends to the records documenting the dates, times, and recipients of text messages.³⁴⁷

These state court decisions just start to scratch the surface of various jurisdictions' notions of reasonable expectations of privacy regarding these matters. It stands to reason that if various people around the country have a reasonable expectation of privacy in preventing law enforcement officials from obtaining their telephone call records based on standard pen register requests, then these same people would have similar privacy expectations in any pen register request for a cell site simulator.

*230 That so many state courts and legislatures conclude that there is a reasonable expectation of privacy regarding pen registers further supports the position that a cell site simulator would have a similar, if not stronger, expectation of privacy. Coupled with the fact that the pen register at issue in *Smith v. Maryland* was a significantly less technologically advanced version of the pen registers typically sought today, there is a good argument that the day for reassessment of the continued viability of the decision is coming. One need look no further than the recent issues involving massive electronic searches of American citizens by the NSA to know that many people believe this day has arrived. Indeed, while a pen register in the *Smith v. Maryland* era obtained the only outgoing telephone numbers called, a pen register for a cell phone provides much more

information today, including the telephone numbers dialed for text messages and phone calls; the date, time, duration of such phone calls and text messages; and the location of the cell phone.³⁴⁸

CONCLUSION

The purpose of this Article is not to reject the use of cell site simulators. Indeed, it is clear that these devices can be effective tools in law enforcement arsenals. For example, the use of a cell site simulator near a prison facility can assist in locating a cell phone used by inmates in furtherance of criminal activity.

Nonetheless, there are significant concerns for the privacy rights and interests of third parties. Regarding the applications for the use of cell site simulators, law enforcement officials should minimize the impact that cell site simulators have on such third parties, including by developing a protocol that explains attempts to minimize the invasion of privacy.³⁴⁹

It is clear that an application for a cell site simulator seeks authorization for a device unanticipated by Congress in the pen register statute. “If courts find that the new methods do not fit into the statutory definition, they may follow the lead of those courts who have regarded the new practices as completely unregulated.”³⁵⁰ For law enforcement officials to obtain judicial approval for the use of cell site simulators, they should have to seek authorization pursuant to a search warrant consistent with [Rule 41 of the Federal Rules of Criminal Procedure](#). Alternatively, they can persuade Congress to amend the pen register statute to authorize cell site simulators.

Scholars have long called for Congress to amend the ECPA in order to update it to address the myriad of technological developments in *231 surveillance since 1986.³⁵¹ As Susan Freiwald has asserted, “[t]he ECPA, because it permits a substantial amount of surveillance to proceed without the requirement of a warrant, let alone the heightened procedural safeguards that apply to wiretapping, should have been quite vulnerable to constitutional challenges.”³⁵² Congressional reticence to amend may require that the courts handle the matter of safeguarding the public: “the Supreme Court has taken a hands-off approach to technological development, refusing to recognize Fourth Amendment privacy barriers to its use. However, the Court has sometimes been willing to intervene even at the risk of dramatically changing Fourth Amendment law.”³⁵³ Because the ECPA does not provide a suppression remedy, individuals cannot assert claims for violations of the statute themselves, and the courts become all the more important.³⁵⁴ Such courts are those presided over by magistrate judges who handle the vast majority of these types of requests at their initial stages. Only if these judges safeguard the Constitution and bring a voice to the countless citizens across the country can the reasonable expectations of so many be protected.

Footnotes

¹ Brian L. Owsley, Assistant Professor of Law, Indiana Tech Law School; B.A., 1988, University of Notre Dame; J.D., 1993, Columbia University School of Law; M.I.A., 1994, Columbia University School of International and Public Affairs. From 2005 until 2013, the Author served as a United States Magistrate Judge for the U.S. District Court for the Southern District of Texas. I am very grateful for valuable comments and critiques provided by Steven Friedland, Jonah Horwitz, Stephen Wm. Smith, and Christopher Soghoian.

² See *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. §2703(d)*, 964 F. Supp. 2d 674, 675 (S.D. Tex. 2013).

³ See *id.*

⁴ See generally Marc Rotenberg & David Brody, *Protecting Privacy: The Role of the Courts and Congress*, 39 HUM. RTS. 7 (2013); Jon Campbell, *LAPD Spied on 21 Using StingRay Anti-Terrorism Tool*, L.A. WEEKLY (Jan. 24, 2013), <http://www.laweekly.com/2013-01-24/news/stingray-LAPD-spying-21-terrorism-tool-against-citizens>; Ryan Gallagher, *FBI Files Unlock History Behind Clandestine Cellphone Tracking Tool*, SLATE (Feb. 15, 2013, 2:34 PM), www.slate.com/blogs/future_tense/2013/02/15/stingray_imsi_catcher_fbi_files_unlock_history&uscore;behind_cellphone_tracking.html; John Kelly, *It's*

Not Just the NSA: An Increasing Number of Police Agencies Across the USA Are Snatching Your Cellphone Data, Whether You're a Suspect or Not, USA TODAY, Dec. 9, 2013, at A1; Leslie Meredith, *Law Enforcement Tracks Phones With Phony Cell Towers*, TECH NEWS DAILY (July 12, 2012), <https://web.archive.org/web/20140531131028/http://www.technewsdaily.com/4537-embargoed-law-enforcement-tracks-real-phones-phony-cell-towers.html>; Ellen Nakashima, *Little-Known Surveillance Tool Raises Questions Over Privacy*, WASH. POST, Mar. 28, 2013, at A3; Jennifer Valentino-Devries, ‘*Stingray*’ Phone Tracker Fuels Constitutional Clash, WALL ST. J. (Sept. 22, 2011), <http://online.wsj.com/article/SB1000142405311904194604576583112723197574.html> see also DAEHYUN STROBEL, IMSI CATCHER 1 (2007), available at http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf (“The IMSI Catcher is an expensive device to identify, track and tap a mobile phone user in such a way, that even the network operator cannot notice anything.”).

⁴ HARRIS WIRELESS PRODS. GRP., HARRIS GCSD PRICE LIST, available at <https://info.publicintelligence.net/Harris-SurveillancePriceList.pdf>; Ryan Gallagher, *Meet the Machines That Steal Your Phone's Data*, ARS TECHNICA (Sept. 25, 2013, 10:00 AM), <http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/>.

⁵ See Nakashima, *supra* note 3; Campbell, *supra* note 3; Valentino-Devries, *supra* note 3.

⁶ See STROBEL, *supra* note 3, at 13-15.

⁷ Kelly, *supra* note 3.

⁸ Campbell, *supra* note 3; see Cyrus Farivar, *Local Cops in 15 U.S. States Confirmed to Use Cell Tracking Devices*, ARS TECHNICA (June 12, 2014, 12:32 PM), <http://arstechnica.com/tech-policy/2014/06/local-cops-in-15-us-states-confirmed-to-use-cell-tracking-devices>.

⁹ In response to a request for information on electronic surveillance, Gilbert police officials informed the ACLU about their cell site simulator purchase: “The Gilbert Police Department obtained a \$150,000 grant from the State Homeland Security Program. These funds, along with \$94,195 of R.I.C.O. monies, were used to purchase cell phone tracking equipment in June 2008 (total acquisition cost of [\$] 244,195).” Letter from Kate Weiby, Gilbert Police Legal Advisor, & Tim Dorn, Gilbert Chief of Police, to Dan Pochoda, ACLU (Sept. 6, 2011), available at http://www.aclu.org/files/assets/town_of_gilberts_response_to_prr_re_cell_phone_location_records.pdf; accord Bob Sullivan, *Pricey ‘Stingray’ Gadget Lets Cops Track Cellphones Without Telco Help*, NBC NEWS (Apr. 3, 2012, 2:47 AM), <http://www.nbcnews.com/business/consumer/pricey-stingray-gadget-lets-cops-track-cellphones-without-telco-help-f635294>. Based on the 2010 U.S. Census, Gilbert had an estimated population of 221,140 in 2012. *Gilbert Quick Facts*, U.S. CENSUS BUREAU, <http://quickfacts.census.gov/qfd/states/04/0427400.html> (last visited Dec. 14, 2014).

¹⁰ Allie Bohm, *You're Getting Warmer ...*, ACLU BLOG OF RTS. (Sept. 26, 2011, 2:12 PM), <http://www.aclu.org/blog/technology-and-liberty/youre-getting-warmer>; see MMI Research Ltd. v. Cellxion Ltd., [2012] EWCA (Civ) 7 (Eng.).

¹¹ Campbell, *supra* note 3; Joel Kurth & Lauren Abdel-Razzaq, *Oakland Deputies Use Cellphone Tracker--Military Device Sweeps All Calls Made in Wide Area*, DETROIT NEWS, Apr. 4, 2014, at A6.

¹² Kurth & Abdel-Razzaq, *supra* note 11.

¹³ 442 U.S. 735 (1979).

¹⁴ 425 U.S. 435 (1976).

¹⁵ See Timothy B. Lee, *Documents Show Cops Making Up the Rules on Mobile Surveillance*, ARS TECHNICA (Apr. 3, 2012, 7:40 AM) <http://arstechnica.com/tech-policy/2012/04/documents-show-cops-making-up-the-rules-on-mobile-surveillance>; see also *In re Application of the U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827, 831 (S.D. Tex. 2010) (“[C]ellular telephones use radio waves to communicate between the user's handset and the telephone network.”); *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 750 (S.D. Tex. 2005) (“A cell phone is a sophisticated two-way radio with a low-power transmitter that operates in a network of cell sites.”); Brian Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 3 (2013).

¹⁶ S. REP. NO. 99-541, at 9 (1986), as reprinted in 1986 U.S.C.C.A.N. 3555, 3563; see *In re Application for Pen Register & Trap/Trace Device*, 396 F. Supp. 2d 750 (“‘Cell’ refers to geographic regions often illustrated as hexagons, resembling a bee's honeycomb;

a ‘cell site’ is where the radio transceiver and base station controller are located (at the point three hexagons meet.”); Aaron Blank, *The Limitations and Admissibility of Using Historical Cellular Site Data to Track the Location of a Cellular Phone*, 18 RICH. J.L. & TECH. 3, 4 (2011) (discussing the honeycomb pattern creating cells); Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 126 (2012) (“Service providers maintain large numbers of radio base stations (also called ‘cell sites’) spread through their geographic coverage areas. These cell sites are generally located on ‘cell towers’ serving geographic areas of varying sizes, depending upon topography and population concentration.”).

¹⁷ Ian Herbert, *Where We Are with Location Tracking: A Look at the Current Technology and the Implications on Fourth Amendment Jurisprudence*, 16 BERKELEY J. CRIM. L. 442, 478 (2012) (quoting *In re Application for Pen Register & Trap/Trace Device*, 396 F. Supp. 2d at 749); see Owsley, *supra* note 15, at 3-4.

¹⁸ *In re Application of the U.S. for Historical Cell Site Data*, 747 F. Supp. 2d at 831 (citations omitted).

¹⁹ *Id.*; see Owsley, *supra* note 15, at 4.

²⁰ S. REP. NO. 99-541, at 9; see Pell & Soghoian, *supra* note 16, at 127 (“mobile telephones (as their name suggests) are portable, and so when a phone moves away from the cell site with which it started a call and nearer to a different cell site, the call is ‘handed over’ from one cell site to another without interruption”); Owsley, *supra* note 15, at 4.

²¹ ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the Comm. on the Judiciary, 111th Cong. 13-14 (2010) (statement of Matt Blaze, Associate Professor, University of Pennsylvania); Stephanie K. Pell & Christopher Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap*, 16 YALE J. L. & TECH. 134, 144 (2014); Blank, *supra* note 16, at 5; see Owsley, *supra* note 15, at 5.

²² *In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 534 F. Supp. 2d 585, 590 (W.D. Pa. 2008) (citation omitted), *rev'd on other grounds*, 620 F.3d 304, 313 (3d Cir. 2010); accord Owsley, *supra* note 15, at 5; Kevin McLaughlin, Note, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 HASTINGS COMM. & ENT. L.J. 421, 426 (2007).

²³ Owsley, *supra* note 15, at 5.

²⁴ U.S. DEPT' OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL 41 (rev. 2005) [hereinafter ELECTRONIC SURVEILLANCE MANUAL], available at www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf; see *In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d 113, 115 (E.D.N.Y. 2011) (“Cell phones work by communicating with cell-sites operated by cell-phone service providers. Each cell-site operates at a certain location and covers a certain range of distance.”).

²⁵ *In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d 526, 532 (D. Md. 2011); see Laurie Thomas Lee, *Can Police Track Your Wireless? Call Location Information and Privacy Law*, 21 CARDOZO ARTS. & ENT. L.J. 381, 384-86 (2003) (discussing the FCC's enhanced 9-1-1 regulations); 47 C.F.R. § 20.18(h) (2013) (setting accuracy standards for cell phone calls within targeted distances).

²⁶ ELECTRONIC SURVEILLANCE MANUAL, *supra* note 24, at 41; *In re Application of the U.S. for & Order: (1) Authorizing the Use of a Pen Register & Trap & Trace Device; (2) Authorizing Release of Subscriber & Other Info.; & (3) Authorizing the Disclosure of Location-Based Servs.*, 727 F. Supp. 2d 571, 573 (W.D. Tex. 2010) (cell site location information “is information that resides on computer servers of telecommunications providers”); see *In re Application of the U.S. for an Order Authorizing the Use of a Cellular Tel. Digital Analyzer*, 885 F. Supp. 197, 199 (C.D. Cal. 1995) (“The telephone company uses this information both to bill the subscriber of the cellular telephone based on its usage and also to connect the cellular telephone to the telephone number called.”); Pell & Soghoian, *supra* note 16, at 128 (“Wireless service providers retain detailed logs for diagnostic, billing, and other purposes.”).

²⁷ STROBEL, *supra* note 3, at 3 (“GSM is the most common standard for communication. It is used in more than 200 countries and territories all over the world.”); Karsten Nohl & Chris Paget, *GSM--SRSLY?*, CHAOS COMM'CN CONG. 2 (Dec. 27, 2009), http://events.ccc.de/congress/2009/Fahrplan/attachments/1519_26C3.Karsten.Nohl.GSM.pdf (noting that GSM is used by eighty percent of the cell phone market, with over four billion users).

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 25 of 41

- 28 *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. §2703(d), 964 F. Supp. 2d 674, 675 (S.D. Tex. 2013); see Analysis of IMEI Numbers, INTL NUMBERING PLANS,* <https://www.numberingplans.com/?page=analysis&sub=imeinr> (last visited Dec. 14, 2014) (“All mobile phones are assigned a unique 15 digit IMEI code upon production.”).
- 29 See STROBEL, *supra* note 3, at 4; *see also* GSM--The Base Station Subsystem (BSS), TUTORIALSPOINT, http://www.tutorialspoint.com/gsm/gsm_base_station_subsystem.htm (last visited Dec. 14, 2014).
- 30 STROBEL, *supra* note 3, at 13; David Talbot, A 50-Watt Cellular Network, MIT TECH. REV. (Feb. 10, 2010), <http://www.technologyreview.com/news/417442/a-50-watt-cellular-network>.
- 31 STROBEL, *supra* note 3, at 4.
- 32 *Id.*
- 33 *Id.* at 4-5; *see* Blank, *supra* note 16, at 5-6 (discussing the handoff process).
- 34 STROBEL, *supra* note 3, at 5.
- 35 *Id.*
- 36 See Ryan Gallagher, *Criminals May Be Using Covert Mobile Phone Surveillance Tech for Extortion*, SLATE (Aug. 22, 2012, 9:00 AM), http://www.slate.com/blogs/future_tense/2012/08/22/imsi_catchers_criminals_law_enforcement_using_high_tech_portable_devices_to_intercept_communications_.html.
- 37 Chris Soghoian, Cellular Phones and Mobile Privacy: Direct Government Surveillance (Stingrays), Location Tracking and Biometrics Conference at Yale Law School (Mar. 3, 2013), *available at* <http://www.youtube.com/watch?v=OwutGSjNQ0k>.
- 38 Declan McCullagh, *FBI Prepares to Defend ‘Stingray’ Cell Phone Tracking*, CNET (Mar. 27, 2013, 4:57 PM), http://news.cnet.com/8301-13578_3-57576690-38/fbi-prepares-to-defend-stingray-cell-phone-tracking; Valentino-Devries, *supra* note 3. Interestingly, while the Harris Corporation notes a number of the products and services it provides to customers on its websites, it does not address this electronic surveillance technology. HARRIS, <http://www.harris.com> (last visited Dec. 14, 2014).
- 39 Location Tracking and Biometrics Conference, *supra* note 37; *see* Gallagher, *supra* note 4; *see also* *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 755 (S.D. Tex. 2005) (defining a TriggerFish as a device that “enables law enforcement to gather cell site data directly, without the assistance of the service provider”).
- 40 Location Tracking and Biometrics Conference, *supra* note 37; Nohl & Paget, *supra* note 27.
- 41 STROBEL, *supra* note 3, at 13; *see* MMI Research Ltd. v. Cellxion Ltd., [2012] EWCA (Civ) 7, [4] (Eng.) (“These are devices used by the police and security services to discover the mobile phone numbers of suspected criminals or terrorists. Every mobile phone has an ‘IMSI’ associated with its SIM card, which is its permanent identity number.”).
- 42 STROBEL, *supra* note 3, at 13; *see* Integrated Ratio Communication Network--Rohde & Schwarz, TIARA COMM'NS, <https://web.archive.org/web/20090209050710/http://tiaracom.com.my/rohde&schwarz.htm> (last visited Dec. 14, 2014) (informational sheet from Rohde & Schwarz regarding its IMSI catcher’s capacities).
- 43 STROBEL, *supra* note 3, at 7.
- 44 *Id.* at 13.
- 45 *Id.*; Pell & Soghoian, *supra* note 21, at 145-46; *see* MMI Research, [2012] EWCA (Civ) 7, [5] (Noting the IMSI catcher created by Rohde & Schwarz “involves the creation of a false base station. Mobile phones in a particular area will transmit information to a base station which operates as a transmitter and a receiver to and from the phones. The IMSI catcher uses a false base station which is constructed in a manner which leads the phone to believe it is genuine, and thereby to communicate with it.”).
- 46 STROBEL, *supra* note 3, at 13; Kelly, *supra* note 3; Pell & Soghoian, *supra* note 21, at 147-48.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338

PAGE 26 of 48

47 STROBEL, *supra* note 3, at 13; Blank, *supra* note 16, at 5 (“When a user places a call, the cell phone connects to the cell site with the strongest signal.”).

48 STROBEL, *supra* note 3, at 13.

49 Kelly, *supra* note 3; Jennifer Valentino-Devries, *How ‘Stingray’ Devices Work*, WALL ST. J. (Sept. 21, 2011, 10:33 PM), <http://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work>.

50 Kelly, *supra* note 3; Jon Campbell, *LAPD Spy Device Taps Your Cell Phone*, L.A. WEEKLY (Sept. 13, 2012), <http://www.laweekly.com/2012-09-13/news/LAPD-stingray-spying-cellphone>.

51 Valentino-Devries, *supra* note 49; Campbell, *supra* note 50.

52 *In re Application of the U.S. for an Order Authorizing the Use of a Cellular Tel. Digital Analyzer*, 885 F. Supp. 197, 199 (C.D. Cal. 1995).

53 Valentino-Devries, *supra* note 49; see Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 712-13 (2011) (discussing triangulation).

54 Valentino-Devries, *supra* note 49.

55 *Id.* Pinging is the system by which a cell phone sends out data to register with the nearest cell phone towers. *Id.* See *United States v. Allums*, No. 2:08-CR-30 TS, 2009 WL 806748, at *3 (D. Utah Mar. 24, 2009) (discussing an agent driving around with the device); *United States v. Rigmaiden (Rigmaiden I)*, 844 F. Supp. 2d 982, 995 (D. Ariz. 2012) (“The FBI used the device in multiple locations. The FBI analyzed signals exchanged between the mobile tracking device and the aircard. The FBI would take a reading, move to another location, take another reading, move to another location, etc.”); *United States v. Rigmaiden (Rigmaiden II)*, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *15 (D. Ariz. May 8, 2013) (same).

56 Valentino-Devries, *supra* note 49.

57 *Allums*, 2009 WL 806748, at *1; see Blank, *supra* note 16, at 30-31 (discussing the admissibility of expert testimony by the FBI agent).

58 *Allums*, 2009 WL 806748, at *1.

59 See *Thomas v. State*, 127 So. 3d 658, 660 (Fla. Dist. Ct. App. 2013); Nathan Freed Wessler, *Victory: Judge Releases Information About Police Use of Stingray Cell Phone Trackers*, ACLU (June 3, 2014, 3:12 PM), <https://www.aclu.org/blog/national-security-technology-and-liberty/victory-judge-releases-information-about-police-use>.

60 See Wessler, *supra* note 59.

61 *Rigmaiden I*, 844 F. Supp. 2d 982, 995 (D. Ariz. 2012); *Rigmaiden II*, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *15 (D. Ariz. May 8, 2013).

62 *Rigmaiden I*, 844 F. Supp. 2d at 995; *Rigmaiden II*, 2013 WL 1932800, at *15.

63 See Wessler, *supra* note 59 (noting that Tallahassee police were using a StingRay without a warrant).

64 18 U.S.C. §3123 (2012).

65 Compare *ID. §3123(a)(1)* (a pen register order is issued “if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation”), with *FED. R. CRIM. P.41(d)(1)* (“After receiving an affidavit or other information, a magistrate judge--or if authorized by *Rule 41(b)*, a judge of a state court of record-- must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device.”).

66 See generally ELECTRONIC SURVEILLANCE MANUAL, *supra* note 24, at 38-400.

67 See *United States v. Giordano*, 416 U.S. 505, 511 n.2 (1974) (noting that a pen register is “a device that records telephone numbers dialed from a particular phone”) (emphasis added); see also *id.* at 549 n.1 (Powell, J., concurring in part and dissenting in part) (“A

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 27 of 41

pen register is a mechanical device attached to a given telephone line and usually installed at a central telephone facility. It records on a paper tape all numbers dialed from that line. It does not identify the telephone numbers from which incoming calls originated, nor does it reveal whether any call, either incoming or outgoing, was completed. Its use does not involve any monitoring of telephone conversations.”).

68 434 U.S. 159 (1977).

69 *Id.* at 161 n.1; *see* 18 U.S.C. §3127(3) (2012).

70 434 U.S. at 166; *see* David McPhie, *Almost Private: Pen Registers, Packet Sniffers, and Privacy at the Margin*, 2005 STAN. TECH. L. REV. 1, 8 (“Almost ten years after Title III had been signed into law, the Supreme Court in *United States v. New York Telephone Company* relied on th[e] legislative history and the statutory language in holding that pen registers did not intercept the ‘contents’ of communications, and so did not fall within the scope of Title III.”).

71 *N.Y. Tel.*, 434 U.S. at 166 (quoting 18 U.S.C. § 2518(1) (1976)) (emphasis in original).

72 *Id.* at 168.

73 *Id.* at 168-69; *see* FED. R. CRIM. P. 41(d) (“After receiving an affidavit or other information, a magistrate judge ... must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device.”).

74 *N.Y. Tel.*, 434 U.S. at 170.

75 S. REP. NO. 99-541, at 9 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3557 (“Title III of the bill addresses pen registers.”).

76 Electronics Communications Privacy Act of 1986, Pub. L. No. 99-5088, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.); *In re Application of the U.S. for an Order Authorizing the Use of a Cellular Tel. Digital Analyzer*, 885 F. Supp. 197, 200 (C.D. Cal. 1995) (addressing the statutory definition); *accord United States v. Forrester*, 512 F.3d 500, 512 (9th Cir. 2008) (citing 18 U.S.C. §3127(3) and explaining this pen register definition applied when the surveillance occurred, between May and July 2001); *Donahue v. Gavin*, 280 F.3d 371, 373 n.3 (3d Cir. 2002); *Brown v. Waddell*, 50 F.3d 285, 290 (4th Cir. 1995) (citing 18 U.S.C. §3127(3)); *see U.S. Telecom Ass'n v. FCC*, 227 F.3d 450, 454 (D.C. Cir. 2000) (“Pen registers record telephone numbers of outgoing calls.”).

77 *See generally* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in scattered sections of 47 U.S.C.); *see also* Timothy Casey, *Electronic Surveillance and the Right to Be Secure*, 41 U.C. DAVIS L. REV. 977, 1003 (2008).

78 47 U.S.C. §1002(a)(2)(B) (2011).

79 *See Police Access to Advanced Communication Systems: Hearing Before the Subcomm. on Tech. & the Law of the Comm. on the Judiciary, U.S. S., and the Subcomm. on Civil & Constitutional Rights of the Comm. on the Judiciary, H.R.*, 103d Cong. (1994) (statement of Louis J. Freeh, Director, FBI), available at 1994 WL 223962; *see also In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register*, 415 F. Supp. 2d 211, 216-17 (W.D.N.Y. 2006) (discussing Director Freeh’s testimony); *In re Application of the U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info.*, 412 F. Supp. 2d 947, 955 (E.D. Wis. 2006) (same).

80 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of 8, 12, 15, 18, 20, 31, 42, 47, 49, 50 and 51 U.S.C.); *see In re Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d 448, 455 (S.D.N.Y. 2006) (discussing legislative history).

81 18 U.S.C. §3127(3) (2012); *see United States v. Jadlowe*, 628 F.3d 1, 6 n.4 (1st Cir. 2010) (“A ‘pen register’ is a device used, inter alia, to record the dialing and other information transmitted by a targeted phone.”). The Patriot Act distinguished a pen register from a trap and trace device, which is defined as “a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.” 18 U.S.C. §3127(4).

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 28 of 41

82 18 U.S.C. §3123(b)(1) (2012) (emphasis added); *see* Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1431-32 (2004) ("[T]he statute required the court order to specify the number of the 'telephone line' to which the pen register or trap and trace would be attached.").

83 U.S. DEPT OF JUSTICE, COMPUTER CRIME AND INTELLECTUAL PROP. SECTION, FIELD GUIDANCE ON NEW AUTHORITIES THAT RELATE TO COMPUTER CRIME AND ELECTRONIC EVIDENCE ENACTED IN THE USA PATRIOT ACT OF 2001 4 (2001), available at <https://www.student.cs.uwaterloo.ca/~cs492/papers/ccips.pdf> [hereinafter FIELD GUIDANCE ON NEW AUTHORITIES]; *see* Patricia Mell, *Big Brother at the Door: Balancing National Security with Privacy Under the USA Patriot Act*, 80 DENV. U. L. REV. 375, 402 n.226 (2002).

84 FIELD GUIDANCE ON NEW AUTHORITIES, *supra* note 83, at 4.

85 *See id.* at 5.

86 *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 753 n.8 (S.D. Tex. 2005); accord *In re Application of the U.S. for an Order (1) Authorizing the Use of Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Information and/or Cell Site Information*, 396 F. Supp. 2d 294, 318 (E.D.N.Y. 2005) (adopting the reasoning of *In re Application for Pen Register & Trap/Trace Device*, 396 F. Supp. 2d 747).

87 *In re Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d 448, 456 (S.D.N.Y. 2006); *see In re Application of the U.S. for an Order Authorizing the Use of a Pen Register & Trap on [xxx]Internet Service Account/User Name [[xxxxxxxxxx@xxx.com]*, 396 F. Supp. 2d 45, 49-50 (D. Mass. 2005) ("There can be no doubt that the expanded definition of a pen register, especially the use of the term 'device or process,' encompasses e-mail communications and communications over the internet.") (emphasis in original).

88 United States v. Jadlowe, 628 F.3d 1, 6 n.4 (1st Cir. 2010); *In re Applications of the U.S. for Orders (1) Authorizing the Use of Pen Registers & Trap & Trace Devices & (2) Authorizing Release of Subscriber Info.*, 515 F. Supp. 2d 325, 328 (E.D.N.Y. 2007) ("In layman's terms, a pen register is a device capable of recording all digits dialed from a particular telephone."); *United States v. Bermudez*, No. IP 05-43-CR-B/F, 2006 WL 3197181, at *8 (S.D. Ind. June 30, 2006) (unpublished) ("A 'pen register' records telephone numbers dialed for outgoing calls made from the target phone."); *In re Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d at 455 (pen registers apply to particular cell phones); *In re Application of the U.S. for an Order for Disclosure of Telecomm. Records & Authorizing the Use of a Pen Register & Trap & Trace*, 405 F. Supp. 2d 435, 438 (S.D.N.Y. 2005) ("Pen Register Statute is the statute used to obtain information on an ongoing or prospective basis regarding outgoing calls from a particular telephone."); *In re Application of U.S. for an Order Authorizing Installation & Use of a Pen Register & a Caller Identification Sys. on Tel. Nos. [Sealed] & [Sealed] & the Production of Real Time Cell Site Info.*, 402 F. Supp. 2d 597, 602 (D. Md. 2005) ("A pen register records telephone numbers dialed for outgoing calls from the target phone..."); *In re Application for Pen Register & Trap/Trace Device*, 396 F. Supp. 2d at 752 ("A 'pen register' is a device that records the numbers dialed for outgoing calls made from the target phone.").

89 *See United States v. N.Y. Tel. Co.*, 434 U.S. 159, 170 (1977).

90 *See id.*

91 18 U.S.C. §3122 (2012); *see United States v. Fregoso*, 60 F.3d 1314, 1320 (8th Cir. 1995) ("[U]pon a proper application being made under 18 U.S.C. §3122, 'the court shall enter an ex parte order authorizing the installation' of such a device." (emphasis in original)).

92 *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 846 F. Supp. 1555, 1559 (M.D. Fla. 1994); *see* Mell, *supra* note 83, at 403.

93 Susan Freiwald, *Uncertain Privacy: Communication Attributes After The Digital Telephony Act*, 69 S. CALIF. L. REV. 949, 988-89 (1996).

94 *See* Bellia, *supra* note 82, at 1431 ("[T]he statute does not appear to require the judge to independently assess the factual predicate for the government's certification."); Lee, *supra* note 25, at 397 ("Pen register and trap and trace authority is also problematic in that orders are generally rubberstamped without question."). *But see In re Application of the U.S. for an Order Authorizing the Installation*

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 29 of 41

& Use of a Device [Pen Register], No. 87-0831RC, 1987 WL 8946 (D. Mass. Apr. 3, 1987) (denying a pen register without prejudice due to deficiencies in the application).

95 See Elec. Privacy Info. Ctr. v. FBI, 933 F. Supp. 2d 42 (D.D.C. 2013) (denying the FBI's motion for a stay of deadline to provide responses to Freedom of Information Act requests regarding StingRay); Paul Ohm, *Electronic Surveillance Law and the Intra-Agency Separation of Powers*, 47 U.S.F. L. REV. 269, 275 (2012) (discussing rumors of various types of electronic surveillance, including StingRays, that have ultimately been confirmed); Kurth & Abdel-Razzaq, *supra* note 11; Nathan Freed Wessler, *U.S. Marshals Seize Local Cops' Cell Phone Tracking Files in Extraordinary Attempt to Keep Information From Public*, ACLU (June 3, 2014, 12:13 PM), <https://www.aclu.org/blog/national-security-technology-and-liberty/us-marshals-seize-local-cops-cell-phone-tracking-files> (discussing the federal government's efforts to prevent disclosure of information related to the Sarasota Police Department's use of a cell site simulator).

96 *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d 747, 747 (S.D. Tex. 2012).

97 Owsley, *supra* note 15, at 40; Pell & Soghoian, *supra* note 16, at 158.

98 Ryan Gallagher, *Judge Oks FBI Tracking Tool That Tricks Cellphones with Clandestine Signal*, SLATE (May 9, 2013, 4:35 PM), http://www.slate.com/blogs/future_tense/2013/05/09_stingray_imsi_catcher_judge_oks_fbi_use_of_controversial_tool_in_daniel.html. Obviously, these nondisclosure agreements do not apply to FBI agents seeking judicial authorization. See Wessler, *supra* note 59 (discussing the FBI's attempt to keep sealed testimony about the Tallahassee Police Department's use of a StingRay); Kurth & Abdel-Razzaq, *supra* note 11.

99 Cyrus Farivar, *Legal Experts: Cops Lying About Cell Tracking "Is a Stupid Thing to Do,"* Ars Technica (June 20, 2014, 9:38 PM), <http://arstechnica.com/tech-policy/2014/06/legal-experts-cops-lying-about-cell-tracking-is-a-stupid-thing-to-do>.

100 *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d at 749.

101 E-mail from Magistrate Judge, U.S. District Court for the Eastern District of Texas, to Brian Owsley (Mar. 5, 2013, 10:58 AM) (on file with author).

102 *Id.*

103 See generally *In re Application of the U.S. for an Order Authorizing the Use of a Cellular Tel. Digital Analyzer*, 885 F. Supp. 197 (C.D. Cal. 1995); see also *Fourth Amendment and the Internet: Hearing Before the Subcomm. on the Constitution of the Comm. on the Judiciary H.R.*, 106th Cong. 165-66 (2000), available at http://commdocs.house.gov/committees/judiciary/hju_66503.000/hju66503_0.htm (prepared statement of Robert Corn-Revere, Att'y, Hogan & Hartson L.L.P.) (discussing the decision from the Central District of California).

104 *In re Application for Use of a Cellular Tel. Digital Analyzer*, 885 F. Supp. at 199.

105 *Id.* at 200.

106 *Id.* at 199.

107 *Id.* (discussing *Smith v. Maryland*, 442 U.S. 735, 742-45 (1979)); see Pell & Soghoian, *supra* note 16, at 157-58.

108 *In re Application for Use of a Cellular Tel. Digital Analyzer*, 885 F. Supp. at 199-200; see Freiwald, *supra* note 93, at 988-89 ("The court, having refused to consider the device a pen register since it did not attach to a telephone line, found that no court order of any kind was required to use the device."); *Fourth Amendment and the Internet: Hearing Before the Subcomm. on the Constitution of the Comm. on the Judiciary H.R.*, 106th Cong. 165 (2000) (prepared statement of Robert Corn-Revere, Att'y, Hogan & Hartson L.L.P.) (noting, regarding this decision, that "[c]onsistent with the statutory language and legislative history, reviewing courts have interpreted these provisions literally, and narrowly").

109 *In re Application for Use of a Cellular Tel. Digital Analyzer*, 885 F. Supp. at 201 (discussing §3123(b)(1)(C)).

110 *Id.* at 201.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 20 of 41

- 111 *Id.*
- 112 *Id.* at 202.
- 113 *Id.*
- 114 *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, No. 2:11-mj-00468 (S.D. Tex Apr. 6, 2011).
- 115 *Id.* at 1.
- 116 *Id.* at 2.
- 117 *Id.*
- 118 *Id.* at 1.
- 119 *Id.* at 2.
- 120 Hearing Minutes, *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, No. 2:11-mj-00468 (S.D. Tex. May 6, 2011).
- 121 *Id.* at 2-3.
- 122 *See generally id.*
- 123 Order Granting Mot. to Withdraw, *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, No. 2:11-mj-00468 (S.D. Tex. May 6, 2011).
- 124 *See generally In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d 747 (S.D. Tex. 2012); *see also* Pell & Soghoian, *supra* note 16, at 160-62.
- 125 *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d at 748.
- 126 *Id.*
- 127 *Id.*; *accord* Pell & Soghoian, *supra* note 16, at 161.
- 128 *See In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d at 748.
- 129 *Id.* at 749; *see* ELECTRONIC SURVEILLANCE MANUAL, *supra* note 24, at 38-40.
- 130 *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d at 749.
- 131 *Id.* at 749 n.1.
- 132 *Id.* at 749 (discussing *United States v. Giordano*, 416 U.S. 505, 512 n.2 (1974) and *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 161 n.1(1977)).
- 133 *Id.* at 749.
- 134 *Id.* at 750-51; *see* Gus Hosein & Caroline Wilson Palow, *Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques*, 74 OHIO ST. L.J. 1071, 1102 (2013).
- 135 *In re Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device*, 890 F. Supp. 2d at 751 (discussing 18 U.S.C. § 3123(b)(1)(C)); Pell & Soghoian, *supra* note 16, at 161.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 31 OF 41

- 136 *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device (N.D. Tex. Apr. 5, 2012) (on file with author).
- 137 *Id.*
- 138 *Id.*
- 139 *Id.* at 1-2.
- 140 *Id.* at 2-3.
- 141 *Id.* at 3 (emphasis in original).
- 142 Order Granting, *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device (N.D. Tex. Apr. 5, 2012).
- 143 *Id.* at 2.
- 144 *Id.* (emphasis in original).
- 145 *Id.*
- 146 E-mail from Magistrate Judge, U.S. District Court for the Northern District of Texas, to Brian Owsley (June 4, 2012, 11:49 AM) (on file with author).
- 147 *Id.*
- 148 *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register/Trap & Trace Device, No. [Redacted] (D. Md. Mar. [Redacted], 2012).
- 149 *Id.*
- 150 *Id.* at 2.
- 151 *Id.* at 3 n.4.
- 152 *Id.*
- 153 *Id.* at 3-4, 4 n.5.
- 154 *Id.* at 4.
- 155 *Id.* at 5.
- 156 *Id.* at 3 n.3 (citing *In re* Application of the U.S. for an Order Authorizing the Use of a Cellular Tel. Digital Analyzer, 885 F. Supp. 197 (C.D. Cal. 1995)).
- 157 *Id.*
- 158 *Id.*
- 159 *In re* Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device for the Cellular Telephone Facility Currently Assigned Telephone Number [Redacted], Mag. No. 12-3016 (D.N.J. Feb. 21, 2012).
- 160 *Id.* at 1.
- 161 *Id.*
- 162 *Id.* at 4.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 32 of 41

163 *Id.*

164 See *Rigmaiden I*, 844 F. Supp. 2d 982, 987-88 (D. Ariz. 2012).

165 *Id.* “Air cards are devices that plug into a computer and use the wireless cellular networks of phone providers to connect the computer to the internet. The devices are not phones and therefore don't have the ability to receive incoming calls...” Kim Zetter, *Secrets of FBI Smartphone Surveillance Tool Revealed in Court Fight*, WIRED (Apr. 9, 2013, 6:30 AM), <http://www.wired.com/threatlevel/2013/04/verizon-rigmaiden-aircard/all>.

