

At direction of counsel

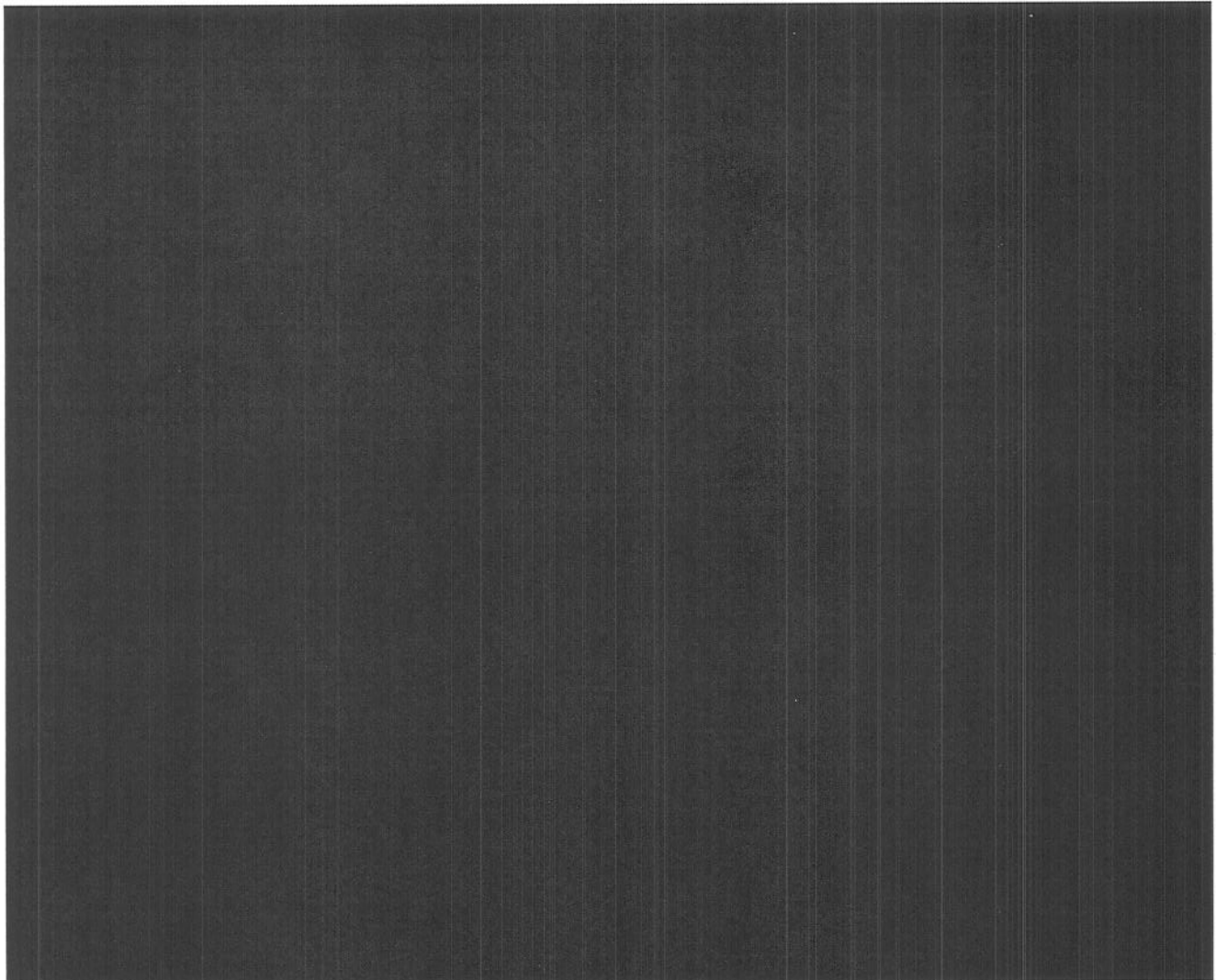
Subject: At direction of counsel

From: [REDACTED]@chicagopolice.org>

Date: 11/18/2014 1:08 PM

To: Roti, Nicholas J. <nicholas.roti@chicagopolice.org>, Carter, Eric M. <eric.carter@chicagopolice.org>, Kennedy, Christoph J. <christoph.kennedy@chicagopolice.org>, Washington, Eric T. <eric.washington@chicagopolice.org>, Dedore, Scott K. <scott.dedore@chicagopolice.org>, Sanchez, James R. <james.sanchez@chicagopolice.org>, [REDACTED]@chicagopolice.org>, Ryle, Michael K. <michael.ryle@chicagopolice.org>, Kilroy Jr, William A. <william.kilroyjr@chicagopolice.org>, O Shea, Daniel F. <daniel.oshea@chicagopolice.org>, Costa, Jack J. <jack.costa@chicagopolice.org>, Daly, Charles G. <charles.daly@chicagopolice.org>

In the pens that I do this is what is in the application the the judge signs. It addresses the use of a Digital Analyzer (stingray, trigger-fish)



From: Roti, Nicholas J.

Sent: Tuesday, November 18, 2014 12:48

To: Carter, Eric M.; Kennedy, Christoph J.; Washington, Eric T.; Dedore, Scott K.; Sanchez, James R.; [REDACTED]; Ryle, Michael K.; Kilroy Jr, William A.; O Shea, Daniel F.; Costa, Jack J.; Daly, Charles G.; [REDACTED]

ZIP 5, Row 6, REMAIL #4 - a 5045358889...

9/18/2015 9:17 AM

At direction of counsel

Subject: Article -

All,

Read the below article as it pertains to legal and operational issues we have been dealing with recently.

Tacoma police change how they seek permission to use cellphone tracker (WA)
http://www.thenewstribune.com/2014/11/15/3488642_tacoma-police-change-how-they.html?sp=/99/289/&rh=1<http://perf.memberclicks.net/message2/link/5507d3b1-016f-4bc7-a9dd-f1a3384415c4/4>

Nicholas J. Roti

Chief

Bureau of Organized Crime

Chicago Police Department

Email - Nicholas.roti@chicagopolice.org<<mailto:Nicholas.roti@chicagopolice.org>>

Office- (312) 745-6086

FW: Pen template

Subject: FW: Pen template

From: [REDACTED] <[REDACTED]@chicagopolice.org>

Date: 4/5/2012 10:29 AM

To: Lipsey, Michael E. <michael.lipsey@chicagopolice.org>, Brian cybrian
(Brian.Cyprian@ic.fbi.gov) <brian.cyprian@ic.fbi.gov>

From: [REDACTED]

Sent: Tuesday, November 29, 2011 1:47 PM

To: Jacobson, Greg J.

Subject: Pen template

[REDACTED]

you need anything call

Attachments:

_Exigent with tracking device template.doc

71.5 KB

tracking cell phone laws.pdf

105 KB

STATE OF ILLINOIS)

)

SS

COUNTY OF COOK)

IN THE CIRCUIT COURT OF COOK COUNTY
COUNTY DEPARTMENT, CRIMINAL DIVISION

IN THE MATTER OF THE)
APPLICATION OF THE PEOPLE)
OF THE STATE OF ILLINOIS) NO.: 2011 PR ??
FOR AN ORDER AUTHORIZING)
THE INSTALLATION AND USE)
OF A PEN REGISTER AND)
CALLER IDENTIFICATION TRAP)
AND TRACE DEVICE)

APPLICATION

NOW COMES Detective [REDACTED] a State Law enforcement or investigative officer employed by the Chicago Police Department, and hereby applies to this court pursuant to Sections 2703(d), 3122, 3123, 3124 and **3125** of Title 18 of the United States Code for an order authorizing the installation and use of a pen register and caller identification trap and trace device on cellular telephone number, [REDACTED] a cellular telephone, and for an order requiring the production of telecommunications records, including subscriber information for telephone numbers identified through the use of the pen register and trap and trace device, and including

In support of this application, applicant states as

follows:


In support of this application, applicant states as follows:

1. Applicant is a State investigative or law enforcement officer and therefore pursuant to Section 3122 (a) (2) of Title 18 of the United States Code may make application for an order authorizing the installation and use of a pen register and caller identification trap and trace device and **in support of the request for an order under Section 3125 (a) (1) (A) of Title 18 of the United States Code authorizing a Law Enforcement Officer to activate a Emergency pen register and caller identification trap and trace device** to a court of competent jurisdiction of this State.

2. Applicant certifies that Chicago Police Department and the Cook County State's Attorney's Office are conducting a criminal investigation of [REDACTED] and yet identified in connection with violations of [REDACTED]. It is believed that the subject of the investigation has in his possession a cellular telephone with the number [REDACTED] in furtherance of the subject offense, and that the information likely to be obtained from the installation and use of a pen register and caller identification trap and trace device is relevant to this ongoing criminal investigation in that it is believed the information will concern the aforementioned offense.