166 *Rigmaiden I*, 844 F. Supp. 2d at 993.

167 [Proposed] Brief Amici Curiae in Support of Daniel Rigmaiden's Motion to Suppress at 14, *Rigmaiden II*, No. CR 08-814-PHX-DGC, 2013 WL 1932800 (D. Ariz. May 8, 2013).

168 *Rigmaiden I*, 844 F. Supp. 2d at 995.

169 *Id.*

170 *Id.*

171 *Id.*

172 *Id.*

173 *Id.*

174 *Id.* at 995-96.

175 *Rigmaiden II*, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *14 (D. Ariz. May 8, 2013).

176 *Id.*

177 *Id.*

178 *Id.*

179 *Id.* at *16.

180 *Id.*

181 *Id.* at *17.

182 *Id.* at *8-9.

183 *Id.* at *18.

184 *Id.* at *19.

185 *Id.* at *33-34.

186 Soghoian, *supra* note 37.

187 E-mail from Magistrate Judge, U.S. District Court for the Western District of Washington, to Brian Owsley (May 31, 2012, 11:40 AM) (on file with author).

188 E-mail from Magistrate Judge, U.S. District Court for the Eastern District of Texas, to Brian Owsley (Mar. 5, 2013, 10:58 AM) (on file with author).

189 *Id.*

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 33 of 41

- 190 *Id.*
- 191 E-mail from Magistrate Judge, U.S. District Court for the Southern District of California, to Brian Owsley (May 31, 2012, 1:01 PM) (on file with author).
- 192 *Id.*; see [United States v. Espudo](#), 954 F. Supp. 2d 1029, 1045 (S.D. Cal. 2013) (denying as moot a motion to suppress evidence obtained by a cell site simulator where the federal agent testified that the information gathered was not “utilized to further the investigation”).
- 193 *The Office of Enforcement Operations--Its Role in the Area of Electronic Surveillance*, 45 U.S. ATT'Y BULL., no. 5, Sept. 1997, at 8, 11, available at http://www.justice.gov/usao/eousa/foia_reading_room/usab4505.pdf.
- 194 *Id.* at 13 (emphasis in original).
- 195 *Id.* at 13-14.
- 196 *Id.* at 14.
- 197 *Id.*
- 198 *Id.*
- 199 *Id.* (emphasis in original).
- 200 *Id.*
- 201 *Id.*
- 202 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 24, at ii.
- 203 *Id.* at 38-41.
- 204 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 24, at 41. The MIN used to be the same as the assigned cell phone number. [United States v. O'Shield](#), No. 97-2493, 1998 WL 104625, at *1 n.1 (7th Cir. Mar. 6, 1998) (per curiam) (unpublished table decision); [United States v. Bailey](#), 41 F.3d 413, 415 (9th Cir. 1994). Pursuant to Federal Communications Commission policy, these numbers are now separate. [Cellular Telecomms. Indus. Ass'n's Petition for Forbearance from Commercial Mobile Radio Servs. No. Portability Obligations & Tel. No. Portability](#), 14 FCC Rcd. 3092, 3105 (1999); see [Pinney v. Nokia, Inc.](#), 402 F.3d 430, 439-40 (4th Cir. 2005).
- 205 *Id.* at 44.
- 206 *Id.*; compare with [Valentino-Devries](#), *supra* note 49.
- 207 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 24, at 171-74.
- 208 *Id.* at 171.
- 209 *Id.* at 173.
- 210 U.S. ATTORNEY'S OFFICE, DISTRICT OF ARIZ., APPLICATION FOR USE OF AN ELECTRONIC SERIAL NUMBER IDENTIFIER [hereinafter ARIZONA FORM APPLICATION] (2012) (on file with author). Acting United States Attorney Ann Birmingham Scheel served until July 3, 2012, when the new United States Attorney was sworn in. See *Meet the U.S. Attorney*, U.S. DEP'T OF JUSTICE, <http://www.justice.gov/usao/az/meettheattorney.html> (last visited Dec. 14, 2014).
- 211 ARIZONA FORM APPLICATION, *supra* note 210, at 1.
- 212 *Id.*
- 213 *Id.*
- 214 *Id.*

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 34 OF 41

- 215 *Id.* at 1-2.
- 216 *Id.* at 2.
- 217 *Id.* at 4.
- 218 *Id.* at 4-5.
- 219 *Id.* at 5.
- 220 *Id.* at 6.
- 221 *Id.* at 9.
- 222 *Id.* at 10.
- 223 *Id.* at 13-14 (discussing *Smith v. Maryland*, 442 U.S. 735 (1979) and *United States v. Forrester*, 495 F.3d 1041, 1049-50 (9th Cir. 2007)).
- 224 *Id.* at 11.
- 225 *Id.* (quoting 18 U.S.C. §3123(b)(1)(C)).
- 226 *Id.*
- 227 *Id.* at 11-12 (discussing *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Authorization*, 396 F. Supp. 2d 747, 761-62 (S.D. Tex. 2005)).
- 228 *Id.* at 12 (discussing *In re Application for Pen Register & Trap/Trace Device*, 396 F. Supp. 2d at 762).
- 229 *Id.* at 13-15.
- 230 *Id.*
- 231 Letter from Donal Brown, Editor, First Amendment Coal., to Martin Bland, Officer-in-Charge, Discovery Section, L.A. Police Dep't (Sept. 29, 2012) (citing CAL. GOV. CODE §6250, *et seq.*), available at firstamendmentcoalition.org/wp-content/uploads/2013/03/LAPD-CPRA.pdf.
- 232 *Id.*
- 233 *Id.*
- 234 *Id.*
- 235 *Id.*
- 236 *Id.*
- 237 Letter from Martin Bland, Officer-in-Charge, Discovery Section, L.A. Police Dep't, to Donal Brown, Editor, First Amendment Coal. (Dec. 14, 2012), available at firstamendmentcoalition.org/wp-content/uploads/2013/03/LAPD-CPRA.pdf.
- 238 *Id.*
- 239 *Id.*
- 240 *Id.* (citing CAL. GOV. CODE §6255).
- 241 Letter from Martin Bland, Officer-in-Charge, Discovery Section, L.A. Police Dep't, to Donal Brown, First Amendment Coal. (Dec. 28, 2012), available at firstamendmentcoalition.org/wp-content/uploads/2013/03/LAPD-CPRA.pdf.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 35 of 41

²⁴² Memorandum from Kirk J. Albanese, Chief of Detectives, L.A. Police Dep't & Stephen R. Jacobs, Chief of Staff, L.A. Police Dep't to All Commanding Officers (Oct. 16, 2012), *available at* firstamendmentcoalition.org/wp-content/uploads/2013/03/LAPD-CPRA.pdf. Indeed, earlier that year, the Supreme Court had concluded that the attachment of a GPS tracking device to the defendant's car, whereby the government monitored its movement on public streets, constituted a Fourth Amendment search and affirmed the suppression of the resulting evidence. *See United States v. Jones*, 132 S. Ct. 945, 964 (2012).

²⁴³ Memorandum from Kirk J. Albanese & Stephen R. Jacobs to All Commanding Officers, *supra* note 242.

²⁴⁴ Letter from Martin Bland to Donal Brown, *supra* note 241.

²⁴⁵ *Id.*

²⁴⁶ *Id.*

²⁴⁷ *Id.*

²⁴⁸ *Id.*

²⁴⁹ *Id.* at 11-13.

²⁵⁰ 18 U.S.C. §2703(c)(2) (In the Stored Communications Act, Congress authorized law enforcement officials to obtain telecommunications customer records, including "name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such service (including any credit card or bank account number)."); accord *In re §2703(d) Order*, 787 F. Supp. 2d 430, 436 (E.D. Va. 2011); *see In re Application of the U.S. for an Order Pursuant to 18 U.S.C. §2703(d)*, 157 F. Supp. 2d 286, 288 (S.D.N.Y. 2001) (a §2703 order authorized law enforcement officials to obtain "the subscriber's name, home address, telephone number, e-mail address and any other identifying information [the provider] may have, such as date of birth, social security number, driver's license number and billing information"). For a court to issue an order pursuant to §2703(d), the government must demonstrate "*specific and articulable facts* showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are *relevant and material to an ongoing criminal investigation*." 18 U.S.C. § 2703(d) (2013) (emphasis added).

²⁵¹ Letter from Martin Bland to Donal Brown, *supra* note 241, at 11-13.

²⁵² Casey, *supra* note 77, at 983.

²⁵³ U.S. CONST. amend IV.

²⁵⁴ *Id.*; *see FED. R. CRIM. P. 41* (addressing the issuance of warrants, including for the seizure of electronically stored information).

²⁵⁵ Casey, *supra* note 77, at 983.

²⁵⁶ *See, e.g.*, Susan W. Brenner, *The Privacy Privilege: Law Enforcement, Technology, and the Constitution*, 7 J. TECH. L. & POL'Y 123, 150 (2002) ("When the Fourth Amendment was adopted, the protection against invasions of privacy lay in trespass law"); Jace C. Gatewood, *Warrantless GPS Surveillance: Search and Seizure--Using the Right to Exclude to Address the Constitutionality of GPS Tracking Systems Under the Fourth Amendment*, 42 U. MEM. L. REV. 303, 333-34 (2011); Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-first Century*, 65 IND. L.J. 549, 556 n.36 (1990) ("Linking the fourth amendment to its historical context, the Supreme Court during the pre-*Katz* era allowed the law of trespass to control the outcome whenever it was claimed that government had conducted a 'search.'"); David E. Steinberg, *The Uses and Misuses of Fourth Amendment History*, 10 U. PA. J. CONST. L. 581, 583 (2008) ("Historical sources indicate that the Framers were focused on a single, narrow problem: physical trespasses into houses by government agents.").

²⁵⁷ (1765) 95 Eng. Rep. 807 (K.B.); Katz, *supra* note 256, at 556 n.36.

²⁵⁸ Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67, 69 (2012); *see* Fabio Arcila, Jr., *GPS Tracking Out of Fourth Amendment Dead Ends: United States v. Jones and the Katz Conundrum*, 91 N.C. L. REV. 1, 21-22 (2012)

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 36 of 41

("*Katz* famously moved search jurisprudence to a privacy model. It did so by rejecting the property-centric Fourth Amendment model that had previously controlled, and which the Court had applied in *Olmstead v. United States*").

259 [Boyd v. United States, 116 U.S. 616, 618 \(1886\)](#).

260 *Id.* at 622 (emphasis in original).

261 *Id.* at 625-28.

262 [277 U.S. 438, 455 \(1928\)](#).

263 *Id.* at 457 (emphasis added); see Henry F. Fradella, et al., *Quantifying Katz: Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289, 325 (2011) ("The majority rested its decision on the premise that since the wiretapping involved no physical trespass onto the defendants' property, there had been no Fourth Amendment violation.").

264 [Olmstead, 277 U.S. at 463](#).

265 [265 U.S. 57, 59 \(1924\)](#) (holding that defendant's illicit whiskey discovered by revenue officers in an open field on the property of the defendant's father's did not violate the Fourth Amendment); see [United States v. Karo, 468 U.S. 705, 712-13 \(1984\)](#) ("technical trespass" in applying the beeper was insufficient to establish a Fourth Amendment violation).

266 [Olmstead, 277 U.S. at 465](#).

267 *Id.* at 473 (Brandeis, J., dissenting) (quoting [Boyd v. United States, 116 U.S. 616, 630 \(1886\)](#)).

268 [316 U.S. 129 \(1942\)](#).

269 *Id.* at 134.

270 *Id.* at 134-35.

271 *Id.* at 136 (Stone, C.J. & Frankfurter, J., dissenting).

272 *Id.* (Murphy, J., dissenting).

273 [389 U.S. 347 \(1967\)](#).

274 *Id.* at 352; see Owsley, *supra* note 15, at 10 (discussing *Katz*). But see Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 821 (2004) (the question of "[e]xactly why the user of the phone booth was constitutionally entitled to his privacy was left to the reader's imagination") (emphasis in original).

275 [Katz, 389 U.S. at 352](#).

276 *Id.* at 353.

277 *Id.* at 360 (Harlan, J., concurring) ("I join the opinion of the Court, which I read to hold only...that an enclosed telephone booth is an area where, like a home, and unlike a field, a person has a constitutionally protected reasonable expectation of privacy") (citations omitted); see Casey, *supra* note 77, at 988 (discussing Justice Harlan's concurrence).

278 [392 U.S. 1, 9 \(1968\)](#) ("We have recently held that 'the Fourth Amendment protects people, not places'...and wherever an individual may harbor a reasonable 'expectation of privacy.'") (quoting [Katz, 389 U.S. at 351; 389 U.S. at 361](#) (Harlan, J., concurring)).

279 [466 U.S. 109 \(1984\)](#).

280 *Id.* at 113 (citations omitted); see [Rakas v. Illinois, 439 U.S. 128, 144 n.12 \(1978\)](#) ("Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.").

281 Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 316 (2012).

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 337 OF 41

- 282 Kerr, *supra* note 274, at 809-10.
- 283 Kerr, *supra* note 281, at 316-17.
- 284 Bellia, *supra* note 82, at 1382.
- 285 442 U.S. 735 (1979).
- 286 *Id.* at 745-46.
- 287 See Casey, *supra* note 77, at 993 (“The Court’s description of a 1971 pen register [in *Smith*] highlights the dramatic change in the capability of a 2007 pen register.”).
- 288 442 U.S. at 736 n.1; see Casey, *supra* note 77, at 992 (“Significantly, the device did not ‘overhear’ oral communications, and was not capable of determining whether or not the call was completed.”).
- 289 See *California v. Riley*, 134 S. Ct. 2473, 2493 (2014) (distinguishing *Smith* in part because “call logs typically contain more than just phone numbers”).
- 290 See Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 S. ILL. U. L.J. 475, 522 (2012) (“[R]ulings associated with more traditional forms of surveillance do not always comport with society’s actual expectations of privacy and often fail to account for relevant differences between the analogized cases.”).
- 291 Scott Shane & Colin Moynihan, *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.’s*, N.Y. TIMES, Sept. 2, 2013, at A1; John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover up Program Used to Investigate Americans*, REUTERS (Aug. 5, 2013, 3:25 PM), <http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805>.
- 292 547 U.S. 103 (2006).
- 293 *Id.* at 107; see Jeremy A. Blumenthal et al., *The Multiple Dimensions of Privacy: Testing Lay “Expectations of Privacy,”* 11 U. PA. J. CONST. L. 331, 334 (2009).
- 294 *Randolph*, 547 U.S. at 107.
- 295 *Id.* at 122-23 (“This case invites a straightforward application of the rule that a physically present inhabitant’s express refusal of consent to a police search is dispositive as to him, regardless of the consent of a fellow occupant. Scott Randolph’s refusal is clear, and nothing in the record justifies the search on grounds independent of Janet Randolph’s consent.”).
- 296 *Id.* at 128 (Roberts, C.J., dissenting) (“The correct approach to the question presented is clearly mapped out in our precedents: The Fourth Amendment protects privacy. If an individual shares information, papers, or places with another, he assumes the risk that the other person will in turn share access to that information or those papers or places with the government.”) (emphasis in original).
- 297 *Id.* at 129-30 (Roberts, C.J., dissenting).
- 298 *Id.* at 131 (Roberts, C.J., dissenting); see Fradella et al., *supra* note 263, at 293 (“[J]udges make no attempt to discern actual societal opinions when adjudicating Fourth Amendment disputes.”); Blumenthal et al., *supra* note 293, at 332 (judges often “made explicit psychological assumptions about perceptions and expectations of privacy, assumptions that are not necessarily supported by empirical findings”).
- 299 Transcript of Oral Argument at 9-10, *United States v. Jones*, 132 S. Ct. 945 (2012) (No. 10-1259); see Arcila, *supra* note 258, at 40 (discussing this exchange).
- 300 Transcript of Oral Argument, *Jones*, 132 S. Ct. 945 (No. 10-12599).
- 301 A significant majority of individuals surveyed have a reasonable expectation of privacy from electronic tracking of one’s vehicle. See Fradella et al., *supra* note 263, at 325.
- 302 *Randolph*, 547 U.S. at 120.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 38 of 41

303 *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (citing *Smith v. Maryland*, 442 U.S. 735, 742 (1979); *United States v. Miller*, 425 U.S. 435, 443 (1976)).

304 *Id.*

305 *ID. at 961* (Alito, J., concurring in judgment).

306 *Id. at 962.*

307 533 U.S. 27 (2001).

308 *Id. at 36. But see City of Ontario v. Quon*, 560 U.S. 746, 759 (2010) (“The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.”); *see also Owsley, supra* note 15, at 11.

309 *United States v. Davis*, 754 F.3d 1205, 1213 (11th Cir. 2014).

310 *Id. at 1215.*

311 *Id. at 1217.*

312 *California v. Riley*, 134 S. Ct. 2473 (2014).

313 *Id. at 2480.*

314 *Id.*

315 *Id. at 2481.*

316 *Id.*

317 *Id.*

318 *Id.*

319 *Id.*

320 *Id.*

321 *Id. at 2482.*

322 *Id. at 2485.*

323 *Id.*

324 *Id. at 2489.*

325 *Id.*

326 *Id. at 2490.*

327 *Id. at 2495.*

328 425 U.S. 435 (1976).

329 *Id. at 437.*

330 *Id. at 438-39.*

331 *Id. at 445.*

332 *Id. at 440.*

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 39 of 40

333 See Blumenthal et al., *supra* note 293, at 334 (“Little relevant empirical research has been conducted on perceptions of privacy....”); Fradella et al., *supra* note 263, at 338 (“Much more research also needs to be conducted to assess the impact of changes in U.S. surveillance and search and seizure jurisprudence on the privacy rights of citizens.”).

334 Fradella et al., *supra* note 263, at 338.

335 *Id.* at 366.

336 *Id.*

337 Christopher Slobogin & Joseph E. Schumacher, *Rating the Intrusiveness of Law Enforcement Searches and Seizures*, 17 LAW & HUM. BEHAV. 183, 198 (1993).

338 460 U.S. 276 (1983).

339 Fradella et al., *supra* note 263, at 366-67.

340 JENNIFER KING & CHRIS JAY HOOFNAGLE, RESEARCH REPORT: A SUPERMAJORITY OF CALIFORNIANS SUPPORTS LIMITS ON LAW ENFORCEMENT ACCESS TO CELL LOCATION INFORMATION 8 (2008), available at www.ftc.gov/os/comments/mobilevoice/534331-00005.pdf.

341 Fradella et al., *supra* note 263, at 366.

342 See, e.g., *State v. McAllister*, 875 A.2d 866, 875 (N.J. 2005); *State v. Thompson*, 810 P.2d 415, 418 (Utah 1991) (the Utah Constitution provides individuals “a right to be secure against unreasonable searches and seizures of their bank statements”); *Winfield v. Div. of Pari-Mutuel Wagering, Dep’t of Bus. Regulation*, 477 So. 2d 544, 548 (Fla. 1985) (“[T]he law in the state of Florida recognizes an individual’s legitimate expectation of privacy in financial institution records.”); *Charnes v. DiGiacomo*, 612 P.2d 1117, 1121-22, 1124 (Colo. 1980) (en banc) (distinguishing *Miller* and holding that “[a]n individual has an expectation of privacy in records of his financial transactions held by a bank in Colorado.”); *People v. Jackson*, 452 N.E.2d 85, 89 (Ill. App. Ct. 1983) (“[W]e reject the idea set out in *Miller* that a citizen waives any legitimate expectation in her financial records when she resorts to the banking system.”).

343 See, e.g., *Commonwealth v. Melilli*, 555 A.2d 1254, 1258 (Pa. 1989) (expressly rejecting *Smith v. Maryland*); *Richardson v. State*, 865 S.W.2d 944, 951-52, 952 n.6 (Tex. Crim. App. 1993) (rejecting *Smith v. Maryland*).

344 See, e.g., *People v. Sporleder*, 666 P.2d 135, 144 (Colo. 1983) (en banc) (holding that the Colorado Constitution provides a telephone subscriber with a reasonable expectation of privacy in the numbers dialed such that they cannot be obtained without a search warrant based on probable cause); *Shaktman v. State*, 553 So. 2d 148, 151-52 (Fla. 1989) (“Because the pen register intrudes upon fundamental privacy interests [based on the Florida Constitution], the state has the burden of demonstrating both that the intrusion is justified by a compelling state interest and that the state has used the least intrusive means in accomplishing its goal.”); *State v. Rothman*, 779 P.2d 1, 7 (Haw. 1989) (“[P]ersons using telephones in the State of Hawaii have a reasonable expectation of privacy, with respect to the telephone numbers they call on their private lines....”); *State v. Thompson*, 760 P.2d 1162, 1165-67 (Idaho 1988) (a pen register was a search pursuant to the Idaho Constitution and required a warrant); *State v. Hunt*, 450 A.2d 952, 956-57 (N.J. 1982) (the New Jersey Constitution affords individuals the right to privacy in their toll billing records and, by implication, pen register records); *Commonwealth v. Beauford*, 475 A.2d 783, 791 (Pa. Super. 1984) (holding that individuals have a reasonable expectation of privacy in the telephone numbers one dials and the Pennsylvania Constitution protects individuals against the installation of pen registers without a demonstration of probable cause); *State v. Gunwall*, 720 P.2d 808, 813 (Wash. 1986) (en banc) (holding that the Washington Constitution barred the use of a pen register without a search warrant); see also *Richardson v. State*, 865 S.W.2d 944, 953 (Tex. Crim. App. 1993) (en banc) (holding that a pen register may be a search pursuant to the Texas Constitution).

345 313 P.3d 732 (Idaho Ct. App. 2013).

346 *Id.* at 738 (discussing *Thompson*, 760 P.2d at 1165).

347 *Id.*

348 Kelly, *supra* note 3.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 40 of 41

- 349 See Owsley, *supra* note 15, at 46.
- 350 Freiwald, *supra* note 93, at 999-1000; see Bellia, *supra* note 82, at 1382 (“Because application of the Fourth Amendment is in doubt, the statutory rules for acquisition of communications are all the more important. Those provisions, however, reflect significant gaps and ambiguities.”).
- 351 See Bellia, *supra* note 82, at 1458 (noting that Congress “could not have anticipated that technological developments would place so many electronic communications in the hands of third parties” when the ECPA was enacted); Orin Kerr, *A User's Guide to the Stored Communications Act and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004) (addressing areas of potential reform); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1559 (2004) (explaining that the statute “has failed to keep pace with changes in and on the Internet and therefore no longer provides appropriate privacy protections”).
- 352 Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, 4 (2007).
- 353 Arcila, *supra* note 258, at 49.
- 354 See 18 U.S.C. §2708 (2013); see also Freiwald, *supra* note 352, at 4.

66 HSTLJ 183

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 41 of 41

113 Mich. L. Rev. First Impressions 75
Michigan Law Review First Impressions
 April, 2015

SPIES IN THE SKIES: DIRTBOXES AND AIRPLANE ELECTRONIC SURVEILLANCE

Brian L. Owsley^{a1}

Copyright © 2015 Michigan Law Review, Brian L. Owsley

INTRODUCTION

Electronic surveillance in the digital age is essentially a cat-and-mouse game between governmental agencies that are developing new techniques and technologies for surveillance, juxtaposed against privacy rights advocates who voice concerns about such technologies. In November 2014, there was a discovery of a new twist on a relatively old theme.

Recently, the *Wall Street Journal* reported that the U.S. Marshals Service was running a surveillance program employing devices--dirtboxes--that gather all cell phone numbers in the surrounding area.¹ Other federal agencies, including the Drug Enforcement Agency, Immigration and Custom Enforcement, and the Department of Homeland Security, are also documented to have used dirtboxes.² These dirtboxes are manufactured by *76 Digital Receiver Technology (DRT), a subsidiary of Boeing. Dirtboxes get their name based on the acronym of the three letters.³ The U.S. Marshals Service uses these dirtboxes to gather information on the locations or the cell phone numbers of criminal suspects and fugitives.

To understand how dirtboxes are used, imagine you are attending some kind of protest. While you are involved in that event, you notice a small airplane overhead. You think nothing of the airplane and soon turn your attention back to the event. That seemingly innocuous aircraft happens to be a government airplane with a dirtbox aboard. Using this device, law enforcement have been gathering cell phone data from all of those who attended the protest. Perhaps they are looking for a specific individual or two, but now they have your cell phone information along with all the other protestors.

I. DIRTBOX TECHNOLOGY AND OPERATION

A dirtbox is a two-foot-square box that operates like a cell site simulator (also known as a StingRay) by mimicking a cell phone tower.⁴ The device is attached to a small plane such as a Cessna that flies over a target area believed to contain the individual subject of the investigation.⁵ Specifically, “the devices force *every* cell phone in a region to connect to them.”⁶ In order to do so, the device briefly jams the signals of nearby cell towers and then requires all cell phones in a given radius to register with the dirtbox, thus obtaining data from not only the subject of the criminal investigation, but also from all nontargeted cell phone users in the immediate vicinity.⁷

Little information exists about StingRays. There is growing anecdotal evidence in media outlets about the public's concern regarding the use of StingRays,⁸ but the information available in the public record no doubt *77 accounts for just a fraction of the use of such technology. Only a few published decisions have addressed StingRays,⁹ and some courts have dealt with applications for authorization to use StingRays in electronic surveillance.¹⁰ However, it is unknown how often the U.S. Marshals Service or other federal agencies use this technology.

Exhibit 2-C

There are no court decisions addressing the use of dirtboxes. Moreover, it is unclear whether law enforcement officials even seek judicial authorization prior to using dirtboxes. It is unclear how often these flights occur, but they apparently take place on a regular basis.¹¹ With this dearth of information regarding the use of dirtboxes, including the authority for such usage, it is important to consider the constitutional implications of dirtboxes.

II. APPLYING FOURTH AMENDMENT PRINCIPLES TO DIRTBOXES

The Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”¹² It further mandates that “no Warrants shall issue, but upon probable cause.”¹³ As discussed below, the use of a dirtbox constitutes a Fourth Amendment search.¹⁴

***78** Since the 1967 decision in *Katz v. United States*,¹⁵ the Supreme Court has used a “reasonable expectation of privacy” standard to determine whether governmental action constitutes a search pursuant to the Fourth Amendment.¹⁶ In *Terry v. Ohio*,¹⁷ the Supreme Court reiterated and reaffirmed this standard.¹⁸ Furthermore, in *United States v. Jacobsen*,¹⁹ the Court explained that “[a] ‘search’ occurs when an expectation of privacy that society is prepared to consider reasonable is infringed.”²⁰ Thus, a primary question regarding whether dirtboxes constitute a search is if they violate a reasonable expectation of privacy.

The Supreme Court has previously addressed surveillance by airplanes. In *California v. Ciraolo*,²¹ police officers learned that Ciraolo was growing marijuana in the backyard and hiding it from terrestrial view by fences.²² Officers trained in the identification of marijuana flew 1,000 feet above the fenced area and were able to secure photographic evidence of marijuana plants.²³ Based on evidence gathered from this airplane surveillance, police officers obtained a search warrant for the residence, seized seventy-three marijuana plants, and charged Ciraolo with the offense.²⁴ He subsequently filed a motion to suppress the evidence obtained from the warrantless search of his backyard, but the trial court denied his motion, and Ciraolo ultimately pled guilty.²⁵

***79** In analyzing the issue, the *Ciraolo* Court relied on *Katz* to consider whether Ciraolo had a reasonable expectation of privacy.²⁶ The Court found that Ciraolo had a subjective expectation of privacy in his backyard, but that society would not recognize this expectation as reasonable.²⁷ Relying on *United States v. Knotts*,²⁸ the *Ciraolo* Court held that the curtilage of the home does not by itself guarantee protection from law enforcement observation, as police officers are not required to shield their eyes from viewing such areas if they are lawfully entitled to be in the place from which the observation occurs.²⁹ Because the officers were on an airplane in public airspace viewing Ciraolo's property with their naked eyes, the Court concluded that the airplane surveillance did not violate his Fourth Amendment rights.³⁰

Similarly, in *Florida v. Riley*,³¹ the Court again grappled with whether the use of a helicopter to discover marijuana plants violated the Fourth Amendment. The county sheriff received an anonymous tip that Riley was growing marijuana in the greenhouse located on the five acres behind his mobile home.³² Although the greenhouse was obscured on two sides by walls, the other two sides were open but obscured from the ground-level view by trees and the mobile home.³³ Based on the tip, a sheriff's deputy flew 400 feet over the greenhouse and identified marijuana growing with his naked eye.³⁴ As a result, the sheriff's department obtained a search warrant for the greenhouse and located the marijuana, leading to charges against Riley for possession of marijuana.³⁵ The trial court granted Riley's motion to suppress, but the Florida appellate court reversed before certifying the question to the state supreme court, which quashed the reversal and reinstated the trial court's order granting Riley's motion to suppress.³⁶

The *Riley* Court analyzed the question pursuant to *Katz* by addressing whether there was a reasonable expectation of privacy from the surveillance by helicopter.³⁷ Relying on *Ciraolo*, the Court concluded that there was no *80 Fourth Amendment violation because the helicopter was lawfully in the airspace above the property.³⁸

In addition to *Katz*, the Court's third party doctrine jurisprudence informs the question of the constitutionality of dirtboxes. In *Smith v. Maryland*, the Court undermined personal privacy rights by holding that the third party doctrine applied to the numbers that one dials on a telephone. In that case, the Court addressed whether the use of a pen register to obtain the suspect's dialed telephone numbers without a search warrant violated the Fourth Amendment.³⁹ Ultimately, the Court concluded that the installation of the pen register was not a Fourth Amendment search because the suspect had no reasonable expectation of privacy in his outgoing call log.⁴⁰ Moreover, as *Knotts* established a few years later, law enforcement officers have a right to view activity that is clearly visible to the public.⁴¹

Arguably, the combination of *Knotts* and *Smith* would contravene the conclusion that the use of dirtboxes is problematic, but the Court has recently issued a few decisions that call into question the rigidity of the third party doctrine. In *United States v. Jones*,⁴² the Court considered whether law enforcement officers could use GPS to track a criminal suspect without a warrant.⁴³ In writing for the majority, Justice Scalia distinguished *Knotts* from *Jones* because *Knotts* was based on the *Katz* reasonable expectation of privacy test as opposed to common law trespass.⁴⁴

Additionally, in *Riley v. California*, the Court considered whether a police officer's warrantless search of a suspect's cell phone violated the Fourth Amendment.⁴⁵ Because cell phones, which the Court described as minicomputers, have a large storage capacity, they hold very large amounts of private personal records.⁴⁶ Indeed, based on this large storage capacity, the Court concluded that a cell phone could hold thousands of personal records such that it was not analogous to circumstances in earlier third party *81 doctrine cases.⁴⁷ Thus, in holding that the warrantless search of cell phones violated the Fourth Amendment, the Court undercut the third party doctrine.

There are no exceptions to the warrant requirement that apply to searches using dirtboxes. Although cell phone users authorize their cell phones to register with their nearest telecommunications provider's cell towers, that authorization is not the same as consenting to the release of the cell phone user's data to law enforcement using a fake cell tower and dirtbox device. Indeed, the data obtained by the devices, like GPS tracking and cell phone searches, exceeds any basis to justify a search or seizure from the fact that the cell phone registers with cell towers.

III. SAFEGUARDING INDIVIDUALS' REASONABLE EXPECTATIONS OF PRIVACY

Warrantless searches of cell phones using a dirtbox are no different than warrantless searches using a StingRay. At least one court has rejected the use of StingRays without a warrant.⁴⁸ In light of *Riley* and *Jones*, the government should, absent exigent circumstances, obtain a warrant for the use of a StingRay. Similarly, the government should also obtain a search warrant in order to use a dirtbox.

It is unclear what judicial authority, if any, the federal government is seeking when using a dirtbox. In seeking authorization to use a StingRay, the federal government typically bases its application on the pen register statute. However, in order to obtain a pen register "the attorney for the Government" must simply certify "that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."⁴⁹ This is an extremely low standard that results in almost all pen register applications being granted, but is much too low for authorization of a StingRay or a dirtbox because they are capable of obtaining a greater amount of data, some of which is arguably private, from a greater number of citizens.⁵⁰

Instead, judicial authorization of a StingRay or a dirtbox should be based on a probable cause standard and any search warrants issued should state *82 with particularity the areas that may be searched.⁵¹ Similarly, because the use of a dirtbox and the gathering of cell phone data constitute a Fourth Amendment search and seizure, the Fourth Amendment applies to any use of it by the government, whether done in an application or not.

In addition to the search warrant, courts issuing orders authorizing dirtboxes should also be mindful of the capture by law enforcement officials of personal information and data regarding nontargeted individuals. In other words, as the Cessna with the dirtbox swoops near you at the protest, all of your cell phone's data are captured and potentially stored on government computers in perpetuity. To protect against this concern, strict guidelines should be adopted regulating the use and admissibility of information obtained with a dirtbox.

Of course, there may be times in which law enforcement legitimately needs to use an electronic surveillance device like a dirtbox and can satisfy a court's probable cause standard. There still needs to be some protection for gathering data from nontargeted individuals. Consequently, courts should implement a protocol safeguarding these third parties and their data whenever they issue orders authorizing the use of a dirtbox.⁵² For example, a court could order law enforcement officials to "return any and all original records and copies, whether hardcopy or in electronic format or storage, to the Provider, which are determined to be not relevant to the Investigative Agency's investigation."⁵³ Former U.S. Magistrate Judge Facciola explained that a protocol was necessary because "some safeguards must be put in place to prevent the government from collecting and keeping indefinitely information to which it has no right."⁵⁴

CONCLUSION

Dirtboxes are here. Just like Pandora's Box, once they have been opened, they cannot be closed. The goal going forward is not only to ensure that law enforcement officials seek judicial authorization before using them, but also that they comply with the Fourth Amendment. In addition to requiring a demonstration of probable cause along with a particularized search warrant, the issuing court should establish a strict protocol to protect nontargeted individuals from law enforcement officials mining their data. Any protocol should provide guidelines for what to do with this captured data to ensure that it does not end up in government databases.

Footnotes

^{a1} Assistant Professor of Law, Indiana Tech Law School; B.A., University of Notre Dame, J.D., Columbia University School of Law, M.I.A., Columbia University School of International and Public Affairs. From 2005 until 2013, the author served as a United States Magistrate Judge for the United States District Court for the Southern District of Texas. The author recognizes both Charles MacLean and Adam Lamparello for their insightful comments and suggestions.

¹ Devlin Barrett, *Americans' Cellphones Targeted in Secret U.S. Spy Program*, WALL ST. J. (Nov. 13, 2014, 8:22 PM), <http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533> [<http://perma.cc/C95M-A4B5>]; see also Sam Frizell, *Is the Government's Aerial Smartphone Surveillance Program Legal?*, TIME (Nov. 15, 2014), <http://time.com/3586511/government-aerial-surveillance/> [<http://perma.cc/WX9W-JEM4>]; Gail Sullivan, *Report: Secret Government Program Uses Aircraft for Mass Cellphone Surveillance*, WASH. POST, (Nov. 14, 2014), <http://www.washingtonpost.com/news/morningmix/wp/2014/11/14/report-secret-government-program-uses-aircraft-for-mass-cellphonesurveillance/> [<http://perma.cc/578F-RSFS>]; Trevor Timm, *First Snowden. Then Tracking You on Wheels. Now Spies on a Plane. Yes, Surveillance is Everywhere*, GUARDIAN (Nov. 15, 2014, 8:30 AM), <http://www.theguardian.com/commentisfree/2014/nov/15/spies-plane-surveillance-us-marshals> [<http://perma.cc/89HM-VAJE>]; Kim Zetter, *The Feds Are Now Using 'Stingrays' in Planes to Spy on Our Phone Calls*, WIRED (Nov. 14, 2014, 2:14 PM), <http://www.wired.com/2014/11/feds-motherfng-stingrays-motherfng-planes/> [<http://perma.cc/5NDU-WEXR>].

² Timm, *supra* note 1; Patrick Gallagher, *CIA and DOJ May Face Litigation over “Dirtbox” Cell Spying Technology*, JOLT DIGEST (Mar. 17, 2015), <http://jolt.law.harvard.edu/digest/privacy/flash-digest-news-in-brief-180> [<http://perma.cc/BVZ7-BX32>]; Julian Hattem, *Dem Senators Warn Cellphone Tracking Could Violate Constitution*, THE HILL (Dec. 14, 2014, 5:58 PM), <http://thehill.com/policy/technology/226711-dem-senators-fear-cell-trackers-could-violateconstitution> [<http://perma.cc/ULP9-CK8X>].

³ Barrett, *supra* note 1.

⁴ Zetter, *supra* note 1; see also Brian L. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183, 191-94 (2014) (discussing how StingRay devices work); Timm, *supra* note 1 (“The plane surveillance operation’s on-the-ground-forebear[er], commonly known as a [StingRay], ... is like a dirtbox on wheels”).

⁵ Barrett, *supra* note 1.

⁶ Zetter, *supra* note 1.

⁷ Barrett, *supra* note 1; see also Owsley, *supra* note 4, at 191-94.

⁸ See, e.g., Michael Bott & Thom Jensen, *Cellphone Spying Technology Being Used Throughout Northern California*, NEWS10 (Mar. 6, 2014, 11:25 PM), <http://www.news10.net/story/news/investigations/watchdog/2014/03/06/cellphone-spyingtech-nology-used-throughout-northern-california/6144949/> [<http://perma.cc/35UV-M8PR>]; Hanni Fakhoury, *Stingrays Go Mainstream: 2014 in Review*, ELECTRONIC FRONTIER FOUND. (Jan. 2, 2015), <https://www.eff.org/deeplinks/2015/01/2014-review-stingrays-go-mainstream> [<https://perma.cc/7XXU-NAUY>] (discussing discoveries of law enforcement’s use of StingRays in Florida, Maryland, and Washington); Jace Larson, *Houston police chief answers questions about cellphone surveillance program*, KPRC HOUSTON (Nov. 19, 2014, 7:09 p.m.), <http://www.click2houston.com/news/investigates/houston-police-have-cell-phone-surveillance-program/29807376> [<http://perma.cc/VB7M-MTU4>].

⁹ See *In re the Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d 747, 748 (S.D. Tex. 2012); *U.S. v. Rigmaiden*, 844 F. Supp. 2d 982, 995 (D. Ariz. 2012) (FBI used a cell site simulator to track defendant’s Verizon aircard); see also *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 755 (S.D. Tex. 2005) (“[A] ‘TriggerFish’ ... enables law enforcement to gather cell site data directly, without the assistance of the service provider.”); *In re the Application of the U.S. for an Order Authorizing Use of a Cellular Telephone Digital Analyzer*, 885 F. Supp. 197, 198-99 (1995) (“[A] ... ‘digital analyzer’ is a portable device that can detect signals emitted by a cellular telephone.”).

¹⁰ Owsley, *supra* note 4, at 200-11 (discussing StingRay applications in various courts).

¹¹ Barrett, *supra* note 1.

¹² U.S. CONST. amend. IV.

¹³ *Id.*; see also FED. R. CRIM. P. 41 (addressing the issuance of warrants, including for the seizure of electronically stored information).

¹⁴ See *infra* notes 16-46 and accompanying text; see also *Riley v. California*, 134 S. Ct. 2473, 2485 (2014) (holding that the Fourth Amendment requires police officers to obtain a warrant before searching the data on a cell phone).

¹⁵ 389 U.S. 347 (1967).

¹⁶ *Katz*, 389 U.S. 347 at 360 (Harlan, J., concurring) (“I join the opinion of the Court, which I read to hold only ... that an enclosed telephone booth is an area where, like a home, and unlike a field, a person has a constitutionally protected reasonable expectation of privacy” (citations omitted)).

¹⁷ 392 U.S. 1 (1968).

¹⁸ *Terry*, 392 U.S. at 9 (“We have recently held that ‘the Fourth Amendment protects people, not places,’ and wherever an individual may harbor a reasonable ‘expectation of privacy.’” (citations omitted) (quoting *Katz*, 389 U.S. at 351; *Katz*, 389 U.S. at 361 (Harlan, J., concurring))).

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 5 of 7

19 466 U.S. 109 (1984).

20 *Jacobsen*, 466 U.S. at 113 (citations omitted); see also *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978) (“[Legitimate] expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.”).

21 476 U.S. 207 (1986).

22 *Ciraolo*, 476 U.S. at 209.

23 *Id.*

24 *Id.* at 209-10.

25 *Id.* at 210.

26 *Id.* at 211 (citing *Smith v. Maryland*, 442 U.S. 735, 740 (1979)).

27 *Id.* at 211-12.

28 460 U.S. 276 (1983).

29 *Ciraolo*, 476 U.S. at 213 (citing *Knotts*, 460 U.S. at 282).

30 *Id.* at 213-15.

31 488 U.S. 445 (1989).

32 *Riley*, 488 U.S. at 448.

33 *Id.*

34 *Id.*

35 *Id.* at 448-49.

36 *Id.* at 449.

37 *Id.*

38 *Id.* at 449-52.

39 *Smith v. Maryland*, 442 U.S. 735, 741 (1979).

40 *Id.* at 745-46.

41 *United States v. Knotts*, 460 U.S. 276, 282 (1983).

42 132 S. Ct. 945 (2012).

43 *Jones*, 132 S. Ct. at 948.

44 *Id.* at 952 (discussing *Knotts*, 460 U.S. at 278).

45 *Riley v. California*, 134 S. Ct. 2473, 2480 (2014).

46 *Id.* at 2489-91; see also Charles E. MacLean, *But Your Honor, a Cell Phone is not a Cigarette Pack: An Immodest Call for a Return to the Chimel Justifications for Cell Phone Memory Searches Incident to Lawful Arrest*, 6 FED. CTS. L. REV. 41, 62 (2012) (“Cell phones are more like extensive computers than wallets.”); Owsley, *supra* note 4, at 226-27 (noting that the Court viewed cell phones as “essentially small computers that stored immense amounts of data and information”).

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 6 of 7

- 47 *Riley*, 134 S. Ct. at 2493; *see also* MacLean, *supra*, note 46, at 61 (dismissing any analogy because “[a] cell phone can hold millions of pages of data, while a wallet may hold a few”).
- 48 *In re the Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trace & Trace Device*, 890 F. Supp. 2d 747, 752 (S.D. Tex. 2012).
- 49 18 U.S.C. § 3123(a)(1); *see also* 18 U.S.C. § 3122(b)(2); Owsley, *supra* note 4, at 199.
- 50 Owsley, *supra* note 4, at 199-200; Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1431 (2004) (“[T]he statute does not appear to require the judge to independently assess the factual predicate for the government's certification.”).
- 51 Owsley, *supra* note 4, at 230-31; *In re the Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trace & Trace Device*, 890 F. Supp. 2d at 752 (rejecting a StingRay application based on the pen register statute in favor of a search warrant based on the Fourth Amendment).
- 52 See *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 964 F. Supp. 2d 674, 678 (S.D. Tex. 2013) (“Although the use of a court-sanctioned cell tower dump invariably leads to such information being provided to the Government, in order to receive such data, the Government at a minimum should have a protocol to address how to handle this sensitive private information.”); *In re U.S. ex rel. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 930 F. Supp. 2d 698, 702 (S.D. Tex. 2012); *see also* Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 46 (2013) (recommending a protocol be designed for courts authorizing cell tower dumps).
- 53 Cf. *In re Search of Cellular Telephone Towers*, 945 F. Supp. 2d 769, 771 (S.D. Tex. 2013) (giving the same instructions in an order authorizing the government to access historical cell site records at cell towers near a crime scene).
- 54 *In re Search of Information Associated with the Facebook Account Identified by the Username Aaron.Alexis*, 21 F. Supp. 3d 1, 9 (D.D.C. 2013).

113 MILRFI 75

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 7 of 7

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

5 Cal. L. Rev. Circuit 259

California Law Review Circuit

May, 2014

**TO UNSEAL OR NOT TO UNSEAL: THE JUDICIARY'S ROLE IN PREVENTING
 TRANSPARENCY IN ELECTRONIC SURVEILLANCE APPLICATIONS AND ORDERS**

Brian L. Owsley ^{a1}

Copyright © 2014 California Law Review, Inc., Brian L. Owsley

INTRODUCTION

For eight years, I served as a United States magistrate judge in the Corpus Christi Division of the Southern District of Texas. In our division, we dealt with a large number of criminal matters, some of which required me to review sealed applications for search warrants, pen registers, trap and trace devices, and other various forms of electronic surveillance, such as those pursuant to the Stored Communications Act.¹ During my term, I signed orders granting hundreds of such applications,² and all of these applications and orders were *260 routinely sealed at the request of the United States Attorney because they involved ongoing criminal investigations.³

It makes sense that they were initially sealed so as to prevent any targets of the investigation from learning that they were indeed being investigated. Otherwise, these suspects might destroy evidence of their crimes, intimidate witnesses from cooperating, or flee the jurisdiction. Eventually, however, these applications and orders should have been unsealed. Documents are not supposed to remain sealed forever. Indeed, the Supreme Court has explained that, as a general rule, judicial records are to be open to the public, in part so that citizens may “keep a watchful eye on the workings of public agencies.”⁴

The process of unsealing electronic surveillance applications and orders falls squarely within a magistrate judge's duties.⁵ This Essay discusses my experience when I attempted to unseal a number of old applications and orders, and analyzes the ramifications of the judiciary's reluctance to unseal such documents.

I.

**ONE MAGISTRATE JUDGE'S FAILED ATTEMPT TO UNSEAL
 APPLICATIONS FOR ELECTRONIC SURVEILLANCE ORDERS**

In April 2013, as I was taking care of various administrative details before leaving the bench, I decided that I was going to unseal most, if not all, of the electronic surveillance applications and orders that I had considered and signed while I served as a magistrate judge unless there was some compelling reason to keep them sealed, such as an ongoing criminal investigation. I did not view this decision as a particularly controversial one. Moreover, I did not consider the matters involved to be extraordinarily interesting to anyone in particular. I instead thought that if I did not unseal these documents, they were likely to remain sealed for all of eternity. I felt that the reason for keeping most, if not all, of the documents sealed no longer existed because the criminal cases that *261 formed the bases of the applications were long over. I also thought that government works best when it is transparent.

I began the process of unsealing these documents by compiling a list of each sealed application that I had previously handled. I then divided the applications into three groups based on when they were filed. Initially, I issued individual orders for each application in the oldest group, explaining that I would unseal the materials unless I received an objection from the United

Exhibit 2-D

States Attorney within a specified time period. This first group contained applications that were all over five years old, so it was quite likely that the investigations were no longer ongoing if arrests had not been made, as the federal criminal statute of limitations would likely have run. Alternatively, any target that was prosecuted would likely have been convicted and sentenced already. After this first wave of orders, I subsequently issued individual orders in two more waves, addressing the remaining two groups of applications.

While I waited for the government to decide whether to object to the unsealing of any applications, I spoke with the supervisory Assistant United States Attorney for the Corpus Christi office regarding my orders. In response to his questions, I explained that his office did not need to file anything if it did not object to the release. Interestingly, because the files in the first group were so old, his office did not even have records regarding each application. Moreover, because they were all still sealed, the other Assistant United States Attorneys and staff could not review them. Ultimately, the supervisory Assistant United States Attorney filed a single global request in each application affected by my show-cause order seeking authority for staff members to review the applications in the clerk's office in order to get the basic information he felt was necessary to respond to my order.

The deadline to respond to the first wave of orders came and went without any objections from the United States Attorney. Consequently, I issued individual orders instructing the Clerk of the Court to unseal the relevant applications and orders and to make them electronically available. I then turned my attention to other matters.

A few days after issuing the orders to unseal the first wave of applications, one of the district judges summoned me into his chambers. He told me that he had learned of my orders to unseal the various applications and that he was not going to allow them to go forward. We discussed the matter briefly, and I explained that the United States Attorney had not objected to the unsealing. I noted that the orders I had issued only affected old cases. I also told the judge that although the sealing of the documents was necessary when the applications were filed, keeping them sealed was no longer necessary, and the federal Courts, like the rest of the federal government, should operate with some transparency. The judge indicated that the United States Attorney's decision not to object was unimportant because its attorneys could not be relied upon to safeguard the all of the relevant interests. In the end, he issued an order *262 quashing my hundreds of orders to unseal. Additionally, his order contained virtually no reasoning or analysis justifying the continued sealing of any of the applications: "The Order of United States Magistrate Judge Brian Owsley providing for notice of unsealing of orders and associated pen register and trap and trace applications is VACATED. Those orders and their applications will remain sealed until further order of the Court."⁶ Of course, the judge's order was also sealed.⁷

It is unusual that a district judge would sua sponte issue an order quashing orders to unseal. If the United States Attorney had filed a motion before the district judge in response to my original order, seeking to bar me from going forward with the unsealing, then the district judge would be in a proper position to address the matter.⁸ Similarly, if the United States Attorney had filed objections indicating the reasons why the applications should remain sealed, but I had nonetheless ordered that they should be unsealed, then the United States Attorney could appeal my order to the district judge, and the district judge would again be in a proper position to address the matter. However, because no party had sought relief or action from the district judge regarding the matter, it struck me as highly irregular for the judge to intervene. Such an intervention was analogous to a trial court rendering a decision in some action and, without any appeal, the appellate court issuing a ruling reversing the trial judge's decision. Furthermore, he perpetuated the sealing of these hundreds of documents, seemingly without ever reviewing any of them.

The district judge's approach here was additionally problematic because the unsealing of files by a magistrate judge is not only permissible but routinely done.⁹ Indeed, a magistrate judge within the same court, the Southern District of Texas, has routinely unsealed similar applications and orders.¹⁰ This demonstrates magistrate judges are able to unseal such documents and that there is no reason to continue sealing all of these documents. Thus, not only is *263 there a problem with the continued sealing of documents, but there is also a problem in the Court appearing inconsistent and arbitrary in its approach to this issue.

III.

WHY DOES SEALING DOCUMENTS IN PERPETUITY MATTER?

Why is all of this important? Maybe it is not. After all, most of these applications and orders are fairly straightforward and routine. In my experience these applications dealt with common crimes in our division: narcotics trafficking, the smuggling of undocumented aliens, child pornography, etc.¹¹ However, they almost never involved any novel issues of law or high-profile investigations. In other words, they would be of little interest to most people.

Nevertheless, even if no one ever wanted to or wants to view these applications and orders, they should still be unsealed and made available barring some extraordinary circumstance that would justify keeping them sealed.¹² Federal courts do not sit as a Star Chamber, deciding matters while cloaked in secrecy.¹³ Indeed, public policy and the U.S. Constitution favor the unsealing of such documents: “A government operating in the shadow of secrecy stands in complete opposition to the society envisioned by the Framers of our Constitution.”¹⁴

Furthermore, even though the applications and orders were routine on an individual level, the privacy implications of perpetually sealed surveillance orders might alarm the public. One need only look at the recent public uproar over NSA's electronic surveillance program to know that most people are very concerned about these invasions of privacy. Unfortunately, continued sealing of applications and orders regarding pen registers, trap and trace devices, search warrants, and § 2703(d) orders¹⁵ prevents the public from understanding the scope of the matters involved and from serving its role as a check on government action.

***264** Given that these documents should be unsealed, one must consider which parties should be responsible for initiating the process. The failure to request the unsealing of old applications can be attributed partly to inertia. In the narrative that I described, the party originally seeking to have the applications and orders sealed no longer felt they needed to be sealed,¹⁶ but this did not mean that the party would actively seek to have them unsealed. Indeed, during my term, the United States Attorney never requested to unseal any of these types of documents. Busy federal prosecutors rightly focus more on the present and future investigation and prosecution of criminal activity, not the reexamination of long-concluded cases and investigations.

Additionally, the targets of such surveillance would seemingly have some interest in unsealing these applications. However, they often have much more pressing concerns, such as staving off charges or a conviction. Moreover, their defense attorneys have little incentive or strategic basis for wasting time focusing on such applications. Defense attorneys would have received the substantive information obtained through the surveillance orders when an Assistant United States Attorney attempted to use it in the course of prosecution. In addition, federal prosecutors would be required to provide any information that formed the basis for the applications or any exculpatory evidence obtained pursuant to the court orders.¹⁷ Even if defense attorneys were able to unseal and review these applications, the revealed information would be of little benefit for most of them, as there is no suppression remedy.¹⁸

That essentially leaves the courts to monitor and unseal these files when appropriate. However, as my former colleague United States Magistrate Judge Stephen Smith has explained, magistrate judges in the Houston Division of the Southern District of Texas issued 3,886 orders regarding electronic surveillance applications between 1995 and 2007.¹⁹ He further concluded that “[a]s of 2008, 99.8% of those orders remained sealed, long after the underlying criminal investigation was closed.”²⁰ Needless to say, there is also inertia on the part of ***265** federal judges, who, like prosecutors, are busy focusing on pending matters not long-closed ones.

To be sure, almost all of these sealed documents are routine in their focus. Nonetheless, as a whole, they paint a telling picture for those who care to look. One can see what types of crimes are investigated. Additionally, one can ascertain the information

that the United States Attorney typically relies on in filing its applications. Upon review of an application, additional research could reveal whether the subjects of the criminal investigation were ever indicted or convicted, as well as whether they were indicted or convicted of the offense that was originally being investigated.

CONCLUSION

How can the problem of unsealing electronic surveillance applications and orders best be addressed? As one might imagine, the solution lies with federal judges. Ideally, magistrate judges and district judges would ensure sealed documents, including those documents that are routinely unsealed in the applications and orders discussed here, would be routinely unsealed after a reasonable time period. Yet, as a practical matter, many judges just do not consider it an issue.

If judges cannot be relied upon to sort this problem out, what other options remain? Prosecutors and defense attorneys have little incentive to unseal documents. Congress is unlikely to enact any legislation on this issue any time soon.²¹ This essentially leaves the public. Individuals will have to make requests to open up access to the courts. Perhaps these requests can be made in conjunction with media interest and public service organizations just as those groups push for transparency by ensuring that newsworthy controversial hearings are open to the public. Eventually, one would hope that such actions would encourage the courts to return to their proper role in regulating the matter of unsealing these surveillance applications and orders in a more transparent fashion.

Footnotes

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 4 of 6

¹ Brian L. Owsley, Visiting Assistant Professor, Texas Tech University School of Law; BA, 1988, University of Notre Dame; JD, 1993, Columbia University School of Law; MIA, 1994, Columbia University School of International and Public Affairs. From 2005 until 2013, the author served as a United States magistrate judge for the United States District Court for the Southern District of Texas. This article was written in the author's private capacity. No official support or endorsement by the United States District Court for the Southern District of Texas or any other part of the federal judiciary is intended or should be inferred. I am very grateful for valuable comments and critiques provided by Jonah Horwitz and the Hon. Stephen Wm. Smith.

² See generally *FED. R. CRIM. P. 41* (search warrants); *18 U.S.C. § 3122 (2014)* (pen registers and trap and trace devices); *18 U.S.C. § 2703 (2009)* (disclosure of cell phone communications or records).

³ The number of sealed documents pertaining to these requests for electronic surveillance authorization is staggering. By one assessment, federal magistrate judges handle over thirty thousand such applications a year. Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 322 (2012).

⁴ See *Kamakana v. City & Cnty. of Honolulu*, 447 F.3d 1172, 1178 (9th Cir. 2006) (noting that a few narrow categories of documents are sealed by federal courts, including "warrant materials in the midst of a pre-indictment investigation"); *United States v. Ketner*, 566 F. Supp. 2d 568, 589 (W.D. Tex. 2008) (explaining the need to seal documents relating to an investigation "to preserve the integrity of the Government's investigation and prevent witness intimidation").

⁵ Nixon v. Warner Commc'nns, Inc., 435 U.S. 589, 598 (1978) (citations omitted); see also *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 707 F.3d 283, 290 (4th Cir. 2013) ("the common law presumes a right to access *all* judicial records and documents" (emphasis in original)).

⁶ See *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 707 F.3d at 289 (stating that the authority to unseal surveillance applications and orders falls within the additional duties contemplated in the Federal Magistrates Act); see also *In re Search of a Residence which is Situated on a Cul-De-Sac at 14905 Franklin Drive, Brookfield, Wis.*, 121 F.R.D. 78, 79 (E.D. Wis. 1988) ("The power to unseal is concomitant to the authority to seal.").

⁷ Order Vacating Order to Show Cause, *In re the Appl. of the United States for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device; & (2) Authorizing Release of Subscriber & Other Info No. 2:05-MC-50*, et al. (S.D. Tex.

Apr. 19, 2013) (citing 18 U.S.C. § 3123(d)(1)). Section 3123(d)(1) simply reiterates that “the order be sealed until otherwise ordered by the court.”

7 Id.

8 As a general rule, district judges conduct the first-line review of many decisions and orders issued by magistrate judges. However, such review presumes that there is some dispute being raised by a party. *See, e.g.,* 28 U.S.C. § 636(b)(1) (discussing review of a magistrate judge's proposed findings and recommendations only after a party has “serve[d] and file[d] written objections to such proposed findings and recommendations as provided by rules of court”).

9 *See, e.g., Search of a Residence which is Situated on a Cul-De-Sac at 14905 Franklin Drive, Brookfield, Wis., 121 F.R.D. at 79.*

10 *See In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders,* 562 F. Supp. 2d 876 (S.D. Tex. 2008) (holding that a fixed expiration date was to be set as to the sealing and non-disclosure of electronic surveillance orders so that they would be unsealed unless the Government filed a motion to continue the sealing).

11 *See, e.g., In re United States for an Order: (1) Authorizing Installation and Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Information; and (3) Authorizing the Disclosure of Location-Based Services,* No. Misc. 07-127, 2007 WL 3341736 (S.D. Tex. Nov. 7, 2007) (involving a narcotics trafficking investigation).

12 *See In re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders,* 562 F. Supp. 2d at 895 (“As a rule, sealing and non-disclosure of electronic surveillance orders must be neither permanent nor, what amounts to the same thing, indefinite.”).

13 *See Doe v. Tenenbaum,* 900 F. Supp. 2d 572, 609 (D. Md. 2012) (“This Court does not customarily sit as a Star Chamber, resolving of cases under the veil of a virtual seal.”).

14 Detroit Free Press v. Ashcroft, 303 F.3d 681, 710 (6th Cir. 2002); *accord* N.Y. Civil Liberties Union v. N.Y.C. Transit Auth., 684 F.3d 286, 299 (2d Cir. 2012).

15 Like pen registers and search warrants, federal magistrate judges routinely handle § 2703(d) orders, in which the government seeks all types of cellphone and internet subscribers' personal information, including name, address, driver's license number, social security number, and means and source of payment. *See* 18 U.S.C. § 2703(c)(2); *see also* Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 14-15 (2013).

16 In the case of pen registers and trap and trace devices, Congress has mandated that “the order be sealed until otherwise ordered by the court.” 18 U.S.C. 3123(d)(1). Interestingly, orders pursuant to the Stored Communications Act are not automatically sealed. *In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information,* 396 F. Supp. 2d 294, 309 (E.D.N.Y. 2005) (noting that “[t]he SCA does not mention sealing”).

17 *See generally* Brady v. Maryland, 373 U.S. 83 (1963).

18 *See* 18 U.S.C. § 2708 (limiting the remedies for violation of the Stored Communications Act); *accord* United States v. Perrine, 518 F.3d 1196, 1202 (10th Cir. 2008); United States v. Smith, 155 F.3d 1051, 1056 (9th Cir. 1998). Similarly, several federal appellate courts have concluded that there is no suppression remedy for the violation of the pen register statute. *See* United States v. Forrester, 512 F.3d 500, 512-13 (9th Cir. 2008); United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995); United States v. Thompson, 936 F.2d 1249, 1249-50 (11th Cir. 1991); *see also* Owsley, *supra* note 15, at 28-29 (discussing cases in which the Government argued that there was no suppression remedy).

19 Smith, *supra* note 3, at 325.

20 *Id.* at 325-26.

21 *See* Owsley, *supra* note 15, at 42 (noting that Congress is recalcitrant to enact legislation in matters concerning electronic surveillance); *see also* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 681, 687 (2011) (“Historically, Congress has dragged its heels in protecting communications privacy until the courts have demanded it.”).

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 5 of 6

5 CALRC 259

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 6 of 6

Unreported Disposition
Slip Copy, 47 Misc.3d 1201(A), 2015 WL 1295966 (Table), 2015 N.Y. Slip Op. 50353(U)

This opinion is uncorrected and will not be published in the printed Official Reports.

In the Matter of New York Civil Liberties Union, Petitioner,
v.
Erie County Sheriff's Office, , Respondent.

2014/000206
Supreme Court, Erie County
Decided on March 17, 2015

CITE TITLE AS: Matter of New York Civ. Liberties Union v Erie County Sheriff's Off.

ABSTRACT

Records

Freedom of Information Law

Court annulled denial of FOIL request for records concerning respondent Sheriff's acquisition and use of cell site simulator and awarded petitioner counsel fees.

New York Civ. Liberties Union, Matter of, v Erie County Sheriff's Off., 2015 NY Slip Op 50353(U). Records—Freedom of Information Law—Court annulled denial of FOIL request for records concerning respondent Sheriff's acquisition and use of cell site simulator and awarded petitioner counsel fees. (Sup Ct, Erie County, Mar. 17, 2015, NeMoyer, J.)

APPEARANCES OF COUNSEL

APPEARANCES:JOHN NED LIPSITZ, ESQ., MARIKO HIROSE, ESQ., andROBERT HODGSON, ESQ., for Petitioner ANDREA SCHILLACI, ESQ., for Respondent

OPINION OF THE COURT

Patrick H. Nemoyer, J.

PAPERS CONSIDERED:the NOTICE OF PETITION, the VERIFIED PETITION, the MEMORANDUM OF LAW IN SUPPORT OF VERIFIED PETITION, and the AFFIRMATION OF MARIKO HIROSE[, ESQ.,] IN SUPPORT OF VERIFIED PETITION, with annexed exhibits;

the VERIFIED ANSWER TO PETITION;

the AFFIRMATION [of Andrea Schillaci, Esq.] IN OPPOSITION TO PETITIONER'S APPLICATION FOR ARTICLE 78 RELIEF, with annexed exhibits, including the untitled affidavit of Bradley S. Morrison and the untitled affidavit of John W. Greenan;

the MEMORANDUM OF LAW IN OPPOSITION TO PETITIONER'S APPLICATION FOR RELIEF PURSUANT TO ARTICLE 78 OF THE CIVIL PRACTICE LAW AND RULES;

Exhibit 3

the reply AFFIRMATION OF NATHAN WHISTLER[, ESQ.], with annexed exhibits;

the reply AFFIRMATION OF Mariko Hirose[, Esq.], with annexed exhibits;

the REPLY MEMORANDUM OF LAW IN SUPPORT OF VERIFIED PETITION; and

the unredacted documents submitted for the Court's in camera

review under cover letters of February 19 and March 13, 2015.

THE PARTIES AND THE NATURE OF THE PROCEEDING:

Petitioner is the New York Civil Liberties Union. Respondent is the Erie County's Sheriff's Office. By this proceeding, which was brought pursuant to CPLR article 78 in November 2014, petitioner nominally challenges respondent's initial complete denial in July 2014 of petitioner's FOIL request for documents relating to respondent's acquisition and use of a "Stingray" device. As recent circumstances have overtaken the pleadings, however, the proceeding actually seeks judicial review of respondent's subsequent limited or qualified granting of such request in January 2015.

THE BACKGROUND:

The Stingray, which is manufactured by Harris Corporation, a Florida-headquartered electronics firm, is an electronic surveillance device originally developed for military uses but now increasingly in the arsenal of civilian law enforcement agencies. Indeed, the Court is led to believe that use of the device may be an important tool of law enforcement agencies in a wide range of missions that include investigating crimes, apprehending suspects and fugitives, rescuing crime victims, locating missing persons, and assisting citizens in distress.

The Stingray device is a cell site simulator. It and like devices are designed to mimic a cell phone tower in a way that enables the device's user to locate and otherwise target cell phones. Typically, before resorting to use of the device, the law enforcement agents will have obtained information that a particular person's cell phone has a particular connection to a certain criminal investigation or matter of public safety, and will have inferred that ascertaining the precise location of that cell phone might likewise reveal the location of the subject suspect, crime victim, missing person, or person in distress. From the wireless carrier that provides service to that cell phone, the law enforcement officials then typically obtain the phone number and the electronic serial number or identifier that are unique to that cell phone and by or through which the wireless carrier communicates with that phone, specifically with respect to geo-location. The law enforcement agents might typically also obtain from the wireless carrier the location of the permanent cellular tower or towers with which that phone usually communicates or perhaps most recently has communicated, and they might also learn within what general radius and from which direction that cell phone usually communicates or recently has communicated with such cell phone tower or towers. Where usual or recent communication has been with multiple towers near one another, the likely origination area can be more closely delineated by triangulation.

Some such information is then inputted into the device, which can be transported in an aircraft or vehicle or hand-carried by the law enforcement officer to the general area where the cell phone usually is or most recently was used or located. When the device is brought within some range of the cell phone, the device simulates the cell phone tower in such a way that the geo-location signals and other communications that otherwise would have passed between the cell phone and that tower are now diverted to or through the device, i.e., the ersatz tower. By means of range and directionality information displayed on the device's map overlay, the user can approximate the current location of the cell phone and move toward it. As the device is moved closer to the cell phone being tracked, that phone's disclosed location becomes less and less approximate until, eventually, the phone's whereabouts may be relatively pinpointed in a particular public place or behind a particular door.

As the Court understands the workings of the device, the cell phone must be “on,” with some battery life remaining, in order to be located and tracked by the device, but a call need not be in progress. *2 However, as the Court understands things, besides displaying the existence and location of the targeted cell phone in an area, the device simultaneously collects and displays information concerning the existence and location of other cell phones being used nearby on at least that wireless network. Apparently such tracking information can be stored with the help of the device for future review and analysis. Evidently, cell site simulators also can be used to ascertain telephone calling information, such as the time of, the location from which, and the number of the call, and the device apparently allows for storage of that kind of information also for future review and analysis. (The record is not definitive concerning whether cell site simulators in general, and the Stingray or other like products of the Harris Corporation in particular, can be used to monitor the content of cell phone conversations or texts.)

Clearly, even apart from any concerns about the “dragnet” or general search capabilities of the device, its employment by law enforcement officers to acquire information of the foregoing type, even if not especially within the context of a specifically targeted criminal investigation, has implications under the Fourth Amendment and its New York analog, and also under federal or state statutes, such as those set forth in CPL articles 700 and 705, governing the issuance of electronic surveillance warrants and pen register and trap and trace orders. The United States Justice Department is apparently of the view, as are some other law enforcement agencies, civil liberties advocates, and courts, that at the very least a pen register or trap and trace order must be obtained before a cell site simulator may be used to “ping” and thereby approximate the location of a particular cell phone and certainly before ascertaining any calling information (i.e., apart from the content of communications, the capture of which would require an eavesdrop warrant). Further, it may be the case that, depending on the circumstances (such as the non-existence of exigencies), the probable cause and the warrant requirements of the Fourth Amendment may have to be satisfied before law enforcement agencies may lawfully engage in real-time mobile tracking of a particular cell phone to an extent that pinpoints the phone's location within a home or other private place.

THE FOIL REQUEST AND THE RESPONSE(S) THERETO:

All of the foregoing is background explaining petitioner's interest in the particular information that it seeks from respondent. That request for documents or public “records” was made pursuant to article 6 of the Public Officers Law, known as the Freedom of Information Law (or FOIL). That request was dated June 16, 2014 and sought eight categories of records, as follows:

- “1. Records regarding the Sheriffs Office's acquisition of cell site simulators, including invoices, purchase orders, contracts, loan agreements, solicitation letters, correspondence with companies providing the devices, and similar documents. In response to this request, please include records of all contracts, agreements, and communications with Harris Corporation.
2. All requests by the Harris Corporation or any other corporation, or any state or federal agencies, to the Sheriff's Office to keep confidential any aspect of the Sheriff's Office's possession and use of cell site simulators, including any non-disclosure agreements between the Sheriff's Office and the Harris Corporation or any other corporation, or any state or federal agencies, regarding the Sheriff's Office's possession and use of cell site simulators.
3. Policies and guidelines of the Sheriff's Office governing use of cell site simulators, including restrictions on when, where, how, and against whom they may be used, limitations on retention and use of collected data, guidance on when a warrant or other legal process must be obtained, and rules governing when the existence and use of cell site simulators may be revealed to the public, criminal defendants, or judges.
4. Any communications or agreements between the Sheriff's Office and wireless service providers (including AT & T, T-Mobile, Verizon, Sprint Nextel, and U.S. Cellular) concerning use of cell site simulators.
5. Any communications, licenses, or agreements between the Sheriff's Office and the Federal Communications Commission or the New York State Public Service Commission concerning use of cell site simulators.

6. Records reflecting the number of investigations in which cell site simulators were used by the Sheriff's Office or in which cell site simulators owned by the Sheriff's Office were used, and the number of those investigations that have resulted in prosecutions.

7. Records reflecting a list of all cases, with docket numbers if available, in which cell site simulators were used by the Sheriff's Office as part of the underlying investigation or in which cell site simulators owned by the Sheriff's Office were used as part of the underlying investigation.

8. All applications submitted to state or federal courts for search warrants or orders authorizing use of cell site simulators by the Sheriff's Office in criminal investigations or authorizing use of cell site simulators owned by the Sheriff's Office, as well as any warrants or orders, denials of warrants or orders, and returns of warrants associated with those applications. If any responsive records are sealed, please provide documents sufficient to identify the court, date, and docket number for each sealed document."

By letter dated July 6, 2014, respondent denied the FOIL request in its entirety for the following reasons:

- “1. If disclosed it would result in an unwarranted invasion of personal privacy.
- 2. Are trade secrets or are submitted to an agency by a commercial enterprise and if disclosed would cause substantial injury to the competitive position of the subject enterprise.
- 3. Identify a confidential source or disclose confidential information relative to a criminal investigation.
- 4. Reveal criminal investigative techniques.
- 5. Could if disclosed endanger the life and safety of a person.
- 6. Are inter-agency or infra-agency communications.
- 7. If disclosed would jeopardize the agency's capacity to guarantee the security of information technology assets.
- 8. The agency is not in possession of item that you requested.”

The agency's letter did not correlate any particular reason or reasons for the denial with any particular one among the eight distinct requests for records made by petitioner. Upon the return of the petition, the *3 Court was told that all eight reasons for denial pertained to each of the eight requests in their entirety, which of course could never have made any sense, and certainly makes no sense in light of subsequent disclosures. The letter advised petitioner of its right to appeal, a right that petitioner exercised by letter dated July 22, 2014. Respondent admits receiving the letter of appeal and failing to respond to it.

Petitioner commenced this proceeding by the filing of the verified petition on November 18, 2014. In challenging the complete denial of its FOIL request, petitioner complained about respondent's failure to search for records (or certify that it had conducted such a search), to produce responsive records, and to respond to requests for records with particularized reasons for any denials. The petition demanded a judgment directing respondent to comply with its duties under FOIL by searching for and disclosing the records sought, and awarding petitioner reasonable attorneys' fees and litigation costs pursuant to FOIL.

By its verified answer dated January 19, 2015, respondent generally denied any violation of its duties under FOIL and sought the denial/dismissal of the petition. On the same day it drafted its answer, however, respondent belatedly made some disclosures to petitioner and the Court, attaching 21 pages, comprising four documents or groupings of documents, to an e-mail¹ sent by respondent's counsel to petitioner's counsel. Respondent simultaneously appended those pages to the affidavit of respondent's counsel submitted in response to the petition and in support of a request for its dismissal. The first three pages turned over at that juncture are three “Purchase Order[s]” by which respondent requisitioned the purchase of a Kingfish system, a Stingray system,

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 4 of 33

and the proprietary software for each, as well as training classes, from the Harris Corporation on three different dates in 2008 and 2012 for a total price of about \$350,000. On the 12/12/2008 purchase order, two evidently descriptive words or phrases are redacted from respondent's disclosure; on the 06/08/2012 purchase order (which later was "cancelled"), one descriptive phrase, one historical phrase, and three figures (i.e., price data) are redacted; and on the 12/28/2012 purchase order, one historical phrase is redacted. The Court has been furnished with unredacted copies of the 2012 purchase orders, but not of the 2008 purchase order (the original unredacted version of that document having been routinely discarded pursuant to the County's records retention policy, according to respondents' counsel).

The fourth page turned over to petitioner on January 19th is a June 5, 2012 letter by a representative of Harris Corporation to the Erie County Sheriff, which letter basically advertised the sale of certain of the equipment and software in question. That document was somewhat heavily redacted. The Court has been provided with an unredacted version, which shows that the redactions are of product trade names and cursory references to the devices' purposes, features, and capabilities, as well as of the identity and phone number of the letter writer.

The next item disclosed by respondent at that time is an eleven-page document entitled "Harris Government Communication System Division Terms and Conditions of Sale for Wireless Equipment, Software and Services, Effective date: June 25, 2012." That document was disclosed in unredacted form, and thus the Court will not further address it.

Finally, the last document belatedly turned over or disclosed on January 19, 2015 is the June 29, 2012 letter from a certain FBI agent to various officers of respondent. The six-page letter constitutes a "non-disclosure agreement" extracted from the Sheriff's Office by the FBI as a condition of the former's acquiring and using the cell site simulator. The letter turned over to petitioner is redacted of all but its heading, preamble, first paragraph, and signature page. The Court has been provided with an unredacted copy of that document, the gist of which is more fully addressed *infra*.