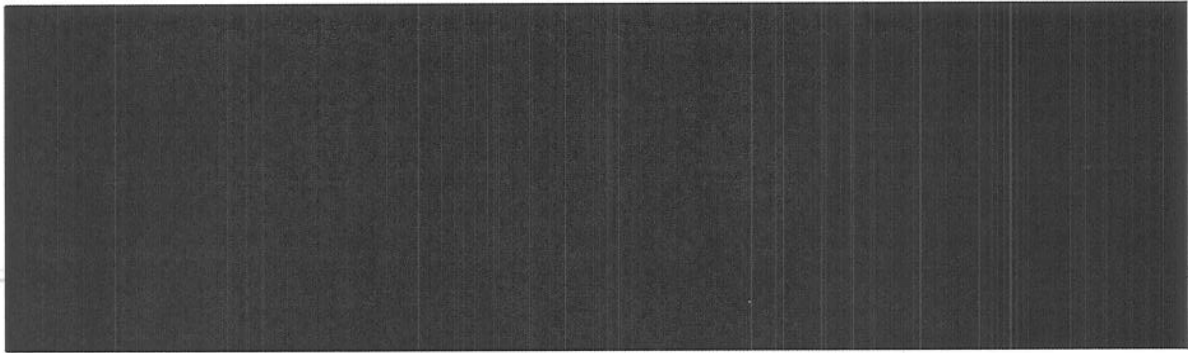
3. Applicant requests that the court issue an order authorizing the installation and use of a pen register to register numbers dialed or pulsed from cellular telephone number [REDACTED] a cellular telephone, as well as a caller identification trap and trace device to display numbers dialed or pulsed to cellular telephone number [REDACTED] a cellular telephone [REDACTED] and to record the date and time of such pulsing or dialing, and to record the length of time the telephone receiver in question is off the hook for incoming or outgoing calls for a period of 60 days and [REDACTED] and incoming and outgoing caller identifications beginning on the [REDACTED] to sixty days from the inception of this pen register. Applicant also requests that US CELLULAR furnish to the Chicago Police Department [REDACTED] for the cell phone number [REDACTED] a cellular telephone, for the duration of this order or until canceled by written notification by the Chicago Police Department.


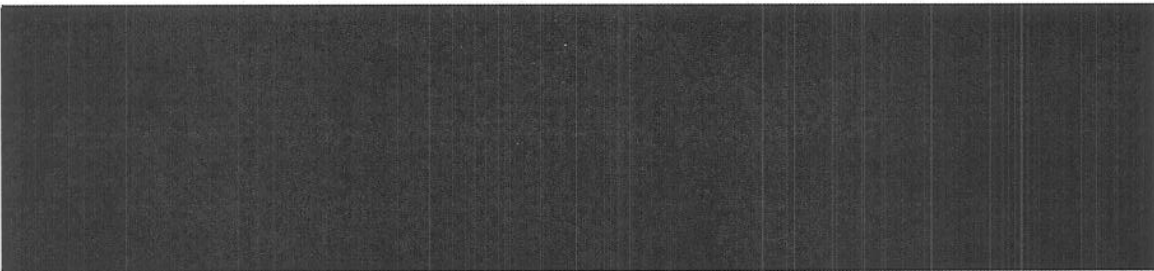
4. The applicant further requests that the order direct the Chicago Police Department to use technology reasonably available to it to restrict the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing so as not to include the contents of any wire or electronic communications.



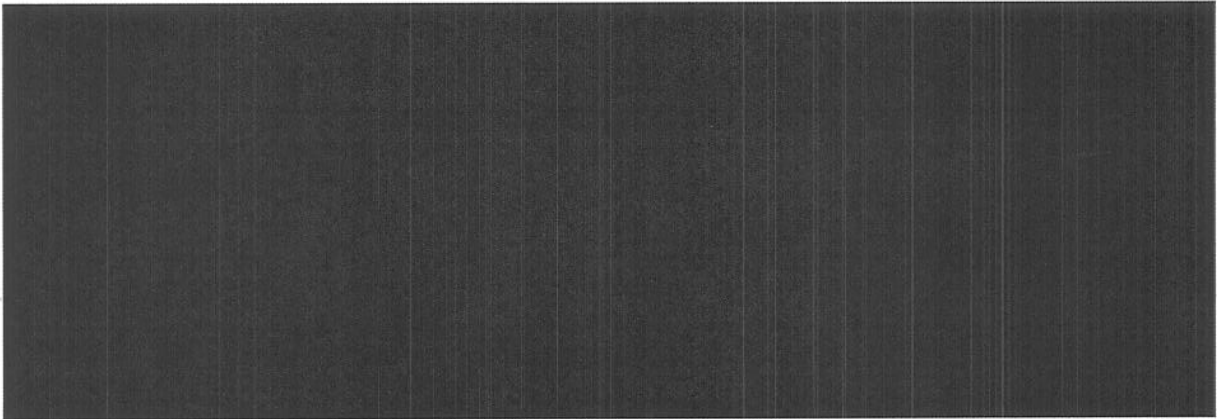
6. The applicant further requests that the order direct the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register and caller identification trap and trace device unobtrusively and with a minimum interference with normal telephone service. The wire communications service provider shall be compensated by the Chicago Police Department for reasonable expenses incurred in providing such facilities and technical assistance.