On January 22, 2015, counsel for petitioner wrote counsel for respondent, seeking clarification of respondent's position with regard to the aforementioned redactions from the documents turned over to *4 petitioner on January 19th. Opposing counsel responded by letter of January 26, 2015, basically setting forth respondent's ostensibly current position with regard to the particular disclosures and redactions from disclosure previously made by respondent on January 19th in response to each specific item of the FOIL request, as well as with regard to the complete withholding of certain documents responsive to that request. Obviously, the new position differs notably from the position set forth in respondent's answer and other formal legal papers, by which respondent initially purported to defend the complete denial of the FOIL request. Given the January 26th letter's sharpening effect upon the issues raised in this proceeding, the Court sets forth that letter in its virtual entirety, as follows:

"1. Records regarding the Sheriff's Office acquisition of cell site simulators, including invoices, purchase orders, contracts, loan agreements, solicitation letters, correspondence with companies providing the devices and similar documents. In response to this request, please include records of all contracts, agreements and communications with Harris Corporation.

RESPONSE: Respondent has identified Purchase Orders no. 4600005905, 4500028732, 4500031273; correspondence from Harris Corporation to the Erie County Sheriff dated June 5, 2012; and Harris Government Communications Systems Division Terms and Conditions of Sale for Wireless Equipment, Software and Services with an effective date of June 25, 2012 as documents responsive to this request. These documents were originally requested by and produced to The Buffalo News in redacted form. Copies of these documents were also provided to Petitioner under cover of correspondence dated January 19, 2015. Redactions were warranted as portions of these documents are exempt from disclosure pursuant to [Public Officers Law §87\(2\)\(e \)\(i, iii and iv\)](#), [Public Officers Law §87\(2\)\(g\)](#), [22 C.F.R. § 121.1](#), 22 C.F.R. Parts 120-130, [22 U.S.C. § 2778](#), and [Executive Order 1363](#).

2. All requests by the Harris Corporation or any other corporation or any state or federal agencies, to the Sheriff's Office to keep confidential any aspect of the Sheriff's Office's [possession and use of cell site simulators, including any non-disclosure

agreements] between the Sheriff's Office and the Harris Corporation or any other corporation, or any state or federal agencies, regarding the Sheriff's Office possession and use of cell site simulators.

RESPONSE: Respondent has identified Harris Government Communications Systems Division Terms and Conditions of Sale for Wireless Equipment, Software and Services with an effective date of June 25, 2012 and the Confidentiality Agreement between the ECSO and the FBI as documents responsive to this request. These documents were provided to Petitioner, without and with redaction respectively, under cover of correspondence dated January 19, 2015. Redactions were warranted as portions of these documents are exempt from disclosure pursuant to [Public Officers Law §87\(2\)\(e \)\(i, iii, and iv\)](#), [Public Officers Law §87\(2\)\(g\)](#), [22 C.F.R. § 121.1](#), 22 C.F.R. Parts 120-130, [22 U.S.C. § 2778](#), and [Executive Order 1363](#).

3. Policies and guidelines of the Sheriff's Office governing use of cell site simulators, including restrictions on when, where, how, and against whom they may be used, limitations on retention and use of collected data, guidance on when a warrant or other legal process must be obtained, and rules governing when the existence and use of cell site simulators may be revealed to the public, criminal defendants, or judges.

RESPONSE: Respondent has conducted a good faith search and responsive documents were identified. *5 These documents are exempt from disclosure pursuant to [Public Officers Law §87\(2\)\(e \)\(i, iii and iv\)](#), [Public Officers Law §87\(2\)\(g\)](#), [22 C.F.R. § 121.1](#), 22 C.F.R. Parts 120-130, [22 U.S.C. § 2778](#), and [Executive Order 1363](#).

4. Any communications or agreements between the Sheriff's Office and wireless service providers including AT & T, [T-Mobile,] Verizon, Sprint Nextel, and U.S. Cellular governing the cell site simulators.

RESPONSE: Respondent has conducted a good faith search and no responsive documents were identified.

5. Any communications, licenses, or agreements between the Sheriff's Office and the Federal Communications Commission or the New York State Public Service Commission concerning use of cell site simulators.

RESPONSE: Respondent has conducted a good faith search and no responsive documents were identified.

6. Records reflecting the number of investigations in which cell site simulators were used by the Sheriff's Office, or in which cell site simulators owned by the Sheriff's Office were used, and the number of those investigations that have resulted in prosecutions.

RESPONSE: Respondent has conducted a good faith search and responsive documents were identified. These documents are exempt from disclosure pursuant to [Public Officers Law §87\(2\)\(e \)\(i, iii and iv\)](#), [Public Officers Law §87\(2\)\(g\)](#), [22 C.F.R. § 121.1](#), 22 C.F.R. Parts 120-

130, [22 U.S.C. § 2778](#), and [Executive Order 1363](#).

7. Records reflecting a list of all cases, with docket numbers if available, in which cell site simulators were used by the Sheriff's Office as part of the underlying investigation or in which cell site simulators owned by the Sheriff's Office were used as part of the underlying investigation.

RESPONSE: Respondent has conducted a good faith search and no responsive documents were identified.

8. All applications submitted to state or federal courts for search warrants or orders authorizing use of the cell site simulators by the Sheriff's Office in criminal investigations or authorizing use of cell site simulators by the Sheriff's Office, as well as any warrants or orders, denials of warrants or orders, and returns of warrants associated with those applications. If any responsive records are sealed, please provide documents sufficient to identify the court, date, and docket number for each sealed document.

RESPONSE: Respondent has conducted a good faith search and no responsive documents were identified."

To recapitulate, in response to the first two of the eight requests, respondent has now disclosed to petitioner the existence of four documents, and has disclosed those documents, albeit with redaction of portions of three of the four. With respect to requests nos. 3 and 6, respondent has acknowledged the *6 existence of responsive documents, but has neither described nor otherwise identified those documents nor turned over any part of them to petitioner, instead merely submitting the documents to this Court for its in camera review. Otherwise, respondent has denied the existence of any documents responsive to FOIL requests nos. 4, 5, 7, and 8. It must be noted that in citing the various federal sources of law as justifications for withholding or redacting certain documents, the reformulated position of respondent, as set forth in the January 26th letter, effectively sets forth the FOIL exemption codified at [Public Officers Law § 89 \(2\) \(a\)](#), which exemption was not invoked by respondent in its July 6th letter (the Court nevertheless will address that FOIL exemption).

Submitted to the Court in camera, as mentioned *supra*, are unredacted versions of the two 2012 purchase orders, the June 5, 2012 letter of Harris Corporation, and the June 29, 2012 letter/non-disclosure agreement between the FBI and respondent. Also included in the in-camera submission but not previously mentioned, except by implication in the January 26th response to request no. 3 (seeking records of respondent's policies and guidelines), is a June 11, 2014 e-mail from one higher-up of respondent to three underlings, to which e-mail is attached a June 11, 2014 two-page "Memorandum" setting forth respondent's "Cellular Tracking Procedures." The nature and contents of that email and policy Memorandum are addressed *infra*.

Also submitted in camera and not previously mentioned, except implicitly in the January 26th response to petitioner's sixth request (for records of investigations involving use of the cell site simulator), is a 47-page set of documents. Each such page constitutes a "Complaint Summary Report" or "Complaint Information" report recording an instance between May 1, 2010 and October 3, 2014 in which the Sheriff's Office's cell site simulator was used to track a cellular phone. Most of those reports set forth or suggest that the cellular tracking was carried out for the purpose of criminal investigation, i.e., to locate a suspect or fugitive or even a crime victim. At least four of the reports, however, recite that the reason for the cellular tracking was to locate a missing person or a potentially suicidal person. A number of the documents do not reveal the precise purpose of the cell phone tracking. Most of the documents recite or suggest that, in conducting the cell phone tracking, respondent was assisting another law enforcement agency at the latter's request. Some but by no means all of the documents recite the name and/or phone number of the person being tracked. Just one of the reports -- the most recent one, in fact -- mentions the obtaining of a pen register or other judicial order as a predicate for engaging in the cellular tracking.

THE LAW:

"The Legislature enacted FOIL to provide the public with a means of access to governmental records in order to encourage public awareness and understanding of and participation in government and to discourage official secrecy" ([Matter of Alderson v New York State Coll. of Agric. & Life Sciences at Cornell Univ.](#), 4 NY3d 225, 230 [2005] [internal quote marks and citation omitted]; see [Perez v City Univ. of New York](#), 5 NY3d 522, 528 [2005] [holding that FOIL guarantees "[t]he people's right to know the process of governmental decision-making and to review the documents . . . leading to determinations"]; see also [Public Officers Law § 84](#) ["(G)oovernment is the public's business and . . . the public . . . should have access to the records of government in accordance with the provisions of (FOIL)"]. To those ends, FOIL imposes a broad duty on government to make its records available to the public (see [Public Officers Law § 84](#) [legislative declaration]; see also [Matter of Gould v New York City Police Dept.](#), 89 NY2d 267, 274-275 [1996]). It is thus well settled that all records of a public agency are presumptively available for public inspection under FOIL, unless the documents in question fall squarely within one of the eight narrow exemptions to disclosure set forth in [Public Officers Law § 87 \(2\)](#) (see [Matter of Capital Newspapers Div. of Hearst Corp. v Burns](#), 67 NY2d 562, 566 [1986]; [Matter of M. Farbman & Sons v New York City Health & Hosps. Corp.](#), 62 NY2d 75, 79-80 [1984]; [Matter of Fink v Lefkowitz](#), 47 NY2d 567, 571 [1979]). Moreover, in order that open government and public *7 accountability be promoted, "FOIL is to be liberally construed and its exemptions narrowly interpreted so that the public is granted maximum access to the records of government" ([Matter of Capital Newspapers v Whalen](#), 69 NY2d 246, 252; see [Buffalo News, Inc. v Buffalo Enterprise Dev. Corp.](#) (84 NY2d 488, 492 [1994]; [Matter of Russo v Nassau County Community Coll.](#), 81 NY2d

690, 697 [1993]). An agency that seeks to withhold documents or portions thereof pursuant to one or more of the statutory exemptions must articulate a “particularized and specific justification” for not disclosing requested documents and moreover must “make a particularized showing that a statutory exemption applies to justify nondisclosure” (*Gould*, 89 NY2d at 273, 275). “[T]he burden rests on the agency to demonstrate that the requested material indeed qualifies for exemption . . . [O]nly where the material requested falls squarely within . . . one of these statutory exemptions may disclosure be withheld” (*Gould*, 89 NY2d at 274-275 [internal quotation marks and citations omitted]). A conclusory contention that an entire category of documents is exempt will not suffice; evidentiary support for that position is required (see *Matter of Washington Post Co. v New York State Ins. Dept.*, 61 NY2d 557, 567 [1984]). In other words, “blanket exemptions for particular types of documents are inimical to FOIL’s policy of open government” (*Gould*, 89 NY2d at 274, citing *Capital Newspapers Div. of Hearst Corp.*, 67 NY2d at 569). Moreover, “just as promises of confidentiality by the [agency] do not affect the status of documents as records, neither do they affect the applicability of any exemption” (*Washington Post Co.*, 61 NY2d at 567). “If the court is unable to determine whether withheld documents fall entirely within the scope of the asserted exemption, it should conduct an in camera inspection of [the] documents and order disclosure of all nonexempt, appropriately redacted material (see, *Matter of Xerox Corp. v Town of Webster*, 65 NY2d 131, 133; *Matter of Farbman & Sons v New York City Health & Hosps. Corp.*, *supra*, 62 NY2d, at 83)” (*Gould*, 89 NY2d at 274).

Rights under FOIL are not determined by the identity or status of the records seeker (see *Matter of Daily Gazette Co. v City of Schenectady*, 93 NY2d 145, 156 [1999]). Indeed, “entitlement to the requested [records] is not contingent upon the showing of some cognizable interest other than that inhering in being a member of the public” (*Matter of Scott, Sardano & Pomeranz v Records Access Officers of City of Syracuse*, 65 NY2d 294, 297 [1985]). Moreover, “access to government records does not depend on the purpose for which the records are sought” (*Gould*, 89 NY2d at 274; see also *Beechwood Restorative Care Ctr. V Signor*, 5 NY3d 436, 440 [2005]).

Applying the foregoing legislative purposes and juridical principles, the Court addresses those issues that remain in dispute between the parties, as follows:

WHETHER RESPONDENT SUFFICIENTLY CERTIFIED THE DILIGENCE OF ITS SEARCH:

The Court must reject petitioner's contention that respondent has not furnished a sufficient certification that a diligent search was made for those records that have been claimed not to exist (see *Public Officers Law § 89 [3]* [a]; cf. *Oddone v Suffolk County Police Dept.*, 96 AD3d 758, 761 [2d Dept 2012]; *Matter of De Fabritis v McMahon*, 301 AD2d 892, 893-894 [3d Dept 2003]; see generally *Beechwood Restorative Care Ctr.*, 5 NY3d at 440-441 [2005] [held: “When faced with a FOIL request, an agency must either disclose the record sought, deny the request and claim a specific exemption to disclosure, or certify that it does not possess the requested document and that it could not be located after a diligent search”]). Certainly, respondent's July 6, 2014 letter denying the FOIL request, by which letter the agency represented that it was “not in possession of item that you requested,” cannot suffice as the requisite certification. For one thing, the statement has been proven untrue by the subsequent disclosures and in-camera submissions made by respondent. More important, though, is the fact that the statement expresses nothing about the diligence of the search for the items.

Nevertheless, as this Court reads the Court of Appeals' decision in *Rattley v New York City Police Dept.*, (96 NY2d 873, 875 [2001]), respondent's counsel's assertion in her January 26, 2015 letter suffices as the essential certification. That letter states in four separate places that respondent had *8 “conducted a good faith search and no responsive documents were identified.” As reasoned in *Rattley*:

“The statute does not specify the manner in which an agency must certify that documents cannot be located. Neither a detailed description of the search nor a personal statement from the person who actually conducted the search is required. Here, the Department satisfied the certification requirement by averring that all responsive documents had been disclosed and that it had conducted a diligent search for the documents it could not locate (*Matter of Gould v New York City Police Dept.*, 89 NY2d 267, 279). To the extent that some courts have held to the contrary, those decisions are not to be followed (see, e.g., *Matter of*

Key v Hynes, 205 AD2d 779; *Matter of Bellamy v New York City Police Dept.*, 272 AD2d 120; *Matter of Sanders v Bratton*, 278 AD2d 10). (*Rattley*, 96 NY2d at 875).

THE PROPRIETY OF THE REDACTIONS FROM THE DISCLOSED DOCUMENTS:

The Purchase Orders:

The purchase orders should have been disclosed in their entirety, without redaction of the various words, phrases, and figures.² The purchase orders (and more particularly the redacted contents) were not "compiled for law enforcement purposes" in the sense meant by the statute but, even if they were, their disclosure would not: "interfere with law enforcement investigations or judicial proceedings"; "identify a confidential source or disclose confidential information relating to a criminal investigation," meaning a particular ongoing one; or "reveal [non- routine] criminal investigative techniques or procedures," meaning techniques a knowledge of which would permit a miscreant to evade detection, frustrate a pending or threatened investigation, or construct a defense to impede a prosecution (see *Public Officers Law § 87* [2] [e] [i], [iii], [iv]; see also *Matter of Fink v Lefkowitz*, 47 NY2d 567, 572 [1979]; *Matter of Moore v Santucci*, 151 AD2d 677, 679 [2d Dept 1989]). Further, the purchase orders (or, more precisely, the information redacted therefrom), although clearly constituting inter-agency materials" (the other agency involved was Erie County and its Office of the Comptroller), amount entirely to "instructions to staff that affect the public" (*Public Officers Law § 87* [g] [ii]). Indeed, the instructions set forth in the purchase orders -- in essence, "Pay this bill of this vendor for this item purchased by the Sheriff's Office at this price" -- was and is of quintessentially compelling interest to and of undeniable impact upon the taxpaying public.

Finally, the Court finds that the purchase orders, and particularly the matters redacted therefrom, are not "specifically exempted from disclosure by state or federal statute"³ (*Public Officers Law § 87* [2] [a]). The Court rejects respondent's argument that the disclosures sought here would, if made, violate a particular federal statute, regulatory scheme, and executive order forbidding (and indeed criminalizing) the export of certain sensitive technology without government license or the illicit revelation of sensitive information about such sensitive technology to foreign nationals. The Court instead is convinced by petitioner's argument that the disclosure of public records pursuant to New York's Freedom of Information Law and the within judicial directive -- even records concerning respondent's ownership and use of a cell site simulator device that itself may or may not be subject to arms/munitions or defense technology export restrictions -- does not amount to the actual export of such arms, munitions, or defense technology. Further, the Court is satisfied by the showing on this record that petitioner, a New York not-for-profit corporation, is not a "foreign person," meaning that the disclosures sought by it pursuant to FOIL would not in fact run afoul of related federal legal restrictions on the revelation of sensitive *9 technical data about export-restricted arms or technology.

The June 5, 2012 letter from Harris Corporation to respondent:

Likewise, the Court concludes that this document ought to have been disclosed in its entirety, without redaction. The letter, and more specifically its redacted verbiage, was not "compiled for law enforcement purposes" in the sense meant by the statute. Even if it was, the Court is certain that its disclosure would not have the prejudicial effect upon a criminal investigation or prosecution that the statute makes the linchpin of the FOIL exemption (see *Public Officers Law § 87* [2] [e] [i]-[iv]). Further, the letter does not qualify as either inter- or intra-agency materials (see *Public Officers Law § 87* [2] [g]), as Harris Corporation does not meet the statutory definition of an "agency" (*Public Officers Law § 86* [3]). Finally, for the reasons stated *supra*, the Court concludes that the disclosures are not specifically precluded by federal legal restrictions on the actual export of military-grade electronic surveillance equipment or the constructive export of technical data about such equipment.

The June 29, 2012 letter/non-disclosure agreement:

Likewise, the Court concludes that this public record ought to have been disclosed in its entirety. As indicated, the agreement was entered into between the FBI and respondent as an apparent pre-condition of respondent's being permitted to acquire and

use the cell site simulator. The gist of the letter is not a recitation of the technological capabilities of the device or even the “hows” and “whens” or the advantages of its use for law enforcement purposes, but rather simply the need for the Sheriff’s Office to avoid disclosing the existence, the technological capabilities, or any use of the device to anyone, lest “individuals who are the subject of investigation . . . employ countermeasures to avoid detection,” thereby endangering the lives and safety of law enforcement officers and others and compromising criminal law enforcement efforts as well as national security. The Court has no difficulty in concluding that the agreement (or, more precisely, each redacted-at-length passage of it) was not “compiled for law enforcement purposes” in the sense meant by the statute ([Public Officers Law § 87 \[2\] \[e\]](#)). Again, even if it was, the Court would conclude that the disclosure of the non-disclosure agreement would not thwart or prejudice any particular ongoing law enforcement investigation or pending prosecution (*see* [Public Officers Law § 87 \[2\] \[e\] \[i\], \[ii\]](#)). Nor, the Court concludes, would the disclosure of the non-disclosure agreement “identify a confidential source or disclose confidential information relating to a criminal investigation,” again meaning a specific ongoing one, or “reveal” other than “routine” “criminal investigative techniques or procedures” (*see* [Public Officers Law § 87 \[2\] \[e\] \[iii\], \[iv\]](#)).

Moreover, the Court must conclude that the document constitutes inter-agency material but nevertheless is not exempt from disclosure pursuant to that exemption inasmuch as it sets forth almost nothing but “instructions to staff that affect the public.” In essence, those instructions are to conceal from the public the existence, technological capabilities, or uses of the device. Indeed, the Sheriff’s Office is instructed, upon the request of the FBI, to seek dismissal of a criminal prosecution (insofar as the Sheriff’s Office may retain influence over it) in lieu of making any possibly compromising public or even case-related revelations of any information concerning the cell site simulator or its use. If that is not an instruction that affects the public, nothing is.

For the reasons summarized *supra*, the Court has no difficulty in concluding that the disclosure of the non-disclosure agreement would not amount to a federally forbidden export of sensitive technology nor a revelation of information about such technology to a foreign person.

THE PROPRIETY OF THE WITHHOLDING OF CERTAIN DOCUMENTS:

The June 11, 2014 Memorandum concerning “Cellular Tracking Procedures”:

That document is a two-page procedural manual for those officers of respondent who are assigned to use the cell site simulator. Again, the Court must conclude that the policy or procedural directive was not “compiled for law enforcement purposes” in the sense meant by the statute. Even if it *10 was, its disclosure would not interfere with or prejudice a particular law enforcement investigation or criminal prosecution, nor would it identify a particular confidential source or disclose particular confidential information, nor would it reveal other than “routine” -- which to the Court merely means somewhat regularly resorted to -- “criminal investigative techniques” ([Public Officers Law § 87 \[2\] \[e\]](#)). Again, the Court concludes that the document constitutes intra-agency materials, but it clearly constitutes or embodies a “final agency policy or determination[]” ([Public Officers Law § 87 \[g\] \[iii\]](#)) and in any event is comprised in its virtual entirety of “instructions to staff that affect the public” ([Public Officers Law § 87 \[g\] \[ii\]](#)). Supporting those characterizations are the policy Memorandum’s rules or instructions that the tracking equipment is to be used only for official law enforcement purposes; that certain records must be made and kept (including notations about who requested the cell phone tracking, what its purpose was, who and which phone were targeted, what legal authority was obtained for the tracking, whether any data was saved); that no data should be saved absent a specific justification; that any saved data should be handled in certain ways and subject to certain procedures prior to and for purposes of any investigative analysis or evidentiary use of such data; and that the foregoing procedures themselves should be kept secret from the public.⁴ Finally, for the reasons stated *supra*, the Court concludes that disclosure of the policy or procedural directive would not violate federal law governing the export of sensitive electronic surveillance technology, or the disclosure of information pertaining thereto to a foreign person.

The Complaint Summary Reports or logs:

The Court concludes that the 47 pages of “Complaint Summary” or “Complaint Information” reports -- i.e., records or logs of occasions on which sheriff’s deputies used the cell site simulator -- likewise must be disclosed pursuant to petitioner’s FOIL request, albeit with the minimal redactions outlined *infra*. The Court concludes that such records have not been shown to be exempt from FOIL pursuant to the first exemption cited by respondent. The Court has no doubt that the records were compiled for law enforcement purposes, i.e., investigating crimes, locating suspects or fugitives, or helping citizens in distress (see [Public Officers Law § 87 \[2\] \[e\]](#)). However, the Court concludes that respondent has not met its burden under FOIL of making the particularized showing necessary to justify withholding any of the 47 reports pursuant to that FOIL exemption. Respondent in particular has not claimed nor shown, in the latter instance by actual evidence, that any of the reports pertain to any specific still-ongoing investigation or pending criminal prosecution, let alone that any such ongoing investigation or prosecution would be interfered with as a result of a disclosure of the pertinent report (see [Public Officers Law § 87 \[2\] \[e\] \[i\]](#)). Moreover, respondent claims, but has not shown by means of any evidence, that disclosure of the reports would identify a confidential source or otherwise disclose confidential information (see [Public Officers Law § 87 \[2\] \[e\] \[iii\]](#)), or would reveal other than routine criminal investigation techniques and procedures (see [Public Officers Law § 87 \[2\] \[e\] \[iv\]](#)). Actually, any reading of the quite cursory reports would refute any such showing by respondent, had such a showing been attempted. The reports do not identify any confidential informants (or even non-confidential witnesses), set forth any confidential information (or even garden-variety statements of witnesses), or set forth any operational procedures of police (even routine procedures).

Likewise, the Court concludes that the second exemption asserted by respondent does not apply to the reports. Clearly, the records in question all constitute inter-agency and/or intra-agency materials (see [Public Officers Law § 87 \[2\] \[g\]](#)). In that connection, the Court notes that each report is in essence a communication between the officer assigned to use the cell site simulator on a particular occasion and *11 that officer’s superiors (see [The New York Times Co. v City of New York Fire Dept.](#), 4 NY3d 477, 487 [2005]). Moreover, a majority of the reports embody or reflect communications between respondent and sister law enforcement agencies. Nonetheless, the reports all clearly fall within the specific exception to that FOIL exemption for “statistical or factual tabulations or data” (see [Public Officers Law § 87 \[2\] \[g\] \[i\]](#)). Indeed, the Court sees almost nothing in any of the reports that could not be regarded as “factual data,” meaning only “objective information, in contrast to opinions, ideas, or advice exchanged as part of the consultative or deliberative process of government decision making” ([Gould](#), 89 NY2d at 277). The complaint summaries are (even at their most detailed) just that -- very brief synopses of those complaints or information, or interagency requests, that led to the Sheriff’s office’s use of its cellular tracking device, and of what resulted, investigatively speaking, when the complaint or information was acted upon.

Finally, the Court again rejects the notion that the reports are exempt from disclosure under FOIL pursuant to other state or federal statute, including federal law prohibiting the export of or revelations about certain sensitive technology (see [Public Officers Law § 87 \[2\] \[a\]](#)).

Although respondent apparently has more recently abandoned the initially raised FOIL exemption available for disclosures that “would constitute an unwarranted invasion of personal privacy under the provisions of” [Public Officers Law § 89 \(2\)](#) ([Public Officers Law § 87 \[2\] \[b\]](#)), the Court sees a need to consider and apply that exemption on its own initiative in the context of two of the complaint summary reports., i.e., those that reflect efforts to find an identified missing person (an 87-year-old dementia case) and prevent an identified person from committing suicide. [Public Officers Law § 89 \(2\)](#) defines the concept of an “unwarranted invasion of personal privacy” as including, but not being limited to, six specific kinds of disclosure, two of which touch upon a person’s “medical” history or information ([Public Officers Law § 89 \[2\] \[b\] \[i\], \[ii\]](#)), and two of which concern “information of a personal nature” that was “reported in confidence to an agency” and/or is “not relevant to the ordinary work” of the agency ([Public Officers Law § 89 \[2\] \[b\] \[iv\], \[v\]](#)). Even in a case in which the statutory definition of an “unwarranted invasion of personal privacy” is not on point, however, the Court nonetheless must decide whether any invasion of privacy is “unwarranted” by balancing the privacy interests at stake against the public interest in disclosure of the information (see [The New York Times Co.](#), 4 NY3d at 485). Engaging in that balancing exercise, and considering the two reports that on their face concern quests to help identified citizens in distress, the Court concludes that disclosure of each report would “constitute an unwarranted invasion of personal privacy” of the missing or suicidal individual -- with particular reference to the individual’s medical and other personal information -- unless the name, address, phone number, and/or vehicle-identification information

of such individual were first redacted from the report ([Public Officers Law § 87 \[2\] \[b\]](#); *see* [Public Officers Law § 89 \[2\]](#)). The Court thus directs the redaction of those two records to the foregoing extent prior to the court-ordered disclosure.

WHETHER PETITIONER IS A PREVAILING PARTY ENTITLED TO ATTORNEYS FEES:

Given that this case at its outset concerned the complete denial of the multi-pronged FOIL request, the Court sees no plausible alternative to denominating petitioner the party that has “substantially prevailed” in the proceeding ([Public Officers Law § 89 \[4\] \[c\]](#)). The Court further sees no alternative but to conclude that “the agency had no reasonable basis for denying access” to the material sought by petitioner and either since voluntarily disclosed or now ordered to be turned over to them ([Public Officers Law § 89 \[4\] \[c\] \[i\]](#)). In any event, the Court must conclude that “the agency failed to respond to a request or appeal within the statutory time” ([Public Officers Law § 89 \[4\] \[c\] \[ii\]](#)). In the foregoing regards, the Court notes that petitioner’s initial FOIL request was met with a blanket denial not merely of the existence of documents that were later conceded to exist, but also of access to various documents that were later turned over to petitioner, at least in redacted form. The Court further notes that there was a complete failure by respondent to do or even say anything in response to petitioner’s administrative appeal of the initial denial (*see* [Public Officers Law § 89 \[4\] \[a\]](#)), a circumstance that *12 violated respondent’s statutory obligation at that stage to “fully explain in writing to the person requesting the record the reason for further denial.” The overriding consideration, however, is that it was only well after the commencement of this proceeding that respondent revealed even the existence of any documents responsive to any of petitioner’s requests, identified any (but no means all) of those documents by nature or title or description, and turned over any of the documents at all, whether in unredacted or redacted form. Clearly, that is not the way things are supposed to work under the statute. Just as clearly, the statutory authorization for an award of attorneys’ fees is designed to deter such unfounded denials and inexcusable delays from occurring in violation of the statute (*see Matter of New York Civ. Liberties Union v City of Saratoga Springs*, 87 AD3d 336, 338 [3d Dept 2011], citing Senate Introducer Mem in Support, Bill Jacket, L 2006, ch 492 at 5). Thus, the Court exercises its discretion to award reasonable counsel fees and litigation costs to petitioner (*see* [Public Officers Law § 89 \[4\] \[c\]](#); *see generally Beechwood Restorative Care Ctr.*, 5 NY3d at 441).

Accordingly, the petition is GRANTED (except insofar as it seeks to compel a further certification), the July 6, 2014 determination of respondent is ANNULLED, and respondent is DIRECTED to disclose to petitioner, in unredacted form, the three purchase orders (or at least the two that still exist in original form), the June 5, 2012 letter, the June 29, 2012 letter/non-disclosure agreement, and the June 11, 2014 Memorandum (and its cover e-mail). With regard to the requested disclosure of the Complaint Summary or Complaint Information reports, respondent is DIRECTED to disclose to petitioner the two reports related to the identified missing person and the identified would-be suicide, but only following the redaction of identifying information about those individuals; in all other instances, respondent is DIRECTED to disclose the reports to petitioner without redaction.

Petitioner is AWARDED reasonable attorneys’ fees and other costs incurred in this proceeding. Petitioner is to submit a quantum meruit application with 30 days of the issuance of this Decision/Judgment, whereupon respondent has 15 days to respond to the application.

SO ORDERED:

HON. PATRICK H. NeMOYER, J.S.C.

FOOTNOTES

Copr. (c) 2015, Secretary of State, State of New York

Footnotes

¹ The Court has not seen that cover email.

- 2 The Court recognizes the claimed loss of an unredacted copy of the 2008 purchase order.
- 3 At the outset, the Court notes its agreement with petitioner's observation that the FBI-drafted non-disclosure agreement is not itself a federal statute specifically exempting anything from disclosure under FOIL pursuant to [Public Officers Law § 87 \(2\) \(a\)](#).
- 4 That last policy rule or instruction is the essence also of the "cover" email dated June 11, 2014, which email also must be turned over to petitioner as intra-agency material that sets forth instructions to staff that affect the public.

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 13 of 13

3 Annotated Patent Digest § 20:42

Annotated Patent Digest (Matthews)

Database updated July 2015

Robert A. Matthews, Jr.

Chapter 20. Utility & Enablement

III. Enablement Under 35 U.S.C.A. § 112(a)

B. Scope of Enablement

[Correlation Table References](#)

§ 20:42. How to make

West's Key Number DigestWest's Key Number Digest, Patents  99**Treatises and Practice Aids**[Moy's Walker on Patents §§ 7:10, 7:12 \(4th ed.\)](#)**Additional References****Eipstein, Modern Intellectual Property CH 6, II, E (2d ed.)**

Under the first prong of the enablement requirement, the patent specification must provide sufficient teaching so one of skill in the art can make the claimed invention. According to the Federal Circuit:

In order to satisfy the enablement requirement of § 112, paragraph 1, the specification must enable one of ordinary skill in the art to practice the *claimed* invention without undue experimentation. Thus, with respect to enablement the relevant inquiry lies in the relationship between the specification, the claims, and the knowledge of one of ordinary skill in the art. If, by following the steps set forth in the specification, one of ordinary skill in the art is not able to replicate the claimed invention without undue experimentation, the claim has not been enabled as required by § 112, paragraph 1.

[National Recovery Technologies, Inc. v. Magnetic Separation Systems, Inc.](#), 166 F.3d 1190, 1196, 49 U.S.P.Q.2d 1671 (Fed. Cir. 1999) (emphasis in original—affirming summary judgment claims lacked an enabling disclosure for having a scope that was broader than that which was enabled).

See also

[Tailored Lighting, Inc. v. Osram Sylvania Products, Inc.](#), 2010 WL 1956547, *9 (W.D. N.Y. 2010) (for a claim directed to an automobile headlight having a “at least one coating on at least one of said surfaces and having a transmittance level in substantial accordance with the formula $T_{(1)} = [D_{(1)} - [S^*_{(1)} \times (1-N)]] / [S_{(1)} \times N]$ wherein $T_{(1)}$ is the transmission of said envelope coating for said wavelength 1 from about 380 to about 780 nanometers, $D_{(1)}$ is the radiance of said wavelength for the desired daylight, $S_{(1)}$ is the radiance of said element at said wavelength at normal incidence to said lamp envelope, $S^*_{(1)}$ is the radiance of said element at said wavelength at non-normal incidence to said lamp envelope, and N is the percentage of visible spectrum radiant energy directed normally towards said exterior surface of said lamp envelope,” and where the court construed the claim to require a coating having a characteristic as given by the recited formula, granting summary judgment of noninfringement because the patentee failed to prove the actual value of two of the parameters, N and $S^*_{(1)}$, but instead the inventor just assumed a value for N and $S^*_{(1)}$, further granting summary judgment finding the claims invalid for lack of enablement since the specification failed to teach one of skill in the art how to make the blub since the value of N and $S^*_{(1)}$ had to be assumed or could only be measured *after* the light blub was made—“... Sylvania argues that because the patent does not sufficiently instruct a person skilled in the art

Exhibit 4

of light-bulb manufacturing as to how to manufacture a light bulb that produces a spectral output similar to daylight at all visible wavelengths, the patent is not enabled. Sylvania contends that the instructions are insufficient because the formula recited in Claim 1 of the '017 patent can not be followed by a bulb manufacturer to make the bulb described in the patent. Sylvania argues that because the N and S*(₁) variables either can not be measured, or can only be determined after an infringing bulb has been manufactured, the formula fails to guide a bulb maker as to what level of transmittance is required for the coating of the bulb. ... In the instant case, I find that the '017 Patent does not meet the enablement requirement of [35 U.S.C.A. § 112](#) because the specification fails to adequately describe how to make a bulb coating with a transmittance level that will achieve the desired results of the patented invention: a bulb which produces a spectral light distribution that is similar to a desired daylight. The '017 Patent claims as novel the ability to create a bulb with a spectral light distribution that is substantially similar to a desired daylight at every wavelength in the viewable spectrum. The Patent further purports to disclose the method for obtaining that result. According to the '017 Patent, the result can be obtained by, *inter alia* making a coating for the bulb that has transmittance characteristics that are in substantial conformity to the formula $T_{(1)} = [D_{(1)} - [S^*_{(1)} \times (1-N)]] / [S_{(1)} \times N]$. As stated above, however, the plaintiff has conceded that the N value of a bulb can not be measured, and instead can only be assumed, and the S*(₁) value can not be measured, but can only be calculated after a coated bulb has been manufactured. The person attempting to make the bulb can then only engage in trial and error to see if he or she can make a bulb with a coating that emits a light that is substantially similar to a desired daylight. Should the maker be successful in doing so, only then can the maker work backwards to determine whether or not the coating of the bulb comports to the formula disclosed in Claim 1. Because the '017 Patent does not describe how to ascertain the appropriate transmittance level for the coating in a manner that can be followed by a person skilled in the art of bulb making, the Patent is not enabled.”)

A specification must enable at least one mode of making the claimed invention. See [§ 20:50 ENABLING OF ANY ONE MODE SUFFICES](#). It need not provide a written description of technological developments in making the claimed invention that arise after the patent application is filed.

[Amgen Inc. v. Hoechst Marion Roussel, Inc., 314 F.3d 1313, 1335, 65 U.S.P.Q.2d 1385 \(Fed. Cir. 2003\)](#) (“[W]here the method is immaterial to the claim, the enablement inquiry simply does not require the specification to describe technological developments concerning the method by which a patented composition is made that may arise after the patent application is filed.’ Thus, the specification’s failure to disclose the later-developed endogenous activation technology cannot invalidate the patent.”—affirming district court’s ruling that claims directed to a DNA product were enabled where patent described at least one way to make claimed product, fact that patent did not disclose a later-developed method to make product, which was used by the accused infringer, was irrelevant to the enablement inquiry)

Westlaw. © 2015 Thomson Reuters. No Claim to Orig. U.S. Govt. Works.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 2 of 2

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

3 Annotated Patent Digest § 20:44

Annotated Patent Digest (Matthews)

Database updated July 2015

Robert A. Matthews, Jr.

Chapter 20. Utility & Enablement

III. Enablement Under 35 U.S.C.A. § 112(a)

B. Scope of Enablement

[Correlation Table References](#)

§ 20:44. How to use

West's Key Number DigestWest's Key Number Digest, Patents  99**Treatises and Practice Aids**[Moy's Walker on Patents §§ 7:13, 7:14 \(4th ed.\)](#)**Additional References****Eipstein, Modern Intellectual Property CH 6, II, E (2d ed.)**

As the second prong of the enablement requirement, a patent specification must teach one of skill in the art how to use the claimed invention. Providing a description that only surmises how the claimed invention could be used, without actual data showing its use, may not suffice. For example, in [In re Cortright, 165 F.3d 1353, 49 U.S.P.Q.2d 1464 \(Fed. Cir. 1999\)](#), the Federal Circuit held that a claim for method of treating baldness by applying BagBalm was enabled because the specification disclosed a working example that showed how much Bag Balm was used and over what time period with a reported result of some regrowth of hair. [165 F.2d at 1359, 49 UPSQ2d at 1468](#). However, a second claim that claimed a method for offsetting the effects of a lower level of male hormones being supplied by the arteries to the papilla of scalp hair by the use of BagBalm was not enabled because the specification did not provide any actual data that low level of male hormones were offset by the use of the BagBalm, but only stated that it “surmised” and “believed” that was the case. [165 F.2d at 1360, 49 UPSQ2d at 1469](#). The court held that because it was not “shown that one of ordinary skill would necessarily conclude from the information expressly disclosed by the written description that the active ingredient reaches the papilla of that offsetting occurs,” the lack of actual observation in the specification was fatal to the how to use prong of the enablement determination. [165 F.2d at 1360, 49 UPSQ2d at 1469](#).

See also

[Rasmussen v. SmithKline Beecham Corp., 413 F.3d 1318, 1323, 75 U.S.P.Q.2d 1297 \(Fed. Cir. 2005\)](#) (“In the context of determining whether sufficient ‘utility as a drug, medicant, and the like in human therapy’ has been alleged, ‘it is proper for the examiner to ask for substantiating evidence unless one with ordinary skill in the art would accept the allegations as obviously correct.’ … [W]here there is ‘no indication that one skilled in [the] art would accept without question statements [as to the effects of the claimed drug products] and no evidence has been presented to demonstrate that the claimed products do have those effects,’ an applicant has failed to demonstrate sufficient utility and therefore cannot establish enablement.”—citations omitted—affirming Board’s ruling that applicant was not entitled to claim priority to several earlier-filed related applications to support claims made in a later application for using a drug called finasteride in a therapeutically effective amount to treat prostate cancer because applications for which the priority claim was sought did not enable one of skill in the art to use finasteride to treat prostate cancer since substantial evidence supported Board’s finding that at the filing dates of the earlier application one of skill did not know that finasteride could be used to treat prostate cancer and the earlier applications did not provide any experimental data to show the successful use of finasteride to treat prostate cancer)

Exhibit 5

[Application of Wilke](#), 50 C.C.P.A. 964, 314 F.2d 558, 563, 136 U.S.P.Q. 435 (1963) (overruled by, [Application of Kirk](#), 54 C.C.P.A. 1119, 376 F.2d 936, 153 U.S.P.Q. 48 (1967)) (finding product claims invalid for failing to teach how to use product even though it taught how to make product)

[In re '318 Patent Infringement Litigation](#), 2008 WL 4376445, *20 (D. Del. Sept. 26, 2008), *aff'd on other grounds*, 583 F.3d 1317, 92 USPQ2d 1385 (Fed. Cir. 2009) (in a bench trial, ruling that claims for treating Alzheimer's disease with galanthamine were invalid for lack of enablement where the specification failed to disclose sufficient parameters of administering the drug to achieve the claimed therapeutic effect, the court noting that since the patentee relied only on the prior art to support the argument that the claims were enabled because the inventor had not completed her testing on the use of the drug to treat the disease until after the notice of allowance for the application had issued, but the court had held that the prior art did not render the claims obvious, the claims could not be both nonobvious over the prior art and enabled by the prior art—"In the case at bar, Dr. Davis stated that, even after conceiving of her invention and constructively reducing it to practice, she 'certainly wasn't sure, and a lot of other people weren't sure[,] that [CIs] would ever work.' As stated in *Rasmusson*, '[i]f mere plausibility were the test for enablement under section 112, applicants could obtain patent rights to 'inventions' consisting of little more than respectable guesses as to the likelihood of their success. When one of the guesses later proved true, the 'inventor' would be rewarded the spoils instead of the party who demonstrated that the method actually worked.' 413 F.3d at 1325. Dr. Davis did not receive any confirming data until after the '318 patent was allowed. In view of the prior art disclosures regarding the flaws of physostigmine in AD treatment, discussed previously in the context of obviousness, it does not follow that a person of ordinary skill in the art, reading the '318 patent, would have recognized that galanthamine would be effective in treating AD in the absence of any experimental proof. Put another way, since plaintiffs rely exclusively on the prior art to establish enablement, the court agrees with defendants that the '318 patent cannot both be nonobvious and enabled. Claim 1 of the '318 patent contains no parameters for the administration of galanthamine to AD patients (aside from a 'therapeutically effective amount'); claim 4 further requires the method of administration to be oral and in the range of 10-2000 mg per day. Plaintiffs assert that 'galanthamine is an old compound for which extensive dosing information existed.' Additionally, Dr. Raskind testified that the standard clinical practice of dose titration could be used to find a therapeutically effective dose of galanthamine. Even assuming this to be the case, this does not correct for the fact that the '318 patent only surmises how the claimed method could be used, rather than teach one of skill in the art how to use the claimed method. [inserted n. 39: In view of 'the complete absence of data supporting the statements which set forth the desired results of the claimed invention,' the application which issued as the '318 patent likely should have been rejected by the examiner for lack of utility in addition to lack of enablement.] The '318 patent is, therefore, invalid for lack of enablement.")

Cf.

[Envirotech Corp. v. Al George, Inc.](#), 730 F.2d 753, 762, 221 U.S.P.Q. 473 (Fed. Cir. 1984) (noting that lack of utility under § 101 may be sustained "when there is a complete absence of data supporting the statements which set forth the desired results of the claimed invention."—vacating finding of invalidity because district court erroneously instructed the jury on the law of utility under § 101)

The Federal Circuit has instructed that the "how to use" requirement serves to insure that only an applicant that gives the public the use of an invention deservedly gets the exclusionary patent rights. The court has stated:

Rasmusson argues that the enablement requirement of section 112 does not mandate a showing of utility or, if it does, it mandates only a showing that it is 'not implausible' that the invention will work for its intended purpose. As we have explained, we have required a greater measure of proof, and for good reason. If mere plausibility were the test for enablement under section 112, applicants could obtain patent rights to 'inventions' consisting of little more than respectable guesses as to the likelihood of their success. When one of the guesses later proved true, the 'inventor' would be rewarded the spoils instead of the party who demonstrated that the method actually worked. That scenario is not consistent with

the statutory requirement that the inventor enable an invention rather than merely proposing an unproved hypothesis.

[Rasmussen v. SmithKline Beecham Corp.](#), 413 F.3d 1318, 1325, 75 U.S.P.Q.2d 1297 (Fed. Cir. 2005) (affirming Board's ruling that applicant was not entitled to claim priority to several earlier-filed related applications to support claims made in a later application for using a drug called finasteride in a therapeutically effective amount to treat prostate cancer because applications for which the priority claim was sought did not enable one of skill in the art to use finasteride to treat prostate cancer since substantial evidence supported Board's finding that at the filing dates of the earlier application one of skill did not know that finasteride could be used to treat prostate cancer and the earlier applications did not provide any experimental data to show the successful use of finasteride to treat prostate cancer).

The how-to-use requirement focuses on the claimed invention. Hence, where a process is claimed, the requirement does not require a teaching of how to use the products that are created by the claimed process.

[Application of Wilke](#), 50 C.C.P.A. 964, 314 F.2d 558, 565–65, 136 U.S.P.Q. 435 (1963) (overruled by, [Application of Kirk](#), 54 C.C.P.A. 1119, 376 F.2d 936, 153 U.S.P.Q. 48 (1967)) (finding process claims were sufficiently enabled under § 112 and stating that “We decline to apply to these process claims … the so called ‘rule of *Bremner*’ that the specification must teach a use for the product of a claimed process. Had this been the intent of Congress, we are certain that it would have been so stated in 35 U.S.C.A. § 112.”)

The how-to-use prong of the [section 112](#) enablement inquiry is related to the utility requirement under [section 101](#). The Federal Circuit has explained:

If the written description fails to illuminate a credible utility, the PTO will make both a [section 112](#), ¶1 rejection for failure to teach how to use the invention and a [section 101](#) rejection for lack of utility. This dual rejection occurs because “[t]he how to use prong of [section 112](#) incorporates as a matter of law the requirement of 35 U.S.C.A. § 101 that the specification disclose as a matter of fact a practical utility for the invention.” Thus, an applicant’s failure to disclose how to use an invention may support a rejection under either [section 112](#), ¶1 for lack of enablement as a result of “the specification’s … failure to disclose adequately to one ordinarily skilled in the art ‘how to use’ the invention without undue experimentation,” or [section 101](#) for lack of utility “when there is a complete absence of data supporting the statements which set forth the desired results of the claimed invention.”

[In re Cortright](#), 165 F.3d 1353, 1356, 49 U.S.P.Q.2d 1464 (Fed. Cir. 1999) (citations omitted—affirming rejection of claim to method of offsetting low level of male hormones by use of particular chemical where disclosure did not report any observation of offsetting effects of lower level of hormones when method was used but only surmised it happened, evidence did not show that one of ordinary skill in the art would necessarily conclude that an offset would occur, other claim that only claimed method of treating baldness by use of same chemical was enabled because data was present showing amount of chemical used, period in which it was used, and results showing some regrowth of hair attributed to the use of the chemical).

Accord

[In re '318 Patent Infringement Litigation](#), 583 F.3d 1317, 1324–27, 92 USPQ2d 1385 (Fed. Cir. 2009) (“The '318 patent’s description of using galantamine to treat Alzheimer’s disease thus does not satisfy the enablement requirement because the '318 patent’s application did not establish utility.”—affirming judgment after a bench trial that claims directed to a method for treating Alzheimer’s disease by administering a specific drug composition, galanthamine, were invalid for lack of enablement because the patent specification failed to show to one of skill in the art a credible utility for using the drug to treat Alzheimer’s disease—“Typically, patent applications claiming new methods of treatment are supported by test results. But it is clear that testing need not be conducted by the inventor. In addition, human trials are not required for a therapeutic invention to be patentable. … In this case, however, neither in vitro test results nor animal test results involving the use of galantamine to treat Alzheimer’s-like conditions were provided. The results from the '318 patent’s proposed animal tests of galantamine for treating symptoms of Alzheimer’s disease were not available at the time of the application, and the district court properly held that they could not be used to establish enablement. Nor does Janssen contend that the prior art animal testing summarized in the '318 patent application’s specification established utility. Indeed, both in responding to the examiner’s obviousness rejection and in responding to

the obviousness defense at trial, the inventor (Dr. Davis) and Janssen's witnesses explicitly stated that the utility of the invention could not be inferred from the prior art testing described in the application. ... [A]greement ... that a person of ordinary skill in the art in early 1986 would have viewed the 'invention as set forth in the patent as scientifically grounded' falls far short of demonstrating that a person of ordinary skill in the art would have recognized that the specification conveyed the required assertion of a credible utility. In fact, the inventor's own testimony reveals that an ordinarily skilled artisan would not have viewed the patent's disclosure as describing the utility of galantamine as a treatment for Alzheimer's disease: '[W]hen I submitted this patent, I certainly wasn't sure, and a lot of other people weren't sure that cholinesterase inhibitors[, a category of agents that includes galantamine,] would ever work.' Thus, at the end of the day, the specification, even read in the light of the knowledge of those skilled in the art, does no more than state a hypothesis and propose testing to determine the accuracy of that hypothesis. That is not sufficient.")

[Process Control Corp. v. HydReclaim Corp.](#), 190 F.3d 1350, 1358, 52 U.S.P.Q.2d 1029 (Fed. Cir. 1999) ("If a patent claim fails to meet the utility requirement because it is not useful or operative, then it also fails to meet the how-to-use aspect of the enablement requirement."—proper claim construction that rendered the claim nonsensical and demonstrated that the claimed invention violated the principle of conservation of mass was invalid for being inoperative, vacating infringement verdict)

[Eli Lilly and Co. v. Actavis Elizabeth LLC](#), 2009 WL 5159650 *15-*18 (D.N.J. 2009), *denying patentee's motion for reconsideration and interlocutory appeal*, 2010 WL 715411 (D.N.J. Feb. 23, 2010) (denying accused infringer's motion for summary judgment that method of treatment claims were invalid for a lack of enablement on the basis that the specification failed to disclose test results showing a utility for the claimed method of treatment, the court rejecting the patentee's contention that one of skill in the art, at the time the application was filed, would have known of its utility sine the evidence relied on was never submitted to the Examiner, however finding that based on prior art cited within the specification an issue of fact existed as to whether this prior art showed that one of skill would have recognized a utility for the claimed method when the application was filed—"Defendants first argue that the '590 Patent's specification fails to establish utility because Plaintiff did not submit test results showing that atomoxetine could be used to treat ADHD. Plaintiff responds that the results of successful clinical test studies were available prior to the issuance date of the patent, and these results indicate that the drug had utility. Further, Plaintiff asserts that doctors approved clinical test studies prior to the patent application date, thus indicating that the claimed method had utility. This Court finds neither of Plaintiff's arguments compelling The test results, here, however cannot establish utility because they were not available at the time of the patent application's filing date Moreover, even if the results were available prior to the application date as required, they still would not be sufficient to establish utility as they were not provided to the examiner Here, Plaintiff did not provide the results of the clinical tests to the patent office. Such results, then, cannot be relied upon to establish utility. Plaintiff also asserts that 'doctors did find that utility [of the '590 Patent was] credible, even before the patent was filed [as] the FDA granted permission to begin human testing of atomoxetine for ADHD, and [MGH] physicians Drs. Biederman and Spencer agreed to conduct the trial.' ... These arguments, however, suffer from the same defects as noted above with respect to the clinical test data—Plaintiff's information regarding utility was never submitted to the PTO Plaintiff cannot satisfy the utility/enablement requirement by relying on non-disclosed materials, even if the materials show that the claimed method is useful Plaintiff claims, alternatively, that even if its clinical testing can not be relied upon to provide evidence of utility, a person of ordinary skill in the art in 1995 (the time of filing) would have recognized the utility of the invention based upon the specification of the '590 Patent Unlike the *Janssen* case, here, there is evidence of record that could support a finding that a person skilled in the art could infer atomoxetine's utility from the selected prior art described in the '590 Patent's specification. As material issues of fact are in dispute, the Court must deny Defendants' motion for summary judgment for lack of enablement."—citations and footnotes omitted)

Westlaw. © 2015 Thomson Reuters. No Claim to Orig. U.S. Govt. Works.

ELECTRONICALLY FILED
9/2/2015 12:12 PM
2014-CH-15338
CALENDAR: 11
PAGE 1 of 31
CIRCUIT COURT OF
COOK COUNTY, ILLINOIS
CHANCERY DIVISION
CLERK DOROTHY BROWN

1 IN THE UNITED STATES DISTRICT COURT
2 NORTHERN DISTRICT OF ILLINOIS
3 EASTERN DIVISION

4 UNITED STATES OF AMERICA,) No. 12 CR 87-1
5)
6 Plaintiff,)
7)
8 v.) Chicago, Illinois
9) October 9, 2013
10 RONALD WATTS,) 1:35 p.m.
11)
12 Defendant.) Sentencing

13 TRANSCRIPT OF PROCEEDINGS
14 BEFORE THE HONORABLE SHARON JOHNSON COLEMAN

15 APPEARANCES:

16 For the Government: HON. GARY S. SHAPIRO
17 United States Attorney, by
18 MS. MARGARET J. SCHNEIDER
19 MS. MEGAN C. CHURCH,
20 Assistant United States Attorneys
21 219 South Dearborn Street
22 Chicago, Illinois 60604

23 For the Defendant: LAW OFFICES OF THOMAS GLASGOW
24 1834 Walden Office Square
25 Suite 500
 Schaumburg, Illinois 60173
 BY: MR. THOMAS T. GLASGOW
 MR. WILLIAM B. BEATTIE

26 U.S. PROBATION: MR. ZAKARY FREEZE

27 TRACEY DANA McCULLOUGH, CSR, RPR
28 Official Court Reporter
29 219 South Dearborn Street
30 Room 1426
31 Chicago, Illinois 60604
32 (312) 435-5570

1 THE CLERK: 12 CR 87, USA versus Ronald Watts for
2 sentencing.

3 MS. SCHNEIDER: Good afternoon, Your Honor. Maggie
4 Schneider and Megan Church for the United States.

5 MR. GLASGOW: Good afternoon, Your Honor. Thomas
6 Glasgow, G-L-A-S-G-O-W, as well as Mr. William Beattie for Mr.
7 Watts.

8 THE COURT: All right. Good afternoon everyone.
9 Good afternoon, Mr. Watts.

10 DEFENDANT WATTS: Good afternoon, Your Honor.

11 MR. FREEZE: Judge, Zakary Freeze with the U.S.
12 Probation office.

13 THE COURT: All right. Mr. Freeze. And we're here
14 for sentencing.

15 MS. CHURCH: Yes, Your Honor.

16 THE COURT: And is everyone ready to proceed?

17 MR. GLASGOW: Yes, Your Honor.

18 MS. SCHNEIDER: Yes, Your Honor.

19 THE COURT: Mr. Watts.

20 DEFENDANT WATTS: Yes, ma'am.

21 THE COURT: The Court wants to point out that I have
22 reviewed the presentence investigation report here that has
23 been presented to the Court, the different written
24 presentations by your lawyers on your behalf and by the
25 government, and just the overall history of this case on the

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 2 of 31

1 docket. Sentencing is the most difficult and probably
2 important task that a judge has to perform. I do not take it
3 lightly.

4 And it is important that this Court not only be aware
5 of the statutory provisions when it comes to the offense that
6 you have pled guilty to. The Court also looks at the guideline
7 provisions, which I'm sure your lawyer has told you -- your
8 lawyers have told you that is advisory, but does give this
9 Court some context on which to base its judgment. The Court
10 looks at again all of the presentations in writing that have
11 been presented. I'll hear oral arguments, and I will also give
12 you the opportunity to address the Court.

13 After having and considering all of that information,
14 the Court then also looks at the sentencing factors under 3553
15 (a) of the statutes to fashion a sentence in your case that is
16 sufficient but not greater than necessary. So, in other words,
17 sir, I look at everything. All right. And so it is not --
18 there's not a cut and dried formula or cut and dried sentence.
19 Every case is different. The Court also notes that the Court
20 has in front of it, of the Court all of the letters that you
21 have presented on your behalf. And the Court notes there are
22 persons in court here to support you.

23 All right. But, first of all, we are going to look
24 at the presentence investigation report. And the presentence
25 investigation report that has been tendered to the Court after

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 3 of 31

1 your guilty plea is a large document which you were able to
2 give input to Probation. Probation got information by you,
3 information probably from some of your relatives, close friends
4 to compile this picture of what your criminal history is, what
5 your personal history is for the Court to review. And it
6 results in after there is a compilation of all that information
7 the Court is recommended a particular offense level and
8 criminal history category.

9 And in this case it is what, Mr. Freeze?

10 MR. FREEZE: Judge, the total offense level or the
11 criminal history category?

12 THE COURT: The category, the category. The offense
13 level.

14 MR. FREEZE: The total offense level that I have
15 calculated --

16 THE COURT: I just wanted to make sure I had the
17 right document.

18 MR. FREEZE: -- is 12.

19 THE COURT: Okay.

20 MR. FREEZE: And with a criminal history category of
21 1, Judge.

22 THE COURT: All right. That's what I had. There was
23 a little bit of confusion on the docket where one of the other
24 defendants was somehow superimposed.

25 MR. FREEZE: I apologize for that, Judge.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 4 of 31

1 THE COURT: That's all right. The Court caught it,
2 and I just wanted to make sure that we're on the record having
3 the right calculations. So that's what the Court had, an
4 offense level presented on the PSI of 12, which would -- and a
5 criminal history category of 1, which would be an advisory
6 guideline provision of 10 months to 16 months in Zone C. With
7 a recommendation of the guidelines of 1 to 3 years of mandatory
8 supervised release, a fine of 3,000 to \$30,000, and a special
9 assessment of \$100. That's the advisory guidelines.

10 Is there any argument from the defense, who I'm
11 certain have gone over this document with your client, as to
12 whether or not this Court should adopt the presentence
13 investigation?

14 MR. GLASGOW: As the Court knows, this was tendered
15 to us. We did get a chance to go over it with Mr. Watts. We
16 went over it in great length. There are no additions,
17 corrections, or deletions. And he concurs with the sentencing
18 guidelines which have been put forth by Probation.

19 THE COURT: All right. Thank you. As to the
20 government, do you have any adjustments that you believe need
21 to be made in the presentence investigation report?

22 MS. SCHNEIDER: We do, Your Honor. We when preparing
23 our sentencing memorandum realized that we failed to advance an
24 enhancement for -- under Section 3 (b) 1.1 (c) for the
25 defendant being a leader or organizer in the offense. We

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 5 of 31

1 believe that that enhancement should apply here. He planned
2 and organized the offense as the point of contact with the
3 confidential source. He recruited Mr. Mohammed to participate.
4 He claimed a larger share of the proceeds of the crime. And as
5 Mohammed's sergeant and organizer -- and as the organizer of
6 the activity, he exercised control. And I think those are all
7 factors that the law says should be considered in applying this
8 enhancement. And given that they are present here, we do
9 believe that two levels should be applied.

10 THE COURT: And you believe the calculation should be
11 a 14 offense level then, is that correct?

12 MS. SCHNEIDER: Yes.

13 THE COURT: Would you like to respond, Counsel.

14 MR. GLASGOW: Yes, Your Honor. The basis for the
15 enhancement that the government has given is based on
16 supposition, and there's been no evidence that's been tendered
17 before the Court to end up adding the enhancement level. The
18 supposition that he ended up being the leader is a bit of a
19 stretch, Judge, considering the fact that Mr. Mohammed and Mr.
20 Watts were alleged throughout the entire course of this case to
21 have worked in concert.

22 Additionally, as Your Honor recalls, from -- as this
23 Court had listened to during the course of the plea of Mr.
24 Mohammed, he claimed that he accepted no cash and had no
25 remuneration whatsoever as a result of any of the schemes,

1 artifices, or of the ongoing issue that Mr. Watts and himself
2 apparently participated in. That's highly unbelievable, Judge.

3 And in addition, Mr. Watts and Mr. Mohammed, there is
4 no showing of who was the leader as there was no audio from Mr.
5 Mohammed nor Mr. Watts as to what was going on during the
6 course of the conversations back and forth. The only thing
7 that the government was able to produce was the fact that they
8 were contacting and talking to each other vis-a-vis the fact
9 that the PIN register indicated that they were calling one
10 another during the course of the commission of the act that has
11 been charged, as well as the aggravating factors set forth in
12 the sentencing memorandum and the government's sentencing
13 memorandum.

14 There has been nothing to substantiate that position.
15 And as such, Judge, I would respectfully object to the Court.

16 MS. SCHNEIDER: Judge, I think that the facts are
17 there given the various documents that we attached to our
18 government's version that lay out the facts. The facts
19 admitted to by Mr. Mohammed in his plea agreement, the facts
20 admitted to by Mr. Watts when he pled guilty all establish that
21 Mr. Watts was running the show when it came to the charged
22 offense. Like I said, he was the one who organized the whole
23 thing, recruited Mr. Mohammed and brought him into it.

24 I would also note that I believe Mr. Mohammed got a
25 reduction for being a minor participant in the offense, which

1 would I think further suggest that Mr. Watts was, in fact, the
2 one who was more culpable and responsible for organizing and
3 leading this offense.

4 THE COURT: Because Mr. Mohammed got a lesser amount
5 and was agreed to in his deal, that assumes that --

6 MS. SCHNEIDER: No, I'm sorry, Judge. He was
7 determined to be a minor participant in the offense under the
8 guidelines. And I think the other side of that coin in part is
9 that Mr. Watts was more culpable. And I think the facts show
10 that he was, in fact, the one who did organize this offense and
11 pushed it forward much more so than Mr. Mohammed.

12 THE COURT: The Court is looking at the factors that
13 would determine whether or not this Court should allow a
14 two-point enhancement for him being -- Mr. Watts being a leader
15 here. There is several things to take a look at here that go
16 on either side of the ledger. The facts that were presented
17 both in Mr. Mohammed's case, both his plea and the review of
18 the offense in his PSI and the plea that was presented by Mr.
19 Watts would tend to indicate that Mr. Watts was the leader.

20 But, of course, as counsel has stated, we have one
21 side. Clearly Mr. Mohammed pled quickly and wanted to take
22 advantage of that obviously for his own benefit. The Court
23 also notes, though, that the defendant Mr. Watts was the senior
24 officer of the two. And it appeared from some of the
25 attachments of the government he was referred to as the big man

1 or the man in some of the attachments that were put forth by
2 the government. Obviously you don't have to be at the same
3 level to have the same participation. Just because you are on
4 different ranks doesn't mean that you have one that may have a
5 lower rank that may not still be running things.

6 This Court believes it's a close call on whether or
7 not in some ways it appears that the defendant was, but the
8 Court also believes we have a defendant Mr. Mohammed whose role
9 at most may have been slightly less. They were in it together
10 throughout. Doing it together. And the Court is going to deny
11 the motion for a two-level enhancement for being a leader or
12 organizer. And so the Court will adopt the presentence
13 investigation report that has been presented by Probation.

14 All right. As to motions for departure, either side.
15 First defendant.

16 MR. GLASGOW: Judge, we accept the sentencing range,
17 and we're not making a move for a downward departure in this
18 matter.

19 THE COURT: All right. Government.

20 MS. SCHNEIDER: Yes, Judge, we are seeking a sentence
21 that is above the guidelines range. Do you want me to proceed
22 with my argument?

23 THE COURT: You know what, why don't you combine it
24 with your total sentencing recommendation.

25 MS. SCHNEIDER: Sure. Proceed?

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 9 of 31

1 THE COURT: Yes.

2 MS. SCHNEIDER: Okay. We do believe that a sentence
3 above the guidelines, and our recommendation is 36 months,
4 would be sufficient but not greater than necessary in this
5 case. It would reflect the serious nature of the offense, the
6 history and characteristics of Mr. Watts, and the goals and
7 purposes of sentencing as set forth in Section 3553 (a).

8 In terms of the nature and circumstances of the
9 offense, the charged conduct and the relevant conduct were
10 serious offenses that were a betrayal of his duty as a police
11 officer. When he was approached by someone that he believed to
12 be a courier for drug dealers, he jumped right on the idea of
13 stealing what he believed to be drug proceeds from the courier
14 and then kicking back a portion to the courier. He did this
15 twice with apparently no second thoughts from what we see on
16 the recordings, and which leads you to wonder how many times he
17 might have done something similar when the government was not
18 involved.

19 So in addition to that, the Court can and should also
20 consider the other criminal conduct that the defendant has
21 engaged in in the course of his career as a police officer. As
22 set forth in the submissions to Your Honor, from at least 2007
23 into 2008 he while working in the Ida B. Wells projects with
24 his co-defendant Mohammed, projects that were plagued with
25 crime, drug dealing, gang activity, rather than serving and

1 protecting the residents of those communities, he and Mohammed
2 worked together to extort protection payments and protect the
3 drug dealers that he should have instead been pursuing.

4 I also would note that he did other things such as
5 putting a false case on the confidential source that was
6 involved in our investigation. Had him arrested on drug
7 charges. And the source, who was a homeless unemployed
8 alcoholic, felt he had no chance of successfully fighting that
9 case so he pled guilty to a crime he didn't commit. So all of
10 these factors and criminal conduct in which the defendant has
11 engaged is very serious and warrants a serious sentence.

12 In terms of his history and characteristics, as you
13 have seen from the defense's submissions, he certainly has some
14 good characteristics. He appears to be a loving father, a good
15 friend. He served in the military and successfully performed
16 some of his duties as a police officer. But it almost makes it
17 worse that despite all these good qualities, he chose to betray
18 his oath as a police officer and instead engage in years of
19 crime. These good qualities should have prevented him from
20 engaging in the crimes that bring him here, but they didn't.
21 He let his greed win out and chose to extort drug dealers and
22 steal from who he believed to be drug couriers.

23 A significant sentence is also needed here to reflect
24 the seriousness of the offense and promote respect for the law.
25 The crime was very serious and undermined the criminal justice

1 system and crimes because of his position as a police officer.
2 Crimes like these give the community reasons to doubt law
3 enforcement and believe that law enforcement can't be trusted.
4 And not just in this case, but in other cases citizens doubt
5 law enforcement and doubt the legitimacy of what are otherwise
6 legitimate criminal prosecutions when they see things like this
7 happening. So a significant sentence is warranted here to
8 address these issues, to promote respect for the law, and to
9 show how serious these offenses are.

10 And finally, I think the government believes a
11 significant sentence is needed to deter both this defendant and
12 others from criminal activity. In terms of the larger general
13 deterrence, the sentence here needs to send a message to the
14 law enforcement community that bad cops will be prosecuted and
15 punished when they use their position to commit crimes.
16 Deterrence is particularly important because of the
17 difficulties that we have in investigating and prosecuting
18 these types of cases.

19 People like the CS in our case or residents in the
20 Ida B. Wells Housing Project don't believe that they will be
21 believed over the words of a police officer, so they don't come
22 forward. Making it very difficult to detect and prosecute
23 these crimes. Also, I think specific deterrence is an issue
24 here with respect to Mr. Watts. He will probably never again
25 be in a law enforcement position, but he faces a future as a

1 convicted felon. His conduct suggests that he may attempt to
2 engage in similar criminal activity when he's living under more
3 dire circumstances, difficulties in being a convicted felon and
4 perhaps have difficulty in obtaining employment. And a
5 sentence here should keep him out of the community long enough
6 to deter him from future criminal activity.

7 THE COURT: A question on that. Do you think his
8 situation changes once he gets out?

9 MS. SCHNEIDER: Well, because --

10 THE COURT: Because he's been in longer, it's going
11 to be better?

12 MS. SCHNEIDER: No, but perhaps a longer sentence
13 will be further deterrence to him to make him think harder
14 about engaging in criminal conduct in the future.

15 THE COURT: Even though he'll be in the same dire
16 circumstances when he gets out?

17 MS. SCHNEIDER: True, but a stiffer sentence makes
18 people think twice about what they might do in the future. So
19 for all of these reasons we believe that a sentence of 36
20 months would be a sentence that is sufficient but not greater
21 than necessary to hold the defendant accountable for his
22 crimes, for his abuse of authority as a sworn Chicago police
23 officer, and for the damage that he caused to the reputation of
24 all sworn law enforcement officers and for the damage that he
25 caused to the communities that he was supposed to serve.

1 THE COURT: And what are you -- do you have any
2 recommendations -- is there a restitution or fine amount that
3 you are recommending or no?

4 MS. SCHNEIDER: There is. We are asking that Your
5 Honor impose as a condition of supervised release that he be
6 required to repay \$15,280 that he received during the offense
7 of conviction on the relevant conduct.

8 THE COURT: All right. Thank you very much.
9 Counsel.

10 MR. GLASGOW: Thank you very much. I appreciate it.
11 May it please the Court, Counsel. The government's version of
12 events are what Mr. Watts has pled guilty to. And he has come
13 forward and he has admitted to this Court his role and
14 responsibility in those actions. He's taken personal
15 responsibility to come before this Court and ended up
16 indicating that he did this and is admitting to the Court and
17 to the public that he committed this crime.

18 That being said, this Court knows that he acted in
19 concert with Mr. Mohammed. And he acted in concert with Mr.
20 Mohammed during the course of the alleged acts that the
21 government has brought forth. The fact that Mr. Watts was
22 charged with one count does not discount the statement that Mr.
23 Mohammed made during the course of his discussions with law
24 enforcement, which was included in the attachments that this
25 Court read that Mr. Mohammed was the one who asserted that he

1 was the one who always accepted extortion payments. Mr. Watts
2 was never there.

3 Additionally, Judge, he claims on page 3 that he
4 never got any payments from the extortions of any dealers or
5 any payments other than a \$200 loan from the charged conduct,
6 which again, is an absurd assertion for this Court -- that
7 the government would put forth to the Court.

8 As for the false case of Mr. Hopkins, this Court
9 knows that the defendant -- or excuse me, Mr. Hopkins has a
10 lengthy criminal record. I believe that we litigated parts of
11 his criminal background, and the Court is well aware of the
12 felonies that Mr. Hopkins has, as well as the crimes of moral
13 turpitude that he has in his background. He admitted to the
14 crimes that he was arrested for. The government's supposition
15 that it was Mr. Watts who put a case on him is nothing more
16 than that. There was nothing that I could find for this Court
17 that would indicate through a transcript or through anything
18 else during the course of his plea that he made any assertion
19 or allegation towards Mr. Watts or any other law enforcement
20 official that they had done anything wrong.

21 This Court has to take into consideration the fact
22 that not only is Mr. Hopkins a convicted felon and served
23 penitentiary time, but he does have severe alcohol and drug
24 problems. Additionally, the Court is well aware that has a
25 propensity to lie due to his prior arrests and convictions that

1 have been brought forward and made part of the litigation in
2 this case. Mr. Hopkins is a questionable individual at best,
3 and he has every reason to lie about his action towards Mr.
4 Watts as he was getting payment from law enforcement for his
5 participation in this matter.

6 Mr. Watts has through the presentation and the
7 attachments that we have presented to this Court, has engaged
8 in a long life of public service. And but for the charges that
9 have been levied against him and the actions which the
10 government ends up alleging, he has had a very storied
11 background as a Chicago police officer. Obtaining numerous
12 awards, gaining the benefit of the community, and helping the
13 community around him. I know this Court has read the letters
14 that have been attached to our sentencing memorandum showing
15 what kind of father and what kind of person he is. It shows
16 the character that Mr. Watts does have, and it shows a
17 rehabilitatable person that is worth saving and worth going the
18 extra mile for.

19 Mr. Watts has numerous amounts of mitigation in this
20 matter, which we have presented. And I always find it
21 interesting that the government attempts to characterize that
22 in some way as aggravation as if he had a lengthy criminal
23 background that would be a much better issue for this Court to
24 take into aggravation. The fact that he has a good background
25 shows that he is somebody that is not deserving of a long

1 criminal sentence.

2 He is agreeing to restitution, Judge. The
3 restitution in this matter should be set for the counts
4 charged, as Mr. Mohammed was only sentenced to pay restitution
5 I believe of \$9900, which does not include any of the other
6 agreed -- excuse me, aggravating circumstances that I believe
7 the government is setting forth in this matter, which the
8 government has alleged and has acknowledged that Mr. Mohammed
9 and Mr. Watts worked in concert with each other. Yet the
10 additional amount that they are attempting to have as
11 restitution, the \$10,000 and change, is something that Mr.
12 Mohammed was not subjected to in his restitution.

13 Mr. Mohammed was made jointly and severally liable I
14 believe for \$5200, which Mr. Watts accepts responsibility for
15 and will pay restitution for and agrees to the \$5200 of
16 restitution. But as for the further amount, Judge, I don't
17 think that that's appropriate for this Court to order based
18 upon the totality of the circumstances and based upon the
19 totality of both pleas.

20 He has no criminal background, Your Honor. He has a
21 level one. He's obeyed every command of this Court while on
22 bond. He has appeared each and every time that Your Honor has
23 asked him to. He has created no problems and no issue for
24 Pretrial. During the course of his plea and discussions with
25 him, Mr. Watts realized that by pleading guilty and accepting

1 responsibility to this he has lost both his career and his
2 pension. He realizes that this amount of stigma that has been
3 brought upon him is something that will never be washed away.
4 And this is something that he will carry with him the remainder
5 of his life.

6 By pleading guilty he has chosen to give up his
7 chosen profession in this world. And he is attempting to make
8 amends for the wrongs that he did by pleading guilty to this
9 Court. A lengthy sentence, Judge, would not serve the interest
10 of justice because of the fact that he is now unemployable in
11 the field which he has been part of for years and years and
12 years. Sending him to the penitentiary, sending him to prison
13 will end up giving and sending the message that deterrence has
14 been met by this Court.

15 It does not further the criminal justice system nor
16 the ends of justice for a lengthy prison term for a man, No. 1,
17 of his age. And No. 2, based on the mitigating factors that
18 have been brought to the Court's attention. Your Honor, the
19 sheer effect of this plea that he voluntarily chose to enter
20 into and accept responsibility should be reflected in the
21 sentence in this matter. We would respectfully ask this Court
22 for a minimum sentence in this matter and restitution of \$5200,
23 plus the additional one year mandatory supervised release.

24 THE COURT: Thank you, Counsel. Mr. Watts -- and
25 counsel can clear out. Mr. Watts, if you wish to address this

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 18 of 31

1 Court, this is your -- you can stand in front of the mike --
2 this is your opportunity to do so. Everyone who stands before
3 this Court prior to sentencing has that opportunity if they
4 wish to take it. I will listen to your comments that you wish
5 to make to the Court or to the Court as a whole or to me in
6 particular about your sentencing. And this is your time, sir.
7 Proceed.

8 DEFENDANT WATTS: I wish not to make a statement.

9 Thank you.

10 THE COURT: All right. Thank you very much.

11 MS. SCHNEIDER: Your Honor, I can clarify the
12 financial issue if you would like.

13 THE COURT: Oh, if you wish to address that, that
14 would be good.

15 MS. SCHNEIDER: Sure. Mr. Mohammed agreed to repay
16 \$9,900, which was the \$5200 from the offense of conviction.
17 Plus as you may recall, he actually stipulated to the Ida B.
18 Wells conduct, and there was certain controlled payments we had
19 that we could add up that he paid. So that was where that
20 number came from. Mr. Mohammed was not involved, or at the
21 very least very minimally involved in the first theft that is
22 the relevant conduct here, the PSI found was relevant conduct.
23 And that one involved 11,000 -- that theft was \$11,650.