7. The applicant further requests, pursuant to Title 18, United States Code, Section 2703 (c) and (d), that **US CELLULAR** shall furnish agents of Chicago Police Department and the Cook County State's Attorney's Office with subscriber information concerning the telephone numbers dialed or pulsed from and to the subject telephone, including the name and address of the subscriber of record, electronic serial number, credit and billing information for the above-listed telephone number and the name and address of the subscribers of record for each outgoing call from and each incoming call to the above- listed telephone number.





10. The applicant further requests that in the event the pen register and caller identification trap and trace device discloses telephone numbers which belong to other telephone companies, namely to Ameritech, Ameritech Wireless, AT&T Wireless, Bell South, Bell South Wireless, Cingular, GTE, MCI, New Millennium Communications, Nextel Communications, Pacific Bell, Pacific Bell Wireless, Southwestern Bell Systems, Southwestern Bell Wireless, Southwestern Bell Mobile Systems, S.B.C. Ameritech, S.B.C. Wireless doing business as Cellular One, Sprint Communications, Sprint Spectrum, Sprint/ Nextel, T-Mobile, US Cellular, Verizon, Verizon Wireless, CellCo Partnership doing business as Verizon Wireless, Voice Stream Wireless, and all other providers of electronic communication service as defined in Title 18, United States Code, Section 2510(15), these companies are to furnish agents of Chicago Police Department and the Cook County State's Attorney's Office with subscriber information concerning the telephone numbers dialed or pulsed from or to the telephone which is the subject of the pen register, including the name and address of the subscriber of record for each outgoing call from and each incoming call to the above listed telephone number. It is provided that said companies are to be compensated there for at the prevailing rates.



[REDACTED]

[REDACTED]

13. In support of this request for a pen register and caller identification trap and trace device, pursuant to Title 18, United States Code, Section 3122, and in support of the request for an order under Title 18, United States Code, Section 2703, and **in support of the request for an order under Section 3125 (a) (1) (A) of Title 18 of the United States Code authorizing a Law Enforcement Officer to activate a Emergency pen register and caller identification trap and trace device** [REDACTED]

[REDACTED] directing the furnishing of the subscriber information, call detail [REDACTED] listed above, the applicant sets forward the following specific and articulated facts showing that the information likely to be obtained from the pen register and caller identification trap and trace device is relevant to an ongoing criminal investigation being conducted by the Chicago Police Department and showing that there are reasonable grounds to believe that the subscriber

information, call detail [REDACTED] or telephone numbers identified through the pen register and caller identification trap and trace device will be relevant and material to this ongoing criminal investigation:

AFFIDAVIT

I, [REDACTED] have been a Chicago Police Officer for

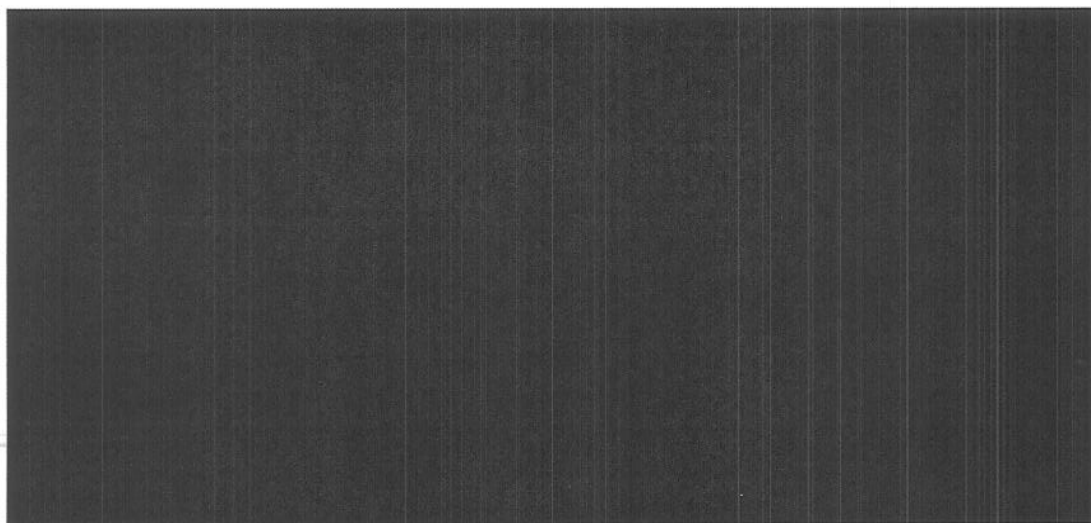