24 So our figure of 15 -- it should be -- I'm sorry. My
25 math is wrong. 16,000.

1 THE COURT: You said he was minimally or not
2 involved?

3 MS. SCHNEIDER: We have no evidence that he was
4 involved. There was some supposition that Mr. Mohammed was
5 involved, but he didn't admit to that, any involvement in that
6 offense.

7 THE COURT: In the offense that involved how much?

8 MS. SCHNEIDER: \$11,650.

9 THE COURT: All right. And so you agree that \$5200
10 is the amount that he should be --

11 MS. SCHNEIDER: Our position is given that the
12 earlier theft was found to be relevant conduct in the PSI, that
13 that should also be imposed -- repayment on that should be
14 imposed.

15 THE COURT: All right. You're going to have to give
16 this to me again.

17 MS. SCHNEIDER: All right. There's -- so there's the
18 offense of conviction, which everyone agrees involved \$5200.

19 THE COURT: Correct.

20 MS. SCHNEIDER: That Mr. Mohammed and Mr. Watts did
21 together. Then there was a March of 2010 transaction that we
22 don't have evidence of Mr. Mohammed's involvement, but
23 significant evidence of Mr. Watts' involvement.

24 THE COURT: Okay.

25 MS. SCHNEIDER: And that one involved \$11,650. So it

1 would appear that my math was bad. It should be 11,650 plus
2 5200. At least that's our position.

3 THE COURT: Counsel.

4 MR. GLASGOW: Your Honor, it seems that the
5 government is relying very heavily on the statements of Mr.
6 Mohammed, who has pled guilty in this matter, and is
7 selectively picking and choosing what they wish to end up
8 delegating to Mr. Watts or not delegating to Mr. Watts. They
9 have made the allegation that they have been -- that they have
10 acted in concert and that somehow Mr. Watts was the primary
11 responsibility of the criminal activity in this matter, but yet
12 have taken on Mr. Mohammed's allegations that other activities
13 were to be attributed to him. But yet the entire activity from
14 beginning to end was supposedly between the two of them and at
15 Mr. Watts' direction.

16 I mean, it seems that they are asking this Court to
17 have it both ways. And most respectfully, Mr. Mohammed did
18 plead guilty. He got to pick and choose what he was going to
19 tell the government. And the fact that there is not evidence
20 that Mr. Mohammed was involved based upon what Mr. Mohammed
21 decided to tell the government does not really bolster the
22 argument that he wasn't. That being said, he was not punished
23 for that in any way. And Mr. Watts is taking the position
24 because this is an uncharged crime and there's not significant
25 evidence that, you know, Mr. Watts and/or Mr. Mohammed were

1 involved in this, that he shouldn't have to pay that
2 restitution, Judge.

3 THE COURT: All right. I've heard the arguments on
4 that. Thank you.

5 As I stated earlier, Mr. Watts, this Court relies on
6 the arguments presented by the government's counsel and your
7 counsel on the PSI, on the history of this case, looking at the
8 documents that have been presented and all of the attachments.
9 In this particular case there is some question that sometimes
10 as to whether or not some of the evidence relied on in your
11 case or at least the arguments relied on as far as your
12 sentencing is concerned are based on information from a
13 co-defendant who may have had reasons of his own to make
14 certain statements. And the Court keeps that in mind also.

15 But, first of all, the Court looks at your
16 background, your history here. And as counsel said, you have
17 no criminal background. You're a level 1 as far as criminal
18 history is concerned. You have a history of service to our
19 country. You have served our community as a police officer,
20 rising to the ranks of sergeant. You have a strong educational
21 background. Although you came from a large family that seems
22 to be fairly close, it also appears that even though you have a
23 family that is somewhat fractured, you still maintain close
24 ties with your children, various children. Several who have
25 done well for themselves and said they did well based on your

1 support.

2 So if the Court were to look at the picture of you
3 through that lens only, this Court would see a picture of a
4 strong male figure not only in his family, but in his ethnic
5 community, professional community, community at large.
6 Somebody to be respected and to be an example. And then the
7 Court has another lens that the Court has to look through. And
8 your counsel is arguing that when I look through that lens, I
9 look through it understanding that you're coming from a point
10 where all things were good and you get credit for that.

11 The problem is that the mistake you made here, even
12 though there is one count that you pled to and there's some
13 questions of whether Mr. Mohammed is putting more on you to get
14 himself out of some of his trouble, this was ongoing. All
15 right. And I don't know who all did what, when, but you were
16 part of more than just one incident. And you were a sergeant,
17 and you were operating in a community that should hold you up
18 as the example I just stated. And you took advantage of that
19 community.

20 The government talks about it being a community, the
21 Ida B. Wells Homes, formally Ida B. Wells Homes, talks about it
22 being a place rampant with crime and drugs and problems. The
23 place was rampant with poverty, underprivileged, addictions,
24 illnesses. The crime stuff comes after. And it's because of
25 that. And you were there to protect those people, and you

1 didn't. And Mr. Hopkins, you know, based on a lot of what I
2 read may be one of the baddest things walking around, but
3 that's why you chose him. Who would believe him? And who
4 would be vulnerable or be amenable to participating.

5 And what really upsets this Court is that, you know,
6 it's bad enough that drugs are brought from the outside into
7 the community that's already down and out, but for you to be
8 part of the face of that or even be condoning it or not
9 stopping it is unconscionable to this Court. So your own
10 children have advantages. You had all those little kids in
11 that area, this is what they see. So they see drugs. They see
12 crime. They see cops shaking down people. They see drug
13 dealers being able -- allowed to continue to do what they're
14 supposed to -- want to do.

15 And then what are they taught? They're taught not to
16 respect men such as yourself or anybody with a badge on, which
17 is a big problem we have here. And it not only goes to the
18 badge, it goes to the whole judicial system, the whole criminal
19 justice system. That we have to constantly work to try to make
20 people understand that we try to be fair. Sometimes we aren't,
21 but we try to be fair. But when they see examples live in
22 front of them, what are they supposed to think?

23 Your actions, sir, were a betrayal to your oath as a
24 police officer. You betrayed your community, both your law
25 enforcement community, the African-American community, that

1 south side community. Your actions were a betrayal. It is a
2 serious offense. Drugs are always serious to this Court. The
3 prevalence of drugs and the business of illegal drugs in --
4 anywhere, but particularly in neighborhoods that have no
5 wherewithal to fight for themselves. It is important that this
6 Court set a sentence that promotes respect for the law, and I'm
7 preaching to the choir, someone who was taught and had a job of
8 respecting the law, but he broke the law.

9 Deterrence as to your criminal conduct. You know,
10 the Court does not know exactly why you went down this road.
11 Based on my review of your background and some of your outside
12 interests, I have an idea as to why you wanted to continue to
13 have money as easily as possible. Maybe it was to support a
14 gambling habit. Maybe it was -- I don't know. I mean, it says
15 here you like to gamble. And maybe again we got facts crossed
16 here. I don't know. But there had to be some reason.

17 But I don't know if whatever we choose here or what
18 this Court determines here would be an adequate deterrence, but
19 this Court needs to make sure that this doesn't continue. Not
20 only for you, but it doesn't continue for anyone else. Let's
21 send a message that the Court doesn't tolerate and the
22 community won't tolerate this activity.

23 The Court notes that Mr. Mohammed got an 18-month
24 sentence. And one of the factors the Court looks at is making
25 sure that there are no unwarranted sentencing disparities among

1 the defendants in this case. I guess you can tell, sir, that
2 as much as I am impressed by your background, by the
3 achievements of your children, the support of the family that
4 wrote letters on your behalf, suffice it to say, that this
5 Court is all the more disappointed based on your position in
6 law enforcement, based on your position as a leader in -- what
7 should have been a leader in the community, and that weighs
8 heavily as a factor that this Court is considering.

9 This Court is going to, therefore, sentence you, Mr.
10 Watts, to an amount above the advisory guidelines. And this
11 Court is going to sentence you to 22 months in the Bureau of
12 Prisons and 1 year mandatory supervised release after the
13 completion of that sentence. The Court is not going to
14 recommend a fine. However, the Court will recommend that
15 restitution be in the amount of \$5,200. A special assessment
16 is going to be \$100.

17 After you are released from your 22-month sentence,
18 sir, you will report within a 72-hour period to Probation, and
19 you will comply with all the conditions that are set forth, the
20 standard conditions of probation. In addition to the standard
21 conditions, you will be providing them if they so request drug
22 samples and enter into any program if they believe one is
23 needed for illegal drugs. You will not be possessing any
24 weapon or destructive device, committing any crimes, state,
25 federal, or local.

1 You will report for any counseling if they believe
2 that counseling is needed. You will also undergo any
3 counseling, financial counseling if they believe that is
4 needed. As to the restitution, what are the requirements
5 again, Mr. Freeze, as to if he's not working?

6 MR. FREEZE: I think it's a repayment of buy money is
7 how that needs to be ordered.

8 THE COURT: All right.

9 MR. FREEZE: And counsel can correct me.

10 MS. SCHNEIDER: I think that's correct, Your Honor.

11 THE COURT: Repayment of buy money of \$5200.

12 MR. FREEZE: The probation office wants to ask the
13 Court and counsel if any of that portion is joint and
14 several -- severally liable with the co-defendant.

15 MR. GLASGOW: Yes, Judge. I believe Mr. Mohammed
16 was --

17 THE COURT: It should be --

18 MR. GLASGOW: -- sentenced jointly and severally.

19 THE COURT: -- jointly and severally.

20 MS. SCHNEIDER: I agree, Judge.

21 MR. FREEZE: In its entirety then, is that correct?

22 THE COURT: For that 52 -- for his definitely, yes.

23 MR. FREEZE: Thank you, Judge.

24 THE COURT: Anything else on behalf of the
25 government?

1 MS. SCHNEIDER: I don't believe so, Your Honor.

2 THE COURT: On behalf of the defense?

3 MR. GLASGOW: Your Honor, we had a couple, if we
4 could, briefly. And I don't know to the extent that the Court
5 has, but I do know Mr. Watts can at least make a suggestion in
6 terms of recommendations for facilities that he would be
7 serving his time at as well as an amount of time in which to
8 get his affairs in order and turn himself in.

9 With that in mind, Mr. Watts had spoken to me before
10 coming in today. He has family both in the western part of the
11 United States and also in Wisconsin. And with that in mind,
12 he -- and I don't know if it's a suggestion, request, however
13 you'd want to phrase it, there is a federal correctional
14 facility in the State of Colorado. I don't think it's to hang
15 out with our former governor, but it is the one that Governor
16 Blagojevich was sentenced to, which is Mr. Watts looked at map
17 in terms of closeness to his family. That would be one that he
18 would ask the Court to consider if the Court has the ability to
19 do that.

20 THE COURT: Yes, the Court only -- the Court can only
21 make a recommendation.

22 MR. GLASGOW: Yes, I understand, Judge. With that in
23 mind --

24 THE COURT: So if you have a specific one, just let
25 us know, and the Court can --

1 MR. GLASGOW: It's that one. There is one in the
2 State of Arizona. I did not -- I don't know specifically the
3 name of that one. And one I think is in Sandstone, Minnesota,
4 which is the southern part I believe of the State of Minnesota.
5 So he would ask that -- request at least those be considered.
6 He would also ask if Your Honor could give him between 30 and
7 60 days to get his affairs in order, sell property, be prepared
8 to turn himself in. His family can take care of the rest of
9 the matters after that.

10 THE COURT: Government position on his request for 30
11 to 60 days.

12 MS. SCHNEIDER: We don't have any objection to that,
13 Your Honor.

14 THE COURT: All right. Sir, I'll give you 60 days.
15 All right. Till after -- make it January -- after the first of
16 the year.

17 THE CLERK: January 10th.

18 THE COURT: You will turn yourself in to the
19 marshal's office.

20 THE CLERK: They will designate him by then.

21 THE COURT: You'll be designated by then as to where
22 you're supposed to be.

23 MR. FREEZE: Judge, I do have one question. Maybe I
24 just didn't hear you. Did you impose the condition of
25 supervised release that would require the defendant to provide

1 the Probation Office with financial records --

2 THE COURT: With a DNA sample?

3 MR. FREEZE: Access to financial information,
4 financial records.

5 THE COURT: You know what, I didn't say that
6 specifically, but that will -- that is part of the order, that
7 Probation have access to his financial information.

8 MR. FREEZE: Thank you, Judge. And I just would
9 remind the defendant -- the Probation Office would remind the
10 defendant that the bond conditions still hold and any pretrial
11 requirements need to be followed.

12 THE COURT: And the Court will remind him of that
13 also. Before we do that, is there anything else from the
14 government?

15 MS. SCHNEIDER: Yes, Your Honor. I neglected to move
16 to dismiss the forfeiture allegation in the indictment.

17 THE COURT: I'm certain that there's no objection.

18 MR. GLASGOW: No objection.

19 THE COURT: It will be granted. All right. Anything
20 else from the government?

21 MS. SCHNEIDER: No, Your Honor.

22 THE COURT: Defense, anything else?

23 MR. GLASGOW: No. Thank you.

24 THE COURT: Was there a waiver of appeal rights here?
25 Sir, you have the opportunity to appeal this Court's decision.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 30 of 31

1 You have to do so within -- let the proper authorities know you
2 want to do so within 14 days. You speak to your counsel, and
3 they will assist you with that.

4 Sir, again this is not a happy day for the Court.
5 Clearly not for you and your family. The Court is certain that
6 you understand that not only do the conditions remain while you
7 are out, but you will clearly not help yourself if for some
8 reason any of these conditions are violated regardless of
9 whatever stress and strain there may be as it leads up to the
10 date. All right. And the Court wishes that after your
11 completion of this sentence that things will go well for you.

12 All right. Thank you very much.

13 MS. SCHNEIDER: Thank you, Your Honor.

14 MR. GLASGOW: Thank you, Your Honor.

15 CERTIFICATE

16 I HEREBY CERTIFY that the foregoing is a true,
17 correct and complete transcript of the proceedings had at the
18 hearing of the aforementioned cause on the day and date hereof.
19

20 /s/TRACEY D. McCULLOUGH

September 4, 2014

21 Official Court Reporter Date
United States District Court
22 Northern District of Illinois
Eastern Division
23

24

25

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

DEBRA GREEN, ANTHONY FISHER, and TANEAL JONES,)	
)	Case Number 11 CV 07067
)	
Plaintiff,)	
)	JUDGE KOCORAS
vs.)	
)	Magistrate Judge Gilbert
CHICAGO POLICE OFFICER SYLSHINA LONDON, Star No. 11636; CHICAGO POLICE OFFICER BENNY WILLIAMS, Star No. 12544, and VARIOUS UNKNOWN OFFICERS OF THE CHICAGO POLICE DEPARTMENT, Individually and as Employees/Agents of the CITY OF CHICAGO, a municipal corporation,)	JURY DEMAND
)	
Defendants.)	

**DEFENDANT LONDON'S ANSWER TO PLAINTIFF'S FIRST AMENDED
COMPLAINT**

Defendant London for her answer to Plaintiffs First Amended Complaint, states as follows:

NATURE OF THE CASE

1. This is an action for monetary damages brought pursuant to 42 U.S.C. § 1983 and the laws of the State of Illinois.

ANSWER: Admit

2. Plaintiffs bring this action to redress for Defendants' misconduct, which includes, among other things, unlawful seizure and detainment of Plaintiffs; causing Plaintiffs to miss the burial of Michelle Green (Plaintiff, Debra Green's sister); falsifying police reports; manufacturing false criminal charges; and perjury at trial.

ANSWER: Defendant admits Plaintiff brings this action Defendant denies any misconduct and denies the allegations of remaining allegations.

JURISDICTION AND VENUE

3. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1331 and §

1343 because Plaintiffs assert herein claims that arise under the Constitution and laws of the United States, and other claims that are so related to claims in the action within the Court's original jurisdiction that they form part of the same case or controversy under Article III of the United States Constitution.

ANSWER: Admit

4. Venue is proper pursuant to 28 U.S.C. §1331(b) because the facts that gave rise to the claims occurred within the Northern District of Illinois.

ANSWER: Admit

THE PARTIES

5. At all relevant times, Plaintiffs Green, Fisher, and Jones resided in Chicago, Illinois.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

6. At all relevant times, Defendant London (Star No. 11636) resided in Illinois, served as a duly appointed City of Chicago and Chicago Police Department employee, and acted in her official capacity and under the color of law as a sworn law enforcement officer.

ANSWER: Admit

7. At all relevant times, Defendant Williams (Star No. 12544) resided in Illinois, served as a duly appointed City of Chicago and Chicago Police Department employee, and acted in his official capacity and under the color of law as a sworn law enforcement officer.

ANSWER: This allegation is not directed towards this Defendant

8. Defendant City of Chicago is a municipal corporation, incorporated under the laws of the State of Illinois that employed each of the defendant police officers at all times relevant to this Complaint.

ANSWER: This allegation is not directed towards this Defendant

FACTUAL BACKGROUND

A. Michelle Green

9. On March 9, 2010, Plaintiff Green's sister, Michelle Green ("Michelle"), passed away after a serious illness.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

10. Plaintiff Green enjoyed a particularly close relationship with Michelle.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

11. They were best friends who spent time with each other nearly every day and spoke in person or via telephone multiple times each day.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

12. In fact, during the years that preceded Michelle's death, Plaintiff Green lived with, assisted, and care for Michelle as she fought for her life.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

13. Michelle's death devastated Plaintiff Green.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

14. Even so, Plaintiff Green was determined to take care of her sister and best friend until the very end.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

B. The Funeral Procession and Unlawful Detention

15. Michelle's funeral and burial took place on Friday, March 19, 2010.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 3 of 22

the truth of the allegation

16. The funeral service was held at A.R. Leak and Sons Funeral Home, located at 78th and Cottage Grove in Chicago, Illinois.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

17. Immediately after the funeral service, the family and fellow mourners gathered so that they could proceed to the Mount Hope Cemetery (located at 115th and Fairfield in Chicago, Illinois) and say their final goodbyes.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

18. Each vehicle in the funeral procession, including Plaintiffs', bore bright stickers that read "FUNERAL."

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

19. Plaintiffs Green and Fisher rode together in a maroon Grand Prix automobile. Plaintiff Fisher drove the maroon Grand Prix. Plaintiff Green sat in the front passenger seat.

ANSWER: Admit

20. Plaintiff Jones drove a maroon Range Rover automobile.

ANSWER: Admit

21. After the funeral procession departed the funeral home (located at 79th and Cottage Grove), it proceeded westbound on 79th Street.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

22. As the funeral procession turned left to travel south on Vincennes, Defendant London, in her Chicago Police Department uniform and operating her personal vehicle, angled her vehicle so that she could cut through the funeral procession.

ANSWER: Deny

23. Shocked and dismayed that someone, especially a Chicago Police Officer, could be so disrespectful during her sister's funeral procession, Plaintiff Green pointed to the bright "FUNERAL" sticker that was displayed in the Grand Prix's windshield; raised her voice at Defendant London; and continued to turn with the funeral procession onto Vincennes Avenue.

ANSWER: Deny

24. Defendant London followed Plaintiff Green's and Plaintiff Fisher's Grand Prix.

ANSWER: Admit

25. Defendant London used her personal cellular telephone to call 911 and reported a "10-1" and stated that she was an officer in distress.

ANSWER: Admit using her personal cellular telephone to call 911, deny the remaining allegations

26. The Chicago Police Department dispatcher notified Chicago Police Officers of the "10-1" call and sent officers to intercept the funeral procession.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

27. At or about 100th and Vincennes, a legion of Chicago Police officers, including Defendant London, Defendant Williams, and various unknown officers pulled over the Grand Prix that contained Plaintiffs Green and Fisher, as well as the Range Rover that Plaintiff Jones drove.

ANSWER: Defendant denies all the allegations relate to her, the Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

28. The Chicago Police Officers, having arrived with their lights blazing and sirens blaring, jumped out of their vehicles, pulled out their guns, and pointed them at Plaintiffs.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

29. The Chicago Police Officers yelled at Plaintiffs to "put your f***ing hands in the air" and to "get the f*** out" of their cars.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

30. Upon exiting the vehicles, Plaintiffs were placed into handcuffs and forced onto their knees.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

31. The Chicago Police Officers searched the Plaintiffs, their possessions, and the vehicles.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

32. Defendant London repeatedly exclaimed that Plaintiff Green had battered Defendant London.

ANSWER: Admit

33. The Chicago Police Officers accepted Defendant London's allegations as true and did not investigate.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

34. The Chicago Police Officers detained the Plaintiffs for at least 45 minutes.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

35. During the detention, Plaintiff Green suffered bodily harm to her arms and wrists.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

36. The Chicago Police Officers also took Plaintiff Fisher's identification and refused to return the identification when Plaintiff Fisher asked for it.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

37. As a result of the detention, Plaintiffs were not able to return to the funeral procession or attend Michelle's burial.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

38. Defendant London, Defendant Williams, and various unknown officers willfully caused Plaintiff Green to miss the burial and laying to rest of her sister and best friend.

ANSWER: Defendant London denies the allegation as to her, this Defendant lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations

C. False Charges and the Arrest of Plaintiff Fisher

39. After Defendant London, Defendant Williams and various unknown officers returned to the police station (located at 7808 S. Halsted in Chicago, Illinois), they began to falsify police reports by stating that Defendant London was assaulted and prepare criminal charges.

ANSWER: Defendant London admits going to the police station, but denies that she had any involvement in drafting police reports, admits to preparing criminal charges related to Plaintiffs

40. The police reports claim that Plaintiff Green assaulted Defendant London by hitting her with a bottle at or about 79th and Vincennes.

ANSWER: Defendant London admits that one or more of the police reports related to this incident state that Defendant London was struck in the face with a glass bottle thrown by Plaintiff Green, in the vicinity of 7900 South Vincennes Avenue

41. Plaintiff Green did not strike, hit, or physically assault Defendant London.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 7 of 22

ANSWER: Deny

42. Plaintiff Green did not hit Defendant London with a bottle.

ANSWER: Deny

43. During the evening of March 19, 2010, Plaintiff Fisher went to the Chicago Police Station (located at 7808 S. Halsted in Chicago, Illinois) to retrieve the identification items that the Chicago Police Officers had seized earlier that day.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

44. When Plaintiff Fisher entered the Chicago Police Station, Defendant London and various unknown officers confronted him.

ANSWER: Defendant London admits that she met Plaintiff Fisher at the Chicago Police Station, but denies the allegations as set forth in this paragraph

45. Defendant London and various unknown officers then placed handcuffs on Plaintiff Fisher and threw him into a cell.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

46. The Chicago Police Officers did not release Plaintiff Fisher until the following day.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

47. The Chicago Police Officers willfully initiated criminal proceedings against Plaintiffs Green, Fisher, and Jones.

ANSWER: Defendant denies the allegations as they relate to her, this Defendant lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations

D. Plaintiff Green Calls the Independent Police Review Authority

48. Distraught over missing her sister's burial and disillusioned by the egregious acts of the Chicago Police Officers, Plaintiff Green called the Independent Police Review Authority ("IPRA") to report what happened.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

49. On March 23, 2011, Investigator Vincent Jones of the IPRA called Plaintiff Green and stated that he would obtain the POD camera recordings.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

50. On information and belief, IPRA or Chicago Police Officers obtained the POD recordings from the cameras located at or near 79th and Vincennes.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

51. The Chicago Police Officers never gave the POD camera recordings to Plaintiffs prior to her criminal trial.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

E. Defendants London and Williams Lie On the Stand at Trial and Plaintiff Green is Convicted.

52. On September 21, 2010, Plaintiffs were tried before the Honorable James Ryan in Branch 46, which is located at George N. Leighton Criminal Court Building at 2600 S. California Avenue.

ANSWER: Defendant admits that on September 21, 2010, Plaintiffs were tried before the Honorable James Ryan in Branch 46, but denies the remaining allegations

53. Each Plaintiff pled not guilty to the charges.

ANSWER: Admit

54. At trial, the state called two witnesses to testify: Defendant London and Defendant Williams.

ANSWER: Admit

55. On the stand and under oath, Defendant London willfully testified, among other things, that at or near the intersection of 79th and Vincennes, while her vehicle was sitting parallel to the vehicle Plaintiff Green was in, Plaintiff Green threw a bottle through Defendant London's open window and hit Defendant London in the face.

ANSWER: Defendant admits that she testified that Plaintiff Green threw a bottle through Defendant London's open window and hit Defendant London in the face but deny the remaining allegations as stated

56. The Honorable James Ryan found Plaintiffs Fisher and Jones not guilty.

ANSWER: Admit

57. Based on the testimony of Defendants London and Williams, the Honorable James Ryan found Plaintiff Green guilty of battery and sentenced her.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

F. The Pod Camera Recordings Surface, Plaintiff Green's Convictions Is Overturned, and Defendant London is Charged With Perjury.

58. After Plaintiff Green was convicted, the Chicago Police Department finally released the POD camera recordings that had captured footage at or near 79th and Vincennes on the day of Michelle Green's funeral and burial.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

59. The recordings show that Plaintiff Green did not throw a bottle or hit Defendant London in the face.

ANSWER: Deny

60. The recordings show that Defendant London's window was closed while her vehicle was parallel with the vehicle that carried Plaintiff Green.

ANSWER: Admit

61. The recordings demonstrate that Defendant London lied on the witness stand.

ANSWER: Deny

62. The recordings demonstrate that Defendant London's claims against Plaintiffs were false.

ANSWER: Deny

63. Defendant London was charged with one count of perjury under indictment number 12 CR 120186 for knowingly testifying falsely on September 21 2010, in the case of People v. Debra Green, No. 10 MCI 213383, that Ms. Green threw a bottle at Defendant London on March 19, 2010, striking her in the face.

ANSWER: Defendant London admit that Defendant London has been charged with perjury but lacks knowledge or information sufficient to form a belief about the truth of the remaining allegations.

64. Plaintiff Green's battery conviction was vacated on August 17, 2011.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

65. On January 18, 2013, Defendant London was found guilty following a bench trial.

ANSWER: Admit, but answering further state that that is the subject of an appeal.

CAUSES OF ACTION

COUNT I

42 U.S.C. § 1983 - UNLAWFUL DETENTION/FALSE ARREST

66. Plaintiffs re-allege paragraphs 1 - 65 as though fully stated here.

ANSWER: Defendant re-allege her Answers to paragraphs 1 - 65 as though fully stated here.

67. Defendant London (Star No. 11636) and Defendant Williams (Star No. 12544) violated the United States Constitution and infringed on Plaintiffs' rights by seizing, detaining, and/or arresting Plaintiffs without justification and/or probable cause.

ANSWER: Deny

68. At all relevant times, Defendant London (Star No. 11636) and Defendant Williams (Star No. 12544) served as duly appointed City of Chicago and Chicago Police Department employees, and acted under the color of law and in their official capacities as sworn law enforcement officers.

ANSWER: Defendant London admits the allegation as it pertains to her.

COUNT II
42 U.S.C. § 1983 - FAILURE TO INTERVENE

69. Plaintiffs re-allege paragraphs 1 - 65 as though fully stated here.

ANSWER: Defendant re-allege her Answers to paragraphs 1 - 65 as though fully stated here.

70. Defendant Williams, various unknown officers who detained Plaintiffs, and various unknown officers working for the Chicago Police Department (including those unknown officers working for the Independent Police Review Authority) knew that Defendant London's allegations were false or acted with reckless disregard as to whether Defendant London's claims were false.

ANSWER: These allegations are not directed to this Defendant

71. Defendant Williams failed to intervene in the detention of Plaintiffs.

ANSWER: These allegations are not directed to this Defendant

72. Defendant Williams failed to intervene prior to or during the criminal proceedings of Plaintiffs.

ANSWER: These allegations are not directed to this Defendant

73. At all relevant times, Defendant Williams (Star No. 12544) served as a duly appointed City of Chicago and Chicago Police Department employee, and acted under the color of law and in his official capacity as sworn law enforcement officer.

ANSWER: These allegations are not directed to this Defendant

COUNT III
42 U.S.C. § 1983 - BRADY SUPPRESSION VIOLATION

74. Plaintiffs re-allege paragraphs 1 - 65 as though fully stated here.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 12 of 22

ANSWER: Defendant re-alleges her Answers to paragraphs 1 - 65 as though fully stated here.

75. At all relevant times, Defendants possessed the POD camera recordings that exonerated Plaintiffs.

ANSWER: Defendant denies the allegations as they relate to her.

76. Defendants withheld and/or hid the existence of the POD camera recordings.

ANSWER: Defendant denies the allegations as they relate to her

77. Defendants failed to tender the POD camera recordings to Plaintiffs prior to trial.

ANSWER: Defendant denies the allegations as they relate to her

78. Defendants were required by the United States Constitution and Supreme Court precedent to tender the POD camera recordings to Plaintiffs prior to trial.

ANSWER: Defendant denies the allegations as they relate to her

79. Plaintiff Green would have never been convicted at trial, nor would the State ever have prosecuted Green, had the Defendants not withheld and/or hid the existence of the POD camera recordings.

ANSWER: Defendant denies the allegations as they relate to her

80. At all relevant times, Defendant London (Star No. 1 1636) and Defendant Williams (Star No. 12544) served as duly appointed City of Chicago and Chicago Police Department employees, and acted under the color of law and in their official capacities as sworn law enforcement officers.

ANSWER: Defendant London admits the allegation as it pertains to her.

COUNT IV

42 U.S.C. § 1983 - MONELL CLAIM AGAINST THE CITY OF CHICAGO

81. Plaintiffs re-allege paragraphs 1 - 65 as though fully stated here.

ANSWER: Defendant re-alleges her Answers to paragraphs 1 - 65 as though fully stated here.

82. The acts of the individual defendants as alleged above were committed pursuant to one or more *de facto* policies, practices, or customs of the City of Chicago, including, but not limited to: (I) the failure to properly investigate allegations of police misconduct; (ii) the failure to have a system which monitors patterns of alleged police misconduct; (iii) the failure to

properly discipline sustained allegations of police misconduct; (iv) the failure to properly maintain records of police misconduct and allegations of police misconduct, including the use of excessive force and false arrest; and (v) the failure to properly hire, train, monitor, and/or supervise police officers.

ANSWER: These allegations are not directed to this Defendant

83. A *de facto* policy, practice, and custom of the police code of silence results in police officers refusing to report instances of police misconduct of which they are aware, despite their obligation to do so.

ANSWER: These allegations are not directed to this Defendant

84. This conduct includes police officers who remain silent or give false or misleading information during official investigations in order to protect themselves or fellow officers from internal discipline or retaliation, civil liability, or criminal prosecution.

ANSWER: These allegations are not directed to this Defendant

85. As a matter of policy and practice, the Defendant City of Chicago facilitates the misconduct at issue here by failing to adequately punish and discipline prior instances of similar misconduct, thereby leading Chicago Police Officers to believe that their actions will never be scrutinized and directly encouraging future abuses such as those that were aimed towards Plaintiffs.

ANSWER: These allegations are not directed to this Defendant

86. As a matter of widespread practice so prevalent as to compromise municipal policy, officers of the Chicago Police Department abuse citizens in a manner similar to that alleged by Plaintiffs on a frequent basis, yet the Chicago Police Department makes findings of wrongdoings in only a handful of cases.

ANSWER: These allegations are not directed to this Defendant

87. The Defendant City of Chicago has failed to act to remedy the patterns of abuse described in the preceding paragraphs, despite actual knowledge of the same, thereby causing the types of injuries alleged here.

ANSWER: These allegations are not directed to this Defendant

COUNT V
STATE LAW CLAIM - FALSE IMPRISONMENT AND FALSE ARREST

88. Plaintiffs re-allege paragraphs 1 - 65 as though fully stated here.

ANSWER: Defendant re-alleges her Answers to paragraphs 1 - 65 as though fully stated here.

89. Defendant London (Star No. 11636), Defendant Williams (Star No. 12544), and various unknown officers restrained and detained Plaintiffs.

ANSWER: Defendant London denies these allegations as they relate to her.

90. Defendant London (Star No. 11636) and Defendant Williams (Star No. 12544) did not have reasonable grounds to believe that Plaintiffs committed an offense.

ANSWER: Defendant London denies these allegations as they relate to her.

91. Defendant London (Star No. 11636), Defendant Williams (Star No. 12544), and a various unknown officers arrested Plaintiff Fisher and kept him in a cell overnight.

ANSWER: Defendant London denies these allegations as they relate to her.

92. Defendant London (Star No. 11636) and Defendant Williams (Star No. 12544) did not have reasonable grounds to believe that Plaintiff Fisher committed an offense.

ANSWER: Defendant London denies these allegations as they relate to her.

93. At all relevant times, Defendant London (Star No. 11636) and Defendant Williams (Star No. 12544) served as duly appointed City of Chicago and Chicago Police Department employees, and acted under the color of law and in their official capacities as sworn law enforcement officers.

ANSWER: Defendant London admits the allegation as it pertains to her.

COUNT VI

STATE LAW CLAIM - FAILURE TO INTERVENE

94. Plaintiffs re-allege paragraphs 1 - 65 as though fully stated here.

ANSWER: Defendant re-alleges her Answers to paragraphs 1 - 65 as though fully stated here.

95. Defendant Williams, various unknown officers who detained Plaintiffs, and various unknown officers working for the Chicago Police Department (including those unknown officers working for the Independent Police Review Authority) knew that Defendant London's allegations were false or acted with reckless disregard as to whether Defendant London's claims were false.

ANSWER: These allegations are not directed to this Defendant

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 15 of 22

96. Defendant Williams and various unknown officers failed to intervene in the detention of Plaintiffs.

ANSWER: These allegations are not directed to this Defendant

97. Defendant Williams and various unknown officers failed to intervene prior to or during the criminal proceedings of Plaintiffs.

ANSWER: These allegations are not directed to this Defendant

98. At all relevant times, Defendant Williams (Star No. 12544) and various unknown officers served as duly appointed City of Chicago and Chicago Police Department employees, and acted under the color of law and in their official capacities as sworn law enforcement officers.

ANSWER: These allegations are not directed to this Defendant

COUNT VII
STATE LAW CLAIM - MALICIOUS PROSECUTION

99. Plaintiffs re-allege paragraphs 1 - 65 as though fully stated here.

ANSWER: Defendant re-alleges her Answers to paragraphs 1 - 65 as though fully stated here.

100. Defendant London (Star No. 11636), Defendant Williams (Star No. 12544), and various unknown officers knew that they lacked justification for seizing, detaining, or arresting Plaintiffs.

ANSWER: Defendant London denies these allegations as they relate to her.

101. Defendant London (Star No. 11636), Defendant Williams (Star No. 12544), and various unknown officers willingly commenced and continued criminal proceedings against Plaintiffs knowing that the underlying allegations were false.

ANSWER: Defendant London denies these allegations as they relate to her.

102. Defendant London (Star No. 11636), Defendant Williams (Star No. 12544), and various unknown officers willingly fabricated information and withheld exculpatory information.

ANSWER: Defendant London denies these allegations as they relate to her.

103. Defendant London (Star No. 11636) willingly testified at trial, under oath, knowing that her testimony against Plaintiffs was false.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 16 of 22

ANSWER: Defendant London denies these allegations as they relate to her.

104. Defendant London (Star No. 11636), Defendant Williams (Star No. 12544), and various unknown officers acted with malice and willfulness.

ANSWER: Defendant London denies these allegations as they relate to her.

105. At all relevant times, Defendant London (Star No. 11636), Defendant Williams (Star No. 12544), and various unknown officers served as duly appointed City of Chicago and Chicago Police Department employees, and acted under the color of law and in their official capacities as sworn law enforcement officers.

ANSWER: Admit

106. As a result of Defendant London (Star No. 11636), Defendant Williams (Star No. 12544), and various unknown officers' malicious prosecution, Plaintiffs were detained.

ANSWER: Defendant London denies these allegations as they relate to her.

107. As a result of Defendant London (Star No. 11636), Defendant Williams (Star No. 12544), and various unknown officers' malicious prosecution, Plaintiff Fisher was arrested.

ANSWER: Defendant London denies these allegations as they relate to her.

108. Plaintiffs Fisher and Jones were found not guilty.

ANSWER: Admit

109. Plaintiff Green's conviction was vacated on August 19, 2011.

ANSWER: Defendant London admit that Plaintiff Green's conviction was vacated, but upon information and belief deny that it was vacated on the date indicated.

COUNT VIII
STATE LAW CLAIM - INTENTIONAL INFILCTION OF EMOTIONAL DISTRESS

110. Plaintiffs re-allege paragraphs 1 - 65 as though fully stated here.

ANSWER: Defendant re-alleges her Answers to paragraphs 1 - 65 as though fully stated here.

111. Defendant London (Star No. 11636), Defendant Williams (Star No. 12544), and various unknown officers' conduct was extreme and outrageous.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 17 of 22

ANSWER: Defendant London denies these allegations as they relate to her.

112. Defendant London (Star No. 11636), Defendant Williams (Star No. 12544), and various unknown officers' intended to cause, or recklessly disregarded the probability of, causing emotional distress.

ANSWER: Defendant London denies these allegations as they relate to her.

113. Plaintiffs have suffered (and continue to suffer) emotional distress in the form of severe grief, humiliation, shame, embarrassment, fright, anxiety, anguish, mental pain, depression, and/or various physical manifestations.

ANSWER: The Defendant lacks knowledge or information sufficient to form a belief about the truth of the allegation

114. The acts of Defendant London (Star No. 11636), Defendant Williams (Star No. 12544), and various unknown officers proximately and directly caused Plaintiffs' emotional distress.

ANSWER: Defendant London denies these allegations as they relate to her.

115. At all relevant times, Defendant London (Star No. 11636), Defendant Williams (Star No. 12544), and various unknown officers served as duly appointed City of Chicago and Chicago Police Department employees, and acted under the color of law and in their official capacities as sworn law enforcement officers.

ANSWER: Defendant London admits the allegation as it pertains to her.

116. At all relevant times, Defendant London (Star No. 11636), Defendant Williams (Star No. 12544), and various unknown officers served as duly appointed City of Chicago and Chicago Police Department employees, and acted under the color of law and in their official capacities as sworn law enforcement officers.

ANSWER: Defendant London admits the allegation as it pertains to her.

COUNT IX
STATE LAW CLAIM - INDEMNIFICATION/RESPONDEAT SUPERIOR

117. Plaintiffs re-allege paragraphs 1 - 65 as though fully stated here.

ANSWER: Defendant re-alleges her Answers to paragraphs 1 - 65 as though fully stated here.

118. Under Illinois law, public entities must pay any tort judgment for compensatory damages for which employees are liable within the scope of their employment activities. 35

ILCS 10/9-102.

ANSWER: Admit

119. At all relevant times, Defendant London (Star No. 11636), Defendant Williams (Star No. 12544), and various unknown officers served as duly appointed City of Chicago and Chicago Police Department employees, and acted under the color of law and in their official capacities as sworn law enforcement officers.

ANSWER: Defendant London admits the allegation as it pertains to her.

AFFIRMATIVE DEFENSES

1. Defendants are government officials who perform discretionary functions. At all times material to the events alleged in Plaintiff's Complaint, a reasonable police officer objectively viewing the facts and circumstances that confronted Defendants could have believed their actions to be lawful, in light of clearly established law and the information that Defendants possessed. Defendants, therefore, are entitled to qualified immunity as a matter of law.
2. To the extent which Plaintiff failed to mitigate any of his claimed injuries or damages, any verdict or judgment obtained by Plaintiff must be reduced by application of the principle that he had a duty to mitigate those claimed injuries and damages, commensurate with the degree of failure to mitigate attributed to Plaintiff by the jury in this case.
3. As to Plaintiff's state law claims, Defendants are not liable for injuries arising out of their exercise of discretionary acts. Illinois Local Governmental and Governmental Employees Tort Immunity Act, 745 ILCS 10/2-201.
4. As to Plaintiff's state law claims, Plaintiff cannot establish willful or wanton conduct on the part of Defendants and therefore they are immune from suit. Illinois

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 19 of 22

Local Governmental and Governmental Employees Tort Immunity Act, 745 ILCS 10/2-202.

5. As to Plaintiff's state law claims, Defendants are not liable for any injury caused by the acts or omissions of another person. Illinois Local Governmental and Governmental Employees Tort Immunity Act, 745 ILCS 10/2-202.

6. As to Plaintiff's state law claims, Defendants are not liable to pay attorney's fees as "the law in Illinois clearly is that absent a statute or contractual agreement 'attorney fees and the ordinary expenses and burdens of litigation are not allowable to the successful party.'" See Kerns v. Engelke, 76 Ill.2d 154, 166 (1979) (citations omitted).

7. As to Plaintiff's state law claims, under the Illinois tort immunity law, Defendants are not liable for any of the claims alleged because a public employee, as such, and acting within the scope of his employment is not liable for any injury caused by the act or omission of another person. 745 ILCS 10/2-204 (2002).

CONCLUSION

WHEREFORE, Defendant London request all Counts of this Complaint be dismissed with prejudice and cost be awarded in her favor and against the Plaintiff and such other relief as the Court deems fit.

JURY DEMAND

Defendants demand trial by jury.

Dated: December 17, 2014

Respectfully submitted,

/s/ Matthew A. Hurd
MATTHEW A. HURD

Deputy Corporation Counsel

30 N. LaSalle Street
Suite 900
Chicago, Illinois 60602
(312) 744-5170 (Phone)
(312) 744-6566 (Fax)
Attorney No. 6191532

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 21 of 22

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

DEBRA GREEN, ANTHONY FISHER, and TANEAL JONES,)	Case Number 11 CV 07067
)	
Plaintiff,)	JUDGE KOCORAS
vs.)	Magistrate Judge Gilbert
CHICAGO POLICE OFFICER SYLSHINA LONDON, Star No. 11636; CHICAGO POLICE)	

OFFICER BENNY WILLIAMS, Star No. 12544,)
and VARIOUS UNKNOWN OFFICERS OF THE)
CHICAGO POLICE DEPARTMENT, Individually)
and as Employees/Agents of the CITY OF)
CHICAGO, a municipal corporation,)
Defendants.)

NOTICE OF FILING AND CERTIFICATE OF SERVICE

TO: Lisa M. Taylor/
Samuel E. Adam
HENDERSON & ADAM LLC
330 S. Wells Street - Suite 300
Chicago, Illinois 60606
(312) 262-2900

PLEASE TAKE NOTICE that on this 17 day of December 2014, I have caused to be e-filed with the Clerk of the United States District Court for the Northern District of Illinois, Eastern Division **DEFENDANT'S ANSWER TO PLAINTIFF'S FIRST AMENDED COMPLAINT**, a copy of which is herewith served upon you.

I hereby certify that I have served this notice and the attached document by causing it to be delivered by electronic means to the person named above at the address shown this 17 day of December 2014.

/s/ Matthew A. Hurd
Matthew A. Hurd
Deputy Corporation Counsel

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 22 of 22

ELECTRONICALLY FILED
 7/2/2015 12:12 PM
 2014-CH-15338
 CALENDAR: 11
DOCKETED
 OCT 19 2000
 CIRCUIT COURT OF
 COOK COUNTY, ILLINOIS
 CHANCERY DIVISION
 CLERK DOROTHY BROWN

UNITED STATES DISTRICT COURT
 NORTHERN DISTRICT OF ILLINOIS
 EASTERN DIVISION

UNITED STATES OF AMERICA)

v.)

FILED)

WILLIAM A. HANHARDT,)

JOSEPH N. BASINSKI,)

PAUL J. SCHIRO,)

SAM DESTEFANO,)

GUY ALTOBELLO, and)

WILLIAM R. BROWN.)

OCT 19 2000
 MICHAEL W. DORRINS, CLERK
 UNITED STATES DISTRICT COURT

NO.)

DOCR 0853

Violations: Title 18,
 United States Code,
 Sections 371, 1962(d),
 2314 and 2315.

JUDGE NOURL

MAGISTRATE JUDGE KENNEDY

COUNT ONE

The SPECIAL JANUARY 1999-1 GRAND JURY charges:

1. At all times material to this indictment:

(a) From July 13, 1953, until his retirement on pension as a captain on March 26, 1986, defendant WILLIAM A. HANHARDT was employed by the Chicago Police Department ("CPD"), and held several supervisory positions, including Chief of Detectives, Chief of Traffic, Commander of the Burglary Section, Deputy Superintendent for the Bureau of Inspectional Services, and District Commander. For a portion of the period of the indictment until the date of the indictment, defendant HANHARDT resided at 835 Heather Road, Deerfield, Illinois.

(b) Defendant GUY ALTOBELLO was employed by Altobello Jewelers, Inc., a retail jewelry store located at 100 East Roosevelt Road, Store 19, Villa Park, Illinois. ALTOBELLO's duties included meeting with traveling wholesale jewelers to

discuss, examine and make wholesale purchases from their jewelry lines.

(c) The Hyatt Corporation was an Illinois corporation. Among other things, it operated the Hyatt Regency Columbus Hotel at 350 North High Street, Columbus, Ohio, which was near the Greater Columbus Convention Center, providing accommodations to travelers. As a service to its guests, the Hyatt provided the use of safety deposit boxes located in a room near the registration desk.

(d) In August 1994, the Greater Columbus Convention Center hosted the 1994 Mid-America Jewelry Show. Many of the attending jewelers stayed at the Hyatt Regency Columbus Hotel. The following entities, which engaged in and had activities that affected interstate commerce, sent representatives to the 1994 Mid-America Jewelry Show, and had representatives who utilized safety deposit boxes at the Hyatt Regency Columbus Hotel:

(i) Mopaz Diamonds, Inc., a New York corporation, was located at 580 Fifth Avenue, New York, New York.

(ii) World Diamond Imports, Ltd., and D&R Diamond Importers, Inc., were Arizona corporations that were located at 6900 East Camelback Road, Scottsdale, Arizona.

(iii) Ragar Company was a partnership in New Jersey.

(iv) Jewel-Que, Inc., doing business as Jeweltique, was a New York corporation located at 15 West 47th Street, New York, New York.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 2 of 32

(v) M.B. Saxon Co., Inc., was an Ohio corporation.

(vi) Koss & Shechter Diamonds Ltd., doing business as Genesis II, was a New York corporation located at 580 5th Avenue, Suite 911, New York, New York.

(vii) Marsha's 14 Karat Gold Jewelry, was a sole proprietorship located in Ohio.

(viii) The Gemological Institute of America was a nonprofit educational organization of the jewelry industry in the United States.

(e) The following entities were all also involved in the jewelry industry and were engaged in and had activities that affected interstate commerce:

(i) Baume & Mercier, Inc. was a corporation organized and existing under the laws of Switzerland. Its subsidiary, Baume & Mercier, was a Division of VLG North America, Inc., located at 663 Fifth Avenue, New York, New York.

(ii) Nafco Gems, Ltd. ("Nafco") was an Arizona corporation located in Scottsdale, Arizona.

(iii) Mayfield's Company was an Arizona corporation located in Scottsdale, Arizona.

(iv) Mikan, Inc., was a Delaware corporation located in Miami, Florida. Mikan, Inc. also had an office in Israel.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 3 of 32

(v) Dennis D. Naughton Jewelers, doing business as Naughton Jewelers, was an Arizona corporation located at 3172 Camelback Road, Phoenix, Arizona.

(vi) Gaston Jewelers Inc. was an Arizona corporation located at 3602 West Bell Road, Glendale, Arizona.

(vii) Golden Rule Jewelers, Inc., doing business as "Jewelry by Albert," was an Arizona corporation. After August 22, 1996, it was located at 8220 North Hayden Road, Suite 111. Before August 22, 1996, it was located at 8180 North Hayden Road, Suite 102D, Scottsdale, Arizona.

(viii) Smith Fine Jewelers, Inc. was an Arizona corporation. After October 1997, it was located at 7704 East Doubletree Ranch Road, Scottsdale, Arizona. Before October 1997 it was located at 8989 East Via Linda, Suite 106, Scottsdale, Arizona.

(ix) Molina, Inc., doing business as Molina Fine Jewelers, was an Arizona corporation located at 3134 East Camelback Road, Phoenix, Arizona.

(x) Elan Ltd. was located at 589 5th Avenue, Suite 1501, New York, New York.

(xi) Kobi Katz, Inc., doing business as Baguette World, was a California corporation located at 640 South Hill Street, Suite 851, Los Angeles, California.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 4 of 32

(xii) Lieber & Solow Ltd. was a Delaware corporation located at 1140 Avenue of Americas, New York, New York.

(xiii) ESY, Inc. was a New York corporation located at 30 West 47th Street, Suite 601, New York, New York.

(xiv) Yahalom Inc., doing business as Baguettes USA, was a California corporation located at 550 South Hill Street, Suite 725, Los Angeles, California.

(xv) J. Schliff and Sons, Inc., doing business as Gem Platinum Manufacturing Company (hereafter "Gem Platinum") was a New York corporation located at 48 West 48th Street, New York, New York.

(xvi) Solar Diamonds, Inc. was a New York corporation located at 580 5th Avenue, New York, New York.

(xvii) Advanced Ring Manufacturing Company through 1986 was a company located at 145 West 45th Street, New York, New York.

(xviii) Oscar Heyman & Brothers, Inc., was a New York corporation located at 501 Madison Avenue, 15th Floor, New York, New York.

(xix) DeBella Fine Gems and Jewelry was a New Mexico corporation located at 100 East Palace Avenue, Santa Fe, New Mexico.

(xx) Rolex Watch USA, Inc., was a New York corporation located at 665 5th Avenue, New York, New York.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 5 of 32

(xxi) Horizon Imports was an Illinois corporation located at 5 South Wabash, Chicago, Illinois.

(xxii) H.K. Mallak, Inc., was a New York corporation located in Great Neck, New York.

(xxiii) Phillip Wolman & Co. was a California corporation located at 550 South Hill Street, Los Angeles, California.

(xxiv) Gordon Brothers Corporation was a Massachusetts corporation located at 40 Broad Street, Boston, Massachusetts.

(f) From January 31, 1996, through February 6, 1996, the American Gem Trade Association ("AGTA") held its annual convention at the Tucson Convention Center, in Tucson, Arizona. This convention was open only to members of the Association, not to the general public. From February 7, 1996 through February 11, 1996, the Tucson Gem and Mineral Society held its trade show at the Tucson Convention Center which the trade show was open to the general public. Throughout the same two week period, several hotels in Tucson, including the Holiday Inn at 181 West Broadway, Tucson, Arizona, held smaller jewelry shows, .

(g) From May 29, 1996, through June 4, 1996, the Jewelers Circular Keystone ("JCK") held its annual JCK International Jewelry Show at the Sands Expo and Convention Center in Las Vegas, Nevada. This show was open to members of the jewelry trade only, not to the general public.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 6 of 32

(h) The Great Lakes Jewelry Show took place on August 24 and 25, 1996, at the Marriott Lincolnshire, Lincolnshire, Illinois.

I. THE ENTERPRISE

2. At all times material to this indictment, there existed a criminal organization, i.e. a group of individuals consisting of defendants WILLIAM A. HANHARDT, JOSEPH N. BASINSKI, PAUL J. SCHIRO, SAM DESTEFANO, GUY ALTOBELLO and others known and unknown, including James D'Antonio and Robert Paul, both now deceased. This group of individuals associated together for the purpose of engaging in an organized plan and scheme to gather information on individuals involved in the jewelry industry for the purpose of committing thefts of jewelry and disposing of the stolen jewelry, at times gathering such information from law enforcement and commercial databases by utilizing intrastate and interstate wire communications. This group of individuals, hereinafter known as "the enterprise," constituted an "enterprise" as that term is used in Title 18, United States Code, Section 1961(4), that is, a group of individuals associated in fact, which enterprise was engaged in and the activities of which affected interstate commerce.

3. The enterprise existed primarily to provide income to certain of its members through illegal activities.

4. In order to carry out its activities, the enterprise utilized individuals employed by and associated with it who had

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 7 of 32

varying roles and responsibilities. The roles and responsibilities were as follows:

DEFENDANT WILLIAM A. HANHARDT

(a) Defendant WILLIAM A. HANHARDT (hereafter "HANHARDT"), was the leader of the enterprise. In that capacity he supervised codefendant JOSEPH N. BASINSKI and together they directed the activities of others employed by and associated with the enterprise. HANHARDT directed the other defendants and others in their gathering of information on potential jewelry theft victims and the surveillance of several such individuals. He utilized certain CPD officers to do database searches of CPD and other law enforcement computers to obtain information concerning jewelry salespersons. Similarly, he caused a private investigator to conduct credit bureau database searches and other database searches to gather information concerning individuals who were traveling jewelry salespersons. At times, HANHARDT used the telephone at his residence at 835 Heather Road, Deerfield, Illinois, to direct certain defendants and others to further the interests of the enterprise. HANHARDT personally participated in the theft of jewelry.

DEFENDANT JOSEPH N. BASINSKI

(b) Defendant JOSEPH N. BASINSKI (hereafter "BASINSKI") served the enterprise by identifying potential targets for the enterprise, including owners of or salespersons to jewelry stores

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 8 of 32

or businesses, by physical surveillances, telephone calls, database searches and other means. He would physically follow and surveill potential victims or locations for the purpose of stealing high quality jewelry. He assisted the enterprise by directing and assisting in directing the activities of one or more of his codefendants in accomplishing the aims of the enterprise, including directing their activities on physical surveillances of locations and individuals and also the actual theft of jewelry. He also served the enterprise by maintaining information on potential victims of the enterprise and certain tools and instrumentalities of the enterprise. BASINSKI personally participated in the theft of jewelry.

DEFENDANT PAUL J. SCHIRO

(c) Defendant PAUL J. SCHIRO (hereafter "SCHIRO") served the enterprise by, among other things, conducting physical surveillances of jewelry stores, jewelry shows, owners of jewelry stores, and jewelry salespersons. SCHIRO personally participated in the theft of jewelry.

DEFENDANT SAM DESTEFANO

(d) Defendant SAM DESTEFANO (hereafter "DESTEFANO") served the enterprise by, among other things, conducting physical surveillances of jewelry stores, owners of jewelry stores, and jewelry salespersons. DESTEFANO personally participated in the theft of jewelry.

DEFENDANT GUY ALTOBELLO

(e) Defendant GUY ALTOBELLO (hereafter "ALTOBELLO) served the enterprise by providing one or more of his co-defendants with information concerning jewelry salespersons that conducted business with Altobello Jewelers, Inc., so that certain of his co-defendants could further identify such persons and determine the most opportune occasion to steal jewelry from such persons.

JAMES D'ANTONIO

(f) Until his death in December 1993, James D'Antonio was a coconspirator and served the enterprise by, among other things, maintaining information of traveling jewelry salespersons and maintaining various tools and instrumentalities of the enterprise.

ROBERT PAUL

(g) Robert Paul, now deceased, was a coconspirator and served the enterprise by conducting physical surveillance of jewelry stores and jewelry salespersons in Arizona and by providing a cellular telephone used by his coconspirators.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 10 of 32

II. THE RACKETEERING CONSPIRACY

5. Beginning in or about the early 1980s and continuing thereafter to in or about April 1998, the exact dates being to the Grand Jury unknown, at Chicago in the Northern District of Illinois, Eastern Division, and elsewhere,

WILLIAM A. HANHARDT,
JOSEPH N. BASINSKI,
PAUL J. SCHIRO,
SAM DESTEFANO, and
GUY ALTOBELLO,

defendants herein, being persons employed by and associated with an enterprise, that is, the enterprise as described in Paragraph 2 above, which enterprise engaged in, and the activities of which affected, interstate commerce, did knowingly conspire together and with other persons known and unknown to the grand jury, to conduct and participate, directly and indirectly, in the conduct of the affairs of the enterprise through a pattern of racketeering activity as those terms are defined in Title 18, United States Code, Section 1961(1), in violation of Title 18, United States Code, Section 1962(c), as further specified in Paragraphs 6 and 7 below,

6. The racketeering activity consisted of:

(a) Transportation of stolen goods of the value of \$5000 or more in interstate commerce, in violation of Title 18, United States Code, Section 2314.

(b) Receipt, possession, concealment, storage, sale and disposal of stolen goods of the value of \$5,000 or more, which had

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 11 of 32

crossed a state boundary after being stolen, knowing the same to have been stolen, in violation of Title 18, United States Code, Section 2315.

7. As part of the conspiracy, each of the defendants and others agreed that a conspirator would commit at least two acts of racketeering in the conduct of the affairs of the enterprise.

III. MANNER AND MEANS OF THE CONSPIRACY

8. Among the manner and means of the conspiracy agreed to by the defendants and others, were the following:

(a) It was part of the conspiracy that one or more of the conspirators would and did steal jewelry and cause some or all of said jewelry to be transported in interstate commerce, including the following:

- 1) The theft from the vehicle of a salesperson for Baume & Mercier, Inc., of approximately 180 watches having a total value of approximately \$310,000 in Glendale, Wisconsin, on October 8, 1984.
- 2) The theft from the vehicle of a salesperson for Rolex Watch USA, Inc., of watches having a value of approximately \$500,000 on or about October 13, 1986, in Monterey, California.
- 3) The theft from the vehicle of a salesperson for Gordon Brothers Corporation of jewelry having a value of approximately \$125,000 in Englewood, Ohio, on or about August 28, 1989.
- 4) The theft of a bag of a salesperson for J. Schliff and Sons, Inc., doing business as Gem Platinum Manufacturing, containing jewelry having a value of approximately \$1,000,000 on or about June 30, 1992, at Dallas/Ft. Worth, Texas.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 12 of 32

- 5) The theft from the rental vehicle of a salesperson for J. Schliff and Sons, Inc., doing business as Gem Platinum Manufacturing, of jewelry having a value of in excess of \$1,000,000 in Flat Rock, Michigan, on June 23, 1993.
- 6) The theft from the rental vehicle of a salesperson for H.K. Mallak, Inc., of jewelry having a value of approximately \$240,000 on August 3, 1993, in Mankato, Minnesota.
- 7) The theft from representatives for Nafco Gems, Ltd. and Mayfield's Company of jewelry having a value in excess of \$170,000 at the Skyharbor Airport, Phoenix, Arizona, on May 7, 1994.
- 8) The theft from safety deposit boxes at the Hyatt Regency Hotel, Columbus, Ohio, of jewelry, gemstones, U.S. currency, and other material of an aggregate value in excess of \$1,500,000 on August 27, 1994. The victims of such theft included the various entities listed in Paragraph 1(e) of this Count.

(b) It was further a part of the conspiracy that one or more of the conspirators would and did attempt to steal and remove jewelry from persons involved in the jewelry trade, including the following:

- 1) The theft from a hotel room at the Los Angeles Airport Hilton of the suitcase of a salesperson for Solar Diamonds, Inc. on or about June 17, 1994, in Los Angeles, California.
- 2) The theft from the vehicle of a salesperson for Baume & Mercier, Inc., of two jewelry cases on October 2, 1996, one of which contained numerous fine watches, in Chesterton, Indiana, as more fully described in Count Two.

(c) It was further part of the conspiracy that one or more of the conspirators would and did physically surveill the residences, places of work, and/or the persons of individuals the

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 13 of 32

conspirators believed to be involved in the jewelry trade, including the following:

- 1) A Nafco Gems, Ltd. representative, his residence, his car and/or place of business in Arizona on various occasions, including in 1995 and 1996.
- 2) A jewelry appraiser, his car and/or residence in Arizona on various occasions including in February and March 1996.
- 3) A Mayfield's Company representative, her car, residence and/or place of business in Arizona and elsewhere including in 1996.
- 4) A Baume & Mercier salesperson, his car and/or residence in Illinois, Wisconsin, and Indiana on several occasions, including between April 1996 and October 1996, as more fully described in Count Two.
- 5) A Kobi Katz, Inc./Lieber & Sollow, Ltd. salesperson's residence in Illinois in August 1996.

(d) It was a part of the conspiracy that, to generate income, certain of the conspirators attempted to identify traveling jewelry salespersons and to obtain personal information on each such salesperson for the purpose of determining the most opportune time and occasion to steal from a car, hotel room, or other location, jewelry being transported by the salesperson.

(e) It was further part of the conspiracy that one or more of the conspirators would and did contact hotels and determine if a traveling jewelry salesperson was staying or was scheduled to stay at the hotel, including defendant HANHARDT contacting three hotels in Illinois on August 23, 1996, to determine if a certain Elan Ltd. salesperson had an advanced reservation, and defendant

DESTEFANO contacting numerous hotels in Minnesota on August 2-3, 1993, to determine the location of a certain H.K. Mallak, Inc., salesperson.

(f) It was further part of the conspiracy that one or more of the conspirators received information from defendant ALTOBELLO concerning, among other things, the identity of certain traveling jewelry salespersons, the nature and quality of their jewelry and/or a portion of the travel schedule of the traveling jewelry salespersons, including in 1996 a Mikan, Inc. salesperson and an ESY, Inc. salesperson.

(g) It was further a part of the conspiracy that, to facilitate the activities of the enterprise, certain of the conspirators obtained, maintained and used communications equipment such as walkie talkies, pagers, skypagers and cellular telephones.

(h) It was further a part of the conspiracy that, to perpetuate the enterprise, certain of the conspirators used and agreed to use money obtained from the pattern of racketeering activity in the operation of the enterprise.

(i) It was further a part of the conspiracy one or more of the conspirators, including defendants HANHARDT, BASINSKI, and SCHIRO, would and did physically surveill jewelry stores as part of a plan and scheme to identify persons that would carry jewelry to and from such jewelry stores, including the following:

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 15 of 32

- 1) Dennis D. Naughton Jewelers, doing business as Naughton Jewelers, and Molina, Inc., doing business as Molina Fine Jewelers, in Phoenix, Arizona, on numerous occasions during the years 1995 and 1996.
- 2) Golden Rule Jewelers, Inc. doing business as Jewelry by Albert, in Scottsdale, Arizona, on February 12, 1996.
- 3) Gaston Jewelers Inc. in Glendale, Arizona, on various occasions in February and March 1996.
- 4) Smith Fine Jewelers, Inc., in Scottsdale, Arizona, on February 12, 1996 and March 1, 1996.

(j) It was further a part of the conspiracy that the conspirators would and did attend jewelry shows designed for jewelry wholesalers and retailers, some not open to the public, to identify persons involved in the jewelry trade, and to evaluate the quality and quantity of the jewelry line of such jewelry wholesalers and retailers, including the following:

- 1) The American Gem Trade Association annual convention, held in 1996 in Tucson, Arizona.
- 2) The Tucson Gem and Mineral Society trade show, held in 1996 in Tucson, Arizona.
- 3) The annual Jeweler's Circular Keystone International Jewelry Show, held in 1996 in Las Vegas, Nevada.

(k) It was further a part of the conspiracy that certain of the conspirators would and did rent vehicles for the purpose of physically surveilling jewelry salespersons and jewelry stores.

(l) It was further a part of the conspiracy that certain of the conspirators obtained, maintained and used various tools and instrumentalities in order to assist in gaining access to vehicles,

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 16 of 32

vehicle trunks, vehicle ignitions, hotel rooms, safety deposit boxes and other locations, to avoid detection or to escape law enforcement, including locksmith tools, keymaking machines, related publications, automobile instruction books, automobile keys, hotel keys, key blanks, lock picks, "slim jims," smoke grenades, fake mustache and fake beard, key cutting dies, wrenches and other hand tools, evasion devices, taser, cam set, key cutters, bullet proof vests, cameras, listening devices, and key code books.

(m) It was further part of the conspiracy that certain of the conspirators would and did obtain luggage to be used to switch with the luggage of jewelry salespersons.

(n) It was further a part of the conspiracy that certain of the conspirators would and did obtain and create keys that provided access to vehicles being driven by jewelry salespersons, to hotel rooms, to safe deposit boxes and to other locations.

(o) It was further a part of the conspiracy that certain of the conspirators would and did request CPD officers, known and unknown, to cause searches to be made from CPD terminals that connected electronically to computer databases located both inside and outside of the State of Illinois, thereby gaining information on jewelry salespersons and cars driven by them in order to determine the most opportune moment to steal jewelry being transported by the salespersons, including the following computer database searches:

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 17 of 32

- 1) The Arizona license plate on the personal car of the Nafco Gems, Ltd. representative, utilizing the National Law Enforcement Telecommunications Systems Inc. ("NLETS") on January 20, 1996.
- 2) The Arizona license plate on the personal car of the jewelry appraiser, utilizing NLETS, on February 7, 1996.
- 3) The Illinois license plate on a rental car, leased by a Mikan, Inc. salesperson, on February 13, 1996.
- 4) The Illinois license plate on a rental car, leased by a Yahalom, Inc. representative, on March 25, 1996.
- 5) The Illinois license plate on the personal car of the Kobi Katz, Inc./Lieber & Solow, Ltd. salesperson on July 30, 1996.
- 6) The Illinois license plate on a rental car, leased by an ESY, Inc. salesperson, on August 29, 1996.

(p) It was further a part of the conspiracy that certain of the conspirators would and did request CPD officers to attempt to obtain car rental contract information on jewelry salespersons, including the rental car contract of a Yahalom, Inc. representative in March 1996, and the rental contract of an ESY, Inc. salesperson in August 1996.

(q) It was further a part of the conspiracy that certain of the conspirators would and did cause a private investigator to conduct database searches to be made of commercial electronic databases through commercial entities such as Trans Union Corporation, Equifax Credit Information Services, Inc., Database Technologies, Inc., and CSC Credit Services, Inc., and other

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 18 of 32

commercial database services, often utilizing the interstate wire communication system, thereby gaining from the databases credit reports and other personal and financial information on jewelry salespersons and others. These databases inquiries included interstate wire transmissions relative to the following jewelry salespersons and manufacturer representatives:

- 1) For a Mikan, Inc. salesperson, his wife, and Mikan, Inc.:
 - a) Database Technologies, Inc. ("DBT") database in Florida on February 27, 1996.
 - b) Equifax's database in Atlanta, Georgia on February 27, 1996.
 - c) Trans Union's database in Chicago on February 27, 1996.
 - d) DBT's database in Florida on March 1, 1996.
 - e) Trans Union's database in Chicago, Illinois on March 4, 1996.
 - f) Equifax's database in Atlanta, Georgia, through a CSC account, on March 8, 1996.
- 2) For a jewelry salesperson for DeBella Fine Gems and Jewelry Arts:
 - a) Trans Union's database in Chicago, Illinois, on or about July 25, 1992.
 - b) Equifax's database in Atlanta, Georgia, on or about July 25, 1992.
- 3) For a former jewelry salesperson for Oscar Heyman & Brothers, Inc.:
 - a) Trans Union's database in Chicago, Illinois, on or about August 7, 1992.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 19 of 32

- b) Equifax's database in Atlanta, Georgia, on or about August 8, 1992.
- 4) For a representative for Horizon Imports:
 - a) Trans Union's database in Chicago, Illinois, on or about April 12, 1994.
 - b) Equifax's database in Atlanta, Georgia, on or about April 12, 1994, relative to.
- 5) For a former jewelry salesperson for Advanced Ring Manufacturing, Inc., and his wife to Trans Union's database in Chicago, Illinois, on or about August 7, 1992.
- 6) For a jewelry salesperson for Phillip Wolman & Co. to Trans Union's database in Chicago, Illinois, on or about August 26, 1992.
- 7) For a jewelry salesperson for Kobi Katz, Inc. to the databases of Trans Union, Equifax, and TRW through Engineered Business Systems, Inc., on or about June 30, 1993.
 - (r) It was further a part of the conspiracy that certain of the conspirators would and did use walkie talkies to communicate for the purpose of conducting physical surveillances of jewelry stores and jewelry salespersons.
 - (s) It was further a part of the conspiracy that certain of the conspirators would and did use telephone calling cards and pay telephones to communicate the status of the conspiracy's activities and to discuss and direct future activity of the conspiracy and its members.
 - (t) It was further part of the conspiracy that certain of the conspirators obtained, created and maintained, various documents concerning numerous individuals involved in the jewelry

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 20 of 32

trade, all for the purpose of attempting to determine the most opportune time and location to steal jewelry from one or more of the individuals, along with attempting to limit the risk of being discovered by law enforcement. These documents included, among other documents, one or more of the following on one or more individuals:

- 1) Specific, detailed and accurate personal descriptive information on such individuals, their family members and their residences.
- 2) Specific, detailed and accurate information related to the businesses of such individuals.
- 3) Specific, detailed and accurate information on vehicles owned or utilized by such individuals, including key codes.
- 4) Travel itineraries and analyses including such information as airlines used, travel information, ticket numbers, travel dates, cities, hotels used, travel agencies and rental car companies utilized, number of miles driven, airline baggage claims tickets and hotel bills.
- 5) Specific, detailed and accurate information concerning various credit card, bank and other accounts of such individuals and, at times, credit bureau reports on certain such individuals.

(u) It was further part of the conspiracy that certain of the conspirators would and did deliver jewelry stolen from traveling salespersons to individuals for purchase.

(v) It was further part of the conspiracy that certain of the conspirators would and did cause money generated from the sale of stolen jewelry to be provided to certain of the conspirators.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 21 of 32

(w) It was further part of the conspiracy that certain of the conspirators misrepresented, concealed and hid, caused to be misrepresented, concealed and hidden, and attempted to misrepresent, conceal and hide the illegal operation of the enterprise and acts done in furtherance of the enterprise, including the following means:

(1) avoiding and limiting discussion of the enterprise's illegal activities over personal telephone lines;

(2) using aliases, including the name "Richard Stevens", when renting hotel rooms and paying in cash to avoid leaving a trail of their activities;

(3) using coded or ciphered language to discuss amongst themselves the attempts to identify jewelry salespersons and other acts to further their conspiracy;

(4) removing front license plates from their vehicles while conducting physical surveillances of jewelry salespersons and jewelry stores;

(5) using a telephone calling card in a fictitious name to communicate;

(6) altering their appearance, by changing clothes and otherwise, while surveilling jewelry salespersons or locations;

(7) using alias identities and possessing identification cards and other documents in alias names; and

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 22 of 32

(8) using prepaid or promotional telephone calling cards.

All of the above in violation of Title 18, United State Code, Section 1962(d).

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 23 of 32

COUNT TWO

The SPECIAL JANUARY 1999-1 GRAND JURY further charges:

2. At all times material to this indictment:

(a) Baume & Mercier, Inc. (hereinafter "Baume & Mercier") was a corporation organized and existing under the laws of the country of Switzerland. Its subsidiary was Baume & Mercier, a Division of VLG North America, Inc., located at 663 Fifth Avenue, New York, New York. Baume & Mercier was engaged in the wholesale fine watch business. An individual (hereinafter "Baume & Mercier salesperson") was a traveling salesperson for the company and lived in Park Ridge, Illinois.

2. Beginning prior to April 1996, and continuing until at least October 1996, in the Northern District of Illinois, Eastern Division and elsewhere,

WILLIAM A. HANHARDT,
JOSEPH N. BASINSKI,
PAUL J. SCHIRO, and
WILLIAM R. BROWN,

defendants herein, did conspire with each other and with others, known and unknown to the grand jury, to commit an offense against the United States, namely: to transport, transmit, and transfer in interstate commerce goods and merchandise of the value of \$5,000 or more, namely: fine watches, the property of Baume & Mercier, knowing the same to have been stolen, converted and taken by fraud, in violation of Title 18, United States Code, Section 2314.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 24 of 32

3. It was part of the conspiracy that the conspirators agreed with each other to steal fine watches being carried by the Baume & Mercier salesperson and to transport, deliver and sell the stolen watches in interstate commerce.

4. It was part of the conspiracy that certain of the conspirators, separately or together, traveled to Wisconsin and Indiana on occasion specifically to identify potential opportunities to steal the fine watches from the Baume & Mercier salesperson.

5. It was further part of the conspiracy that certain of the conspirators used duplicate vehicle keys and walkie-talkie radios while carrying out the planned theft of fine watches from the Baume & Mercier salesperson.

6. It was further part of the conspiracy that codefendant BASINSKI and defendant HANHARDT communicated by telephone and Skypager.

7. It was further part of the conspiracy that one or more of the conspirators would and did rent vehicles for the purpose of surveilling the Baume & Mercier salesperson in Illinois, Wisconsin, and Indiana.

8. It was further part of the conspiracy that one or more of the conspirators would and did conduct surveillances of the Baume & Mercier salesperson at his house and in his car.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 25 of 32

9. It was further part of the conspiracy that one or more of the conspirators would and did obtain and create keys that would provide access to the vehicle driven by the Baume & Mercier salesperson.

10. It was further part of the conspiracy that on October 2, 1996, near the Spa Restaurant in Chesterton, Indiana, the defendants entered the trunk of the vehicle of the Baume & Mercier salesperson and did remove from the vehicle two cases, one of which contained fifteen fine watches of an approximate value of \$58,000.

11. It was further part of the conspiracy that the conspirators would and did misrepresent, conceal, and hide, and cause to be misrepresented, concealed and hidden the purposes of and the acts done in furtherance of the conspiracy, and would and did use other means to avoid detection and apprehension by law enforcement authorities and otherwise to provide security for the members of the conspiracy.

OVERT ACTS

12. In furtherance of the conspiracy to effect the objects thereof, the defendants committed or caused to be committed, the following overt acts, among others:

- (a) On April 25, 1996, defendant HANHARDT and defendant BASINSKI had a telephone conversation.
- (b) On July 25, 1996, defendant BASINSKI surveilled the residence of the Baume & Mercier salesperson.

- (c) On July 30, 1996, defendants HANHARDT and BASINSKI surveilled the residence of the Baume & Mercier salesperson.
- (d) On August 16, 1996, defendant BASINSKI caused a telephone call to be made to a location in Michigan which could provide the key code for making a key for certain Lincoln automobiles manufactured by the Ford Motor Company.
- (e) On September 6, 1996, defendants HANHARDT and BASINSKI followed the Baume & Mercier salesperson in Illinois while the salesperson was driving his Lincoln.
- (f) On September 12, 1996, defendants HANHARDT and BASINSKI followed the Baume & Mercier salesperson as he drove his Lincoln from Illinois to Wisconsin.
- (g) On September 24, 1996, defendant HANHARDT followed the Baume & Mercier salesperson as he drove his Lincoln to the post office.
- (h) On September 30, 1996, defendant BASINSKI caused a telephone call to be made to a location in Michigan which could provide the key code for making a key for certain Lincoln automobiles manufactured by the Ford Motor Company.
- (i) On October 1, 1996, defendants HANHARDT, BASINSKI, SCHIRO and BROWN, followed the Baume & Mercier salesperson as he drove his Lincoln from Illinois to Wisconsin.
- (j) On October 2, 1996, defendants HANHARDT, BASINSKI, SCHIRO and BROWN, followed the Baume & Mercier salesperson from Illinois into Indiana.
- (k) On October 2, 1996, in Chesterton, Indiana, while the Baume & Mercier salesperson was in a restaurant, with defendants HANHARDT, SCHIRO and BROWN serving as lookouts, defendant BASINSKI, using a key, entered the trunk of the salesperson's Lincoln and removed two jewelry cases, one of which contained fifteen fine watches of an approximate value of \$58,000, and place the cases in the trunk of a rental car.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 27 of 32

- (l) On October 2, 1996, in Chesterton, Indiana, defendant BASINSKI drove the rental car a short distance from the restaurant, opened the rental car's trunk, lifted the two jewelry cases, replaced the cases back in the rental car's trunk and closed the trunk, and returned to the parking lot of the restaurant.
- (m) On October 2, 1996, in Chesterton, Indiana, with HANHARDT, SCHIRO and BROWN serving as lookouts, defendant BASINSKI returned to the Baume & Mercier salesperson's Lincoln that was parked in the restaurant parking lot, reopened the Lincoln's trunk and returned the two jewelry cases.

All in violation of Title 18, United States Code, Section 371.

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 28 of 32

FORFEITURE ALLEGATION

The SPECIAL JANUARY 1999-1 GRAND JURY further charges:

1. The allegations contained in Count One of the indictment are realleged and incorporated by reference for the purposes of alleging forfeiture pursuant to Title 18, United States Code, Section 1963.

2. As a result of the violation of Title 18, United States Code, Section 1962(d), as alleged in the foregoing indictment

WILLIAM A. HANHARDT,
JOSEPH N. BASINSKI,
PAUL J. SCHIRO,
SAM DESTEFANO, and
GUY ALTOBELLO,

defendants herein:

(a) have acquired and maintained interests in violation of Title 18, United States Code, Section 1962, which interests are subject to forfeiture to the United States pursuant to Title 18, United States Code, Section 1963(a)(1);

(b) have interests in, securities of, claims against, and property and contractual rights affording sources of influence over the enterprise described in Count One which defendants established, operated, controlled, conducted, and participated in the conduct of, and conspired to do so, in violation of Title 18, United States Code, Section 1962, thereby making all such interests, securities, claims, and property and contractual rights subject to forfeiture

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 29 of 32

to the United States of America pursuant to Title 18, United States Code, Section 1963(a)(2);

(c) have property constituting and derived from proceeds which obtained, directly and indirectly, from racketeering activity in violation of Title 18, United States Code, Section 1963 (a)(3).

3. The interests of the defendants, jointly and severally subject to forfeiture to the United States pursuant to Title 18, United States Code, Section 1963(a)(1), (a)(2), and (a)(3) include but are not limited to:

(a) \$4,845,000

(b) Miscellaneous jewelry, gems and watches

(c) As to defendant WILLIAM A. HANHARDT only:

Real property at 835 Heather Road, Deerfield, Illinois, being more particularly described as:

Lot 1 in Hamilton's Subdivision, being a subdivision of part of the south 355.30 feet (except the west 494.55 feet thereof) of the west $\frac{1}{4}$ of the southeast $\frac{1}{4}$ of the southeast $\frac{1}{4}$ of Section 28, Township 43 North, Range 12, East of the Third Principal Meridian, according to the Plat thereof recorded May 20, 1976 as document 1767938, in Book 54 of Plats, Page 48, in Lake County, Illinois.

(d) As to defendant SAM DESTEFANO only:

Real property at 2216 Durand Drive, Downers Grove, Illinois, being more particularly described as:

That part of Lot 12, of the Villas of Bending Oaks, being a subdivision of part of Sections 12 and 13, Township 38 North, Range 10, East of the Third Principal Meridian, lying Ely of a line described as being 58.68 feet W, as measured along the Sly line thereof, from the E line of said Lot 12, and

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
PAGE 30 of 32

67.87 feet W, as measured along the Nly line thereof, from the E line of said Lot 12, all in DuPage County, Illinois.

4. To the extent that the proceeds and property described above as being subject to forfeiture pursuant to Title 18, United States Code, Section 1963, as a result of any acts or omission by any defendant:

- (1) cannot be located upon the exercise of due diligence;
- (2) has been transferred or sold to, or deposited with, a third party;
- (2) has been placed beyond the jurisdiction of the Court;
- (3) has been substantially diminished in value, or;
- (4) has been commingled with other property which cannot be subdivided without difficult;

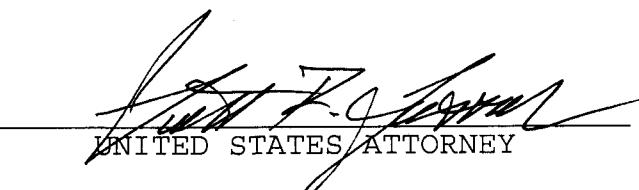
it is the intent of the United States of America, pursuant to Title 18, United States Code, Section 1963(m) to seek forfeiture of any other property of the defendants up to the value of the proceeds and property described above as being subject to forfeiture;

All pursuant to Title 18, United States Code, Section 1963.

A TRUE BILL:



FOR PERSON



UNITED STATES ATTORNEY

ELECTRONICALLY FILED
7/2/2015 12:12 PM
2014-CH-15338
NO PAGE 32 of 32

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA

vs.

WILLIAM A. HANHARDT,
JOSEPH N. BASINSKI,
PAUL J. SCHIRO,
SAM DESTEFANO,
GUY ALTOBELLO, and
WILLIAM R. BROWN.

I N D I C T M E N T

Violation(s) : Title 18, United States Code,
Sections 371 1962 (d), 2314 and 2315

A true bill,

Andrew Branchi

Foreman

Filed in open court this 19 day of October, A.D. 2000

MICHAEL W. DOBBINS

Michael W. Dobbins

Bail, \$ _____

Clerk

ELECTRONICALLY FILED
PAGE # 4595
9/2/2015 12:12 PM
2014-CH-15338
CALENDAR: 11
PAGE 1 of 1
CIRCUIT COURT OF
COOK COUNTY, ILLINOIS
CHANCERY DIVISION
CLERK DOROTHY BROWN

United States District Court, Northern District of Illinois

Name of Assigned Judge or Magistrate Judge	Charles R. Norgle	Sitting Judge if Other than Assigned Judge	CHANCERY DIVISION CLERK DOROTHY BROWN
CASE NUMBER	00 CR 853 - 1	DATE	10/25/2001
CASE TITLE	UNITED STATES OF AMERICA vs. WILLIAM A. HANHARDT		

[In the following box (a) indicate the party filing the motion, e.g., plaintiff, defendant, 3rd party plaintiff, and (b) state briefly the nature of the motion being presented.]

MOTION:

ANSWER

DOCKET ENTRY:

- (1) Filed motion of [use listing in "Motion" box above.]

(2) Brief in support of motion due _____.

(3) Answer brief to motion due _____. Reply to answer brief due _____.

(4) Ruling/Hearing on _____ set for _____ at _____.

(5) Status hearing[held/continued to] [set for/re-set for] on _____ set for _____ at _____.

(6) Pretrial conference[held/continued to] [set for/re-set for] on _____ set for _____ at _____.

(7) Trial[set for/re-set for] on _____ at _____.

(8) [Bench/Jury trial] [Hearing] held/continued to _____ at _____.

(9) This case is dismissed [with/without] prejudice and without costs[by/agreement/pursuant to]
 FRCP4(m) General Rule 21 FRCP41(a)(1) FRCP41(a)(2).

(10) [Other docket entry] Status hearing held. Defendant withdraws his plea of not guilty and enters a plea of guilty as to Counts One and Two of the superseding indictment. Defendant informed of his rights. Case referred to the probation department for a presentence investigation. Government's oral motion for an additional 21 days within which to tender their submissions to the probation department is granted. Sentencing set for January 31, 2002 at 9:30 a. m.

(11) [For further detail see order (on reverse side of/attached to) the original minute order.]

	No notices required, advised in open court.		35	Document Number
	No notices required.		45M	
	Notices mailed by judge's staff.			
	Notified counsel by telephone.			
✓	Docketing to mail notices.			
	Mail AO 450 form.			
	Copy to judge/magistrate judge.			
EF	courtroom deputy's initials		OCT 30 2001 JMS docketing deputy initials 35	236
			date mailed notice	
		Date/time received in central Clerk's Office	mailing deputy initials	

The Federal Information Manual

SECOND EDITION

How the Government
Collects, Manages, and
Discloses Information under
FOIA and Other Statutes

P. STEPHEN GIDIÈRE III



The materials contained herein represent the views of the author and should not be construed as the views of the author's firms, employers, or clients, or of the American Bar Association or the Section of Environment, Energy, and Resources, unless adopted pursuant to the bylaws of the Association.

Nothing contained in this book is to be considered as the rendering of legal advice for specific cases, and readers are responsible for obtaining such advice from their own legal counsel. This book is intended for educational and informational purposes only.

© 2013 American Bar Association. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher. For permission, complete the online request form at <http://www.americanbar.org/reprint>.

Printed in the United States of America

17 16 15 14 13 5 4 3 2 1

Library of Congress Cataloging-in-Publication Data

Gidere, P. Stephen, 1970-

The federal information manual : how the government collects, manages, and discloses information under FOIA and other statutes / by P. Stephen Gidere, III. — Second edition.

pages cm.

Includes bibliographical references and index.

ISBN 978-1-62772-252-5 (print : alk. paper)

1. Freedom of information—United States. 2. Government information—United States. 3. Public records—Access control—United States. I. Title. KF5753.G53 2013 342.73'0662—dc23

2013028020

Discounts are available for books ordered in bulk. Special consideration is given to state bars, CLE programs, and other bar-related organizations. Inquire at ABA Publishing, American Bar Association, 321 North Clark Street, Chicago, Illinois 60654-7598.

www.ShopABA.org

SUMMARY OF CONTENTS

LIST OF FIGURES AND TABLES	xii
ACKNOWLEDGMENTS	xiii
ABOUT THE AUTHOR	xv
LIST OF ABBREVIATIONS	xvii

CHAPTER 1: AN OVERVIEW OF FEDERAL INFORMATION DISPUTES	1
CHAPTER 2: AGENCY COLLECTION OF INFORMATION	15
CHAPTER 3: MANAGEMENT OF AGENCY RECORDS	45
CHAPTER 4: CLASSIFIED INFORMATION	69
CHAPTER 5: ACCESS TO FEDERAL RECORDS	113
CHAPTER 6: ELECTRONIC RECORDS AND FEDERAL PUBLIC WEBSITES	145
APPENDIX: RECOMMENDED GUIDELINES FOR FEDERAL PUBLIC WEBSITES	
DEVELOPED BY THE INTERAGENCY COMMITTEE ON GOVERNMENT INFORMATION PURSUANT TO THE E-GOVERNMENT ACT OF 2002	174
CHAPTER 7: THE ELEMENTS OF A SUCCESSFUL FOIA REQUEST	177
CHAPTER 8: REASONS FOR THE WITHHOLDING OF AGENCY RECORDS	215
APPENDIX: SELECTED EXEMPTION 3 STATUTES CITED BY FEDERAL AGENCIES	296
CHAPTER 9: LITIGATION INVOLVING FEDERAL RECORDS	317
CHAPTER 10: HOMELAND SECURITY INFORMATION	365

deferece in interpreting the FOIA itself, since no single federal agency is charged with its administration.¹²¹ Of course, deference in the Exemption 3 context is predicated on the fact that “the agency has adopted an interpretation of the [non-FOIA] statute and that the court knows what that interpretation is.”¹²²

8.4 TRADE SECRETS AND CONFIDENTIAL OR PRIVILEGED BUSINESS INFORMATION

Exemption 4 is the FOIA exemption of most interest to individuals and businesses that submit information about their financial and business affairs to federal agencies. Exemption 4 protects “trade secrets and commercial or financial information obtained from a person and privileged or confidential.”¹²³ The purpose of Exemption 4 is to prevent federal agencies from simply becoming conduits for the wholesale transfer of commercially valuable information from one competitor to another for, at most, the cost of minimal search, review, and copy fees. As expressed in legislative hearings on the FOIA, Congress, in enacting the broad disclosure statute, was *not* motivated to change “the ground rules of American business so that any person can force the Government to reveal information which relates to the

the CIA's reasons [for nondisclosure pursuant to the National Security Act] are entitled to deference; the CIA's declarations must still describe the justifications for nondisclosure with reasonably specific detail, demonstrate that the information withheld logically falls within the claimed exemptions, and show that the justification are not controverted by contrary evidence in the record or by evidence of CIA bad faith.” (citations and quotations omitted); *Cent. Plate Natural Res. Dist. v. U.S. Dep't of Agric.*, 643 F.3d 1142, 1147 (8th Cir. 2001) (“Generally a district court reviews FOIA complaints *de novo* . . . but the statutory *de novo* standard has been modified in FOIA exemption 3 cases. In such cases, a district court reviews *de novo* whether the statute qualifies for FOIA exemption 3 and whether the requested information at least arguably falls within the ambit of the withholding statute. If the district court determines that these two requirements are met, the FOIA *de novo* review normally ends.” (citations and quotation omitted. italics in original)).

^{121.} *Tax Analysts*, 117 F.3d at 613; *Carlson v. U.S. Postal Serv.*, 504 F.3d 1123, 1127 (9th Cir. 2007) (refusing to give the U.S. Postal Serv. deference in determining that “requested information was information of a commercial nature” under FOIA and noting that “[g]iven the court's responsibility to ensure that agencies do not interpret the exemptions too broadly, deference appears inappropriate in the FOIA context.” (citation omitted)).

^{122.} *Tax Analysts*, 117 F.3d at 613.

^{123.} 5 U.S.C. § 552(b)(4).

business activities of his competitor.”¹²⁴ Actions seeking to enjoin agencies from disclosing information under Exemption 4 are sometimes referred to as “reverse-FOIA actions” since the purpose is essentially the opposite of a normal FOIA lawsuit.¹²⁵ Reverse-FOIA actions are discussed in chapter 9. Exemption 4 protects three kinds of information: trade secrets, confidential commercial or financial information, and privileged commercial or financial information.

8.4.1 Trade secrets

The “trade secret” aspect of Exemption 4 has been given a fairly narrow scope by the courts. The D.C. Circuit in *Public Citizen Health Research Group v. Food and Drug Administration* defined the term as “a secret, commercially valuable plan, formula, process, or device that is used for the making, preparing, compounding, or processing of trade commodities and that can be said to be the end product of either innovation or substantial effort.”¹²⁶ Subsequent decisions have confirmed that the *Public Citizen* definition “narrowly cabins trade secrets to information relating to the ‘productive process’ itself.”¹²⁷ However, some courts have been willing to consider as a trade secret even a novel, unproven process that “may” have commercial value so long as it is both a “secret” and considered to be valuable by its proprietor.¹²⁸ Although there is little case law applying the trade secret aspect of Exemption 4, and courts generally have not moved far beyond the *Public Citizen* definition, this part of Exemption 4 remains a viable means of prohibiting disclosure of certain kinds of commercially valuable information.

^{124.} *Hearings on S. 1666 Before the Subcomm. on Administrative Practice and Procedure of the S. Comm. on the Judiciary*, 88th Cong. 1-2 (1964).

^{125.} See, e.g., *United Tech. Corp. v. U.S. Dep't of Def.*, 601 F.3d 557 (D.C. Cir. 2010); *Canadian Commercial Corp. v. Dep't of Air Force*, 514 F.3d 37 (D.C. Cir. 2008) (“A person whose information is about to be disclosed pursuant to a FOIA request may file a ‘reverse-FOIA action’ and seek to enjoin the government from disclosing it.” (citations omitted)).

^{126.} *Pub. Citizen Health Research Grp. v. Food & Drug Admin.*, 704 F.2d 1280, 1289-90 (D.C. Cir. 1983).

^{127.} *Ctr. for Auto Safety v. Nat'l Highway Transp. Safety Admin.*, 244 F.3d 144, 151 (D.C. Cir. 2001).

^{128.} *Freeman v. Bureau of Land Mgmt.*, 526 F. Supp. 2d. 1178, 1189 (D. Or. 2007); see also *Watkins v. Bureau of Customs & Border Prot.*, 643 F.3d 1189 (9th Cir. 2011).

8.4.2 Confidential business information

The real action under Exemption 4 is the phrase “commercial or financial information obtained from a person and . . . confidential.” Information falling within this aspect of Exemption 4 is commonly referred to as “confidential business information” or CBI. To qualify as CBI, information must be (1) commercial or financial information, (2) obtained from a person, and (3) confidential.¹²⁹

The words “commercial” or “financial” are given their ordinary meaning in the context of Exemption 4.¹³⁰ Most decisions do not spend much time discussing the issue; courts usually readily recognize that the information at issue is “commercial” or “financial.”¹³¹ One early case observed simply that “commercial” “surely means pertaining or relating to or dealing with commerce.”¹³²

In some cases involving natural resources, however, the commercial or financial nature of the information can be in dispute and the outcome is fact-dependent. For example, the D.C. Circuit has held that information about the location of endangered pygmy owls shared between a federal and a state agency was not commercial in nature or function and therefore does not fall within Exemption 4.¹³³ Information related to the proposed cleanup of polychlorinated biphenyls in the Hudson River that was submitted to EPA by an international corporation that is “clearly a commercial entity” was held not to constitute “commercial” information for Exemption 4 purposes by one district court.¹³⁴ In contrast, information about the allocation of water rights on the Flathead Indian Reservation was held to be commercial information within the meaning of the exemption,¹³⁵ as was information about wells and water on land held in trust for the La Posta Band of

Mission Indians because release of the information would interfere with the band’s ability to negotiate or litigate its water rights.¹³⁶

In addition, the term “person” is interpreted broadly to cover “a wide range of entities including corporations, associations and public or private organizations other than agencies.”¹³⁷ A Native American tribe is a “person” for Exemption 4 purposes.¹³⁸ Most disputes over CBI center on whether the information can be considered “confidential” for Exemption 4 purposes, and not all courts agree on which ways are permissible.

8.4.2.1 The competitive harm and impairment prongs

The parameters of what qualifies as “confidential” business information were first discussed in the seminal case of *National Parks and Conservation Association v. Morton*.¹³⁹ In *National Parks*, the D.C. Circuit held that information qualifies as “confidential” for purposes of FOIA’s Exemption 4 if it meets either a “competitive harm” or “impairment” test. In its now widely cited test, the court stated that “commercial or financial matter is ‘confidential’ for purposes of the Exemption if disclosure of the information is likely to have either of the following effects: (1) to impair the Government’s ability to obtain necessary information in the future; or (2) to cause substantial harm to the competitive position of the person from whom the information was obtained.”¹⁴⁰ These two tests are commonly referred to as the “impairment prong” and the “competitive harm prong” of Exemption 4. Nearly all of the other courts of appeals have adopted the D.C. Circuit’s test for confidentiality as stated in *National Parks*, and none have expressly rejected it.¹⁴¹ The impairment prong stems from the need of government officials

-
129. GC Micro Corp. v. Def. Logistics Agency, 33 F.3d 1109, 1112 (9th Cir. 1994); Bloomberg, L.P. v. Bd. of Governors of Fed. Reserve Sys., 601 F.3d 143, 147 (2d Cir. 2010).
130. Dow Jones Co. v. Fed. Energy Regulatory Comm’n, 219 F.R.D. 167, 176 (C.D. Cal. 2003) (citing *Pub. Citizen Health Research Grp.*, 704 F.2d at 1290).
131. *Id.* at 176.
132. Am. Airlines, Inc. v. Nat'l Mediation Bd., 588 F.2d 863, 870 (2d Cir. 1978).
133. *Nat'l Ass'n of Home Builders*, 309 F.3d at 38-39.
134. N.Y. Pub. Interest Research Grp. v. Envtl. Prot. Agency, 249 F. Supp. 2d 327 (S.D.N.Y. 2003).
135. Flathead Joint Bd. of Control v. Dep’t of the Interior, 309 F. Supp. 2d 1217, 1222 (D. Mont. 2004).

to access private information in order to carry out their duties in an intelligent and well-informed manner. If public release of the subject information would impair the government's ability to collect such information in the future—such as by discouraging submitters from cooperating and providing reliable information—then the information is protected by Exemption 4.¹⁴²

The competitive harm prong of Exemption 4 recognizes that submitters of valuable financial or commercial information would suffer very real competitive disadvantages if that information were published. The determination of competitive harm is typically made on a case-by-case basis. The party opposing disclosure need not show *actual* competitive harm.¹⁴³ Rather, the general standard recited by the courts requires that the submitter actually face competition and that substantial competitive injury would probably result from disclosure.¹⁴⁴ This standard does not require the court to "conduct a sophisticated economic analysis of the likely effects of disclosure."¹⁴⁵ At the same time, however, conclusory and generalized allegations are not sufficient to show competitive harm.¹⁴⁶ Affidavit testimony is usually the primary proof that is offered to make the competitive harm showing.¹⁴⁷

Under this standard, courts have found myriad types of information to be entitled to confidential treatment, including a lease for the storage of spent nuclear fuel;¹⁴⁸ information identifying individual employees, sub-

^{142.} (2d Cir. 1977); *Westinghouse Elec. Corp. v. Schlesinger*, 542 F.2d 1190 (4th Cir. 1976); *Cont'l Oil Co. v. Fed. Power Comm'n*, 519 F.2d 31 (5th Cir. 1975).

^{143.} See also *Cf. United Tech. Corp.*, 601 F.3d at 565 (citing impairment prong from *National Parks*, but noting that it may be inappropriate to apply in a reverse-FoIA situation); *Inner City Press/Cmty. on the Move v. Bd. of Governors of Fed. Reserve Sys.*, 463 F.3d 239, 245–48 (2d Cir. 2006) (explaining that while there is presumably no *National Parks* impairment to public disclosure where the person was compelled to submit the information to the agency, the agency must "both possess and exercise the legal authority to obtain information for the resulting submission of information to be deemed 'mandatory' under the *National Parks* test.").

^{144.} *GC Micro Corp.*, 33 F.3d at 1113.

^{145.} *Lion Raisins, Inc. v. Dep't of Agric.*, 354 F.3d 1072, 1079 (9th Cir. 2004); *Utah v. Dep't of the Interior*, 256 F.3d 967, 970 (10th Cir. 2001); *Niagara Mohawk Power v. Dep't of Energy*, 169 F.3d 16 (D.C. Cir. 1999).

^{146.} *Id.* 256 F.3d at 970 (quotations omitted).
^{147.} See, e.g., *United Tech. Corp.*, 601 F.3d at 564 ("But where, as here, a contractor pinpoints by letter and affidavit technical information it believes that its competitors can use in their own operations, the agency must explain why substantial competitive harm is not likely to occur if the information is disclosed.").

^{148.} *Id.* at 968.

jecting them to "employee raiding" and decreased morale;¹⁴⁹ information regarding the capabilities of equipment;¹⁵⁰ and production, market share, and sales volumes.¹⁵¹

8.4.2.2 The "third prong" of national parks

In addition to the impairment and competitive harm prongs, courts have elaborated on a so-called third prong under Exemption 4, focusing more broadly on the governmental interests that justify not releasing information received from other people. In *9 to 5 Organization for Women Office Workers v. Board of Governors of the Federal Reserve System*, the First Circuit recognized that footnote 18 of the *National Parks* decision left open the possibility that other governmental interests may be served by Exemption 4.¹⁵² Thus, the First Circuit's analysis went beyond just the possible impairment to the government process that might result from disclosure to include the consideration of the substantive harm to the government's statutory responsibility that might be caused by the release of specific information. "The inquiry in each case," reasoned the court, "should be whether public disclosure of the requested commercial or financial information will harm an identifiable private or governmental interest which the Congress sought to protect by enacting Exemption 4 of the FOIA."¹⁵³ Not all courts have adopted this third prong of Exemption 4.¹⁵⁴

In *9 to 5*, the Board of Governors of the Federal Reserve had withheld from a FOIA requester data prepared by the Boston Salary Group Survey on salaries, which the board was utilizing to recommend and approve salaries for Federal Reserve Bank employees. Although the district court had rejected the board's Exemption 4 claim because it did not meet the impairment prong of *National Parks*, the First Circuit looked to the "efficient operation" of government as justification for withholding information, reasoning that "it would do violence to the statutory purpose of Exemption 4 were the government to be disadvantaged by disclosing information which

^{149.} *Burroughs Corp. v. Brown*, 501 F. Supp. 375 (E.D. Va. 1980).
^{150.} *Racial-Milgo Gov't Sys. v. Small Bus. Admin.*, 559 F. Supp. 4 (D.D.C. 1981).

^{151.} *Lion Raisins, Inc.*, 354 F.3d at 1081; *Sharkey v. Food & Drug Admin.*, 250 F. App'x 284 (11th Cir. 2007).
^{152.} 9 to 5, 721 F.2d 1.

^{153.} 9 to 5, 721 F.2d, at 10.

^{154.} See, e.g., *Utah*, 256 F.3d at 969 n.1; *Nadler v. Fed. Deposit Ins. Corp.*, 92 F.3d 93, 96 n.2 (2d Cir. 1996).

serves a valuable purpose and is useful for the effective execution of its statutory responsibilities.¹⁵⁵

The D.C. Circuit accepted the First Circuit's third prong analysis in the first *Critical Mass* appellate decision.¹⁵⁶ On remand after that decision, the district court found that the release of information would hinder the future submission of information necessitating some form of litigation by the agency, along with accompanying expense and delay.¹⁵⁷ Although in its *en banc* review in *Critical Mass* the D.C. Circuit concluded that specific information should be released, the court still recognized the validity of the third prong, stating that in certain instances information could be withheld to protect a "governmental interest in administrative efficiency and effectiveness."¹⁵⁸

8.4.2.3 *Voluntarily submitted information:* *The Critical Mass decision*

In *Critical Mass Energy Project v. Nuclear Regulatory Commission*, an en banc D.C. Circuit reaffirmed *National Parks*, but "correct[ed] some misunderstandings as to its scope and application."¹⁵⁹ First, the *Critical Mass* court explained that the threshold determination to be made under Exemption 4 is whether the information was submitted to the government voluntarily or whether it was required to be submitted. If the information was given over to the government voluntarily, then the only question is whether it is the type of information that "for whatever reason, would customarily not be released to the public by the person from whom it was obtained."¹⁶⁰ This is a considerably easier test for the submitter to meet.¹⁶¹

also readily apparent that the information is of a kind that [the submitter] would not customarily share with its competitors or the general public.").

162. *Utah*, 256 F.3d at 969.

163. *Inner City Press/Cmty. on the Move*, 463 F.3d at 245 n.6; *Wickwire Gavin, P.C. v. U.S. Postal Serv.*, 356 F.3d 588, 597 (4th Cir. 2004); *Frazee v. U.S. Forest Serv.*, 97 F.3d 367, 372 (9th Cir. 1996); *Nadler*, 92 F.3d at 96 n.1; cf. *Utah*, 256 F.3d at 969.

155. *9 to 5*, 721 F.2d at 11.
156. *Critical Mass Energy Project v. Nuclear Regulatory Comm'n*, 830 F.2d 278, 286 (D.C. Cir. 1987) (citing *9 to 5*, 721 F.2d at 11).
157. *Critical Mass Energy Project v. Nuclear Regulatory Comm'n*, 731 F. Supp. 554, 557 (D.D.C. 1990).
158. *Critical Mass Energy Project v. Nuclear Regulatory Comm'n*, 975 F.2d 871, 879 (D.C. Cir. 1992).
159. *Id.* at 875.
160. *Id.* at 878.
161. See, e.g., *Cortez III v. Nat'l Aeronautics & Space Admin.*, 921 F. Supp. 8, 13 (D.D.C. 1996); *Gov't Accountability Project v. Nuclear Regulatory Comm'n*, 1993 WL 13033518, at *5 (D.D.C. July 2, 1993) (relying on company employee's affidavit to conclude that the fact that the company's "files are unavailable to the public is not to be doubted"); *Envl. Tech., Inc. v. Envtl. Prot. Agency*, 822 F. Supp. 1225, 1229 (E.D. Va. 1993) ("Applying the *Critical Mass* test to the facts stated above, it is clear that the information at issue was submitted voluntarily . . . It is
-
165. See, e.g., *Envl. Tech., Inc.*, 822 F. Supp. 1226.
166. *Id.*
167. *Id.*

issue, it must actually exercise that authority for a submission to be considered required (that is, not voluntary).¹⁶⁸ This test recognizes that "in certain circumstances an agency may decline to require information that it has the authority to compel and instead pursue voluntary compliance."¹⁶⁹

The fact that the submitter mistakenly believed that the agency possessed the authority to require the information does not make the submission involuntary. In *Center for Auto Safety v. National Highway Traffic Safety Administration*, the D.C. Circuit held that an agency's failure to comply with the requirements of the Paperwork Reduction Act (which requires Office of Management and Budget approval for all information collections¹⁷⁰) meant that the agency did not have the legal authority to require enforcement of the information collection, the submission should be treated as "voluntary," even if the agency asserted the authority and the submitter believed the assertion.¹⁷¹ In holding that the information at issue was voluntarily submitted, the court reasoned that "the agency essentially 'flashed its badge' to gain entrance to a private sphere when it had no legal authority to do so, and this misrepresentation must tip the balance of interests in favor of the private parties."¹⁷²

The issuance and enforcement of a subpoena will be one indication that when a business cooperated with agency officials and provided the agency all the information they requested prior to the issuance of any subpoenas or warrants so that the agency's investigation was neither delayed nor impeded, all the information provided was done so "voluntarily."¹⁷³ Another district court has held that a submission was voluntary even though the agency had the authority to issue a subpoena and had in fact done so.¹⁷⁴ In that case, the agency had not sought or obtained judicial enforcement of the subpoena. The court reasoned that subpoenaed parties may challenge subpoenas both

administratively and through objections to enforcement proceedings, which this business had not done.

The government takes a more narrow view of the circumstances in which information is submitted "voluntarily" for *Critical Mass* purposes. For example, the Department of Justice has taken the position that even if the underlying activity is of a voluntary nature—for example, bidding on a government contract—information submissions required as part of that activity are "required" for *Critical Mass* purposes.¹⁷⁵ Aspects of DOJ's position have found some support among the district courts.¹⁷⁶ But this acceptance has not been universal.¹⁷⁷ Moreover, this aspect of DOJ's 1993 *Critical Mass* guidance has been criticized by the D.C. Circuit, which found it "somewhat troubling that Justice, in 1993, instructed the agencies that they 'should' treat 'most' information given to the government as 'required,' without any serious effort analytically to distinguish voluntarily supplied information from that which is required within the meaning of *Critical Mass*.¹⁷⁸

8.4.3 Privileged business information

Information also falls within Exemption 4 if it is "commercial or financial information obtained from a person and *privileged*.¹⁷⁹ Thus, courts treat "privileged" and "confidential" information as separate and independent aspects of Exemption 4.¹⁸⁰ The "privileged" aspect of Exemption 4 is utilized considerably less than the "confidential" aspect.

175. Dep't of Justice, FOIA UPDATE, Spring 1993, available at <http://www.usdoj.gov/joip/foia-upd.htm>.

176. See, e.g., Pub. Citizen Health Research Grp. v. Food & Drug Admin., 997 F. Supp. 56 (D.D.C. 1998) (information required to be submitted as part of application for drug approvals deemed "required").

177. See, e.g., Envir. Tech., Inc., 822 F. Supp. 1226 (information submitted by EPA contractor deemed "voluntary").

178. McDonnell Douglas Corp. v. Nat'l Aeronautics & Space Admin., 180 F.3d 303, 306 (D.C. Cir. 1999).

179. 5 U.S.C. § 552(b)(4) (emphasis added).

180. Washington Post Co. v. Dep't of Health & Human Servs., 690 F.2d 252, 267 n.50 (D.C. Cir. 1982); see also Indian Law Res. Ctr. v. Dep't of the Interior, 477 F. Supp. 144, 146 (D.D.C. 1979) (stating that commercial or financial information can fall within Exemption 4 if "the withheld information is either confidential or privileged").

The traditional discovery privileges provide “rough analogies” for determining whether information is “privileged” under Exemption 4.¹⁸¹ As evidenced in the FOIA’s legislative history, Exemption 4 easily covers information falling within the attorney-client privilege.¹⁸² It also includes the work-product doctrine.¹⁸³ Other less commonly cited privileges, like the common interest privilege and the confidential report privilege, have likewise been applied by courts under Exemption 4.¹⁸⁴

8.5 PRIVILEGED INTERAGENCY OR INTRA-AGENCY MEMORANDA OR LETTERS

The FOIA’s Exemption 5 applies to “inter-agency or intra-agency memoranda or letters which would not be available by law to a party other than an agency in litigation with the agency.”¹⁸⁵ To satisfy Exemption 5, “a document must thus satisfy two conditions: its source must be a Government agency, and it must fall within the ambit of a privilege against discovery under judicial standards that would govern litigation against the agency that holds it.”¹⁸⁶

The vast majority of Exemption 5 disputes involve this second condition—whether the document would be shielded from discovery. This condition means that Exemption 5 protects from disclosure “those documents, and only those documents, normally privileged in the civil discovery context.”¹⁸⁷ The exemption “incorporates the privileges which the Government enjoys under the relevant statutory and case law in the pretrial discovery context.”¹⁸⁸ Thus, the issues that arise in the Exemption 5 context also fre-

181. *Washington Post Co.*, 690 F.2d at 267; *see also Washington Post Co. v. Dep’t of Health & Human Servs.*, 603 F. Supp. 235, 238 (D.D.C. 1985), *rev’d on other grounds*, 795 F.2d 205 (D.C. Cir. 1986).

182. *Id.* at 267 n.50; *see also Miller, Anderson, Nash, Yerke, & Wiener v. Dep’t of Energy*, 499 F. Supp. 767, 771 (D. Or. 1980).

183. *Indian Law Res. Ctr.*, 477 F. Supp. at 148.

184. *Hunton & Williams v. U.S. Dep’t of Justice*, 590 F.3d 272 (4th Cir. 2010); *Washington Post Co.*, 603 F. Supp. at 237–38, *rev’d on other grounds*, 795 F.2d 205 (D.C. Cir. 1986).

185. 5 U.S.C. § 552(b)(5); *see, e.g.*, *Wood v. FBI*, 432 F.3d 78, 83 (2d Cir. 2005).

186. *Dep’t of the Interior v. Klamath Water Users Protective Ass’n*, 532 U.S. 1, 8 (2001); *Elec. Frontier Found. v. Office of the Dir. of Nat’l Intelligence*, 639 F.3d 876, 889 (9th Cir. 2010).

187. *Nat’l Labor Relations Bd. v. Sears, Roebuck & Co.*, 421 U.S. 132, 149 (1975); *see also Dep’t of Justice v. Julian*, 486 U.S. 1, 11 (1988).

188. *Fed. Trade Comm’n v. Grolier, Inc.*, 462 U.S. 19, 26 (1983) (“The test under Exemption 5 is whether the documents would be ‘routinely’ or ‘normally’ disclosed upon a showing of relevance.”); *Renegotiation Bd. v. Grumman-Aircraft Eng’g Corp.*, 421 U.S. 168, 184 (1975); *see also Nadler v. Dep’t of Justice*, 898 F.2d 72, 72 (1990).

quently arise in the context of non-FOIA civil litigation with an agency, and vice versa.¹⁸⁹ The FOIA, however, does not expand or contract the scope of existing privileges or create new ones.¹⁹⁰

8.5.1 Interagency or intra-agency memoranda or letters

The threshold requirement under Exemption 5 is whether the record in question is an “interagency or intra-agency memorandum or letter.”¹⁹¹ This threshold requirement, though less often in dispute, is “no less important” than the requirement that the record fall within a recognized privilege.¹⁹² The requirement typically comes into play when the record at issue has been prepared by or shared with nonfederal entities or people outside the federal government.

The FOIA does not define the terms “interagency” and “intra-agency.” The term “agency,” however, is defined as “each authority of the Government of the United States”¹⁹³ and “includes any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the Government . . . or any independent regulatory agency.”¹⁹⁴ With this definition in mind, a strict or literal reading of the phrase “interagency or intra-agency” would mean that only documents generated by federal agency employees and shared only with other federal agency employees would qualify for Exemption 5 protection.¹⁹⁵ Several courts of appeals have eschewed such a strict reading and held that documents prepared by outside consultants engaged by an agency may qualify as inter- or intra-agency.¹⁹⁶

189. See section 9.3.2.

190. *Ass’n for Women in Science v. Califano*, 566 F.2d 339, 342 (D.C. Cir. 1977).

191. *Elec. Frontier Found.*, 639 F.3d at 890 (citing 5 U.S.C. § 552(b)(5)).

192. *Klamath Water Users*, 532 U.S. at 9.

193. 5 U.S.C. § 551(l).

194. 5 U.S.C. § 552(f).

195. *Dep’t of Justice v. Julian*, 486 U.S. 1, 18 n.1 (1988) (Scalia, J., dissenting).

196. *See, e.g.*, *Hoover v. Dep’t of the Interior*, 611 F.2d 1132, 1138 (5th Cir. 1980) (“We . . . hold that the appraisal report in the present case, although prepared by an outside expert, is an intra-agency memorandum within the meaning of Exemption 5 . . .”); *Lead Indus. Ass’n v. Occupational Safety & Health Admin.*, 610 F.2d 70, 83 (2d Cir. 1979) (“We note preliminarily that in our view, nothing turns on the point that the [documents] were prepared by outside consultants who had testified on behalf of the agency rather than agency staff.”).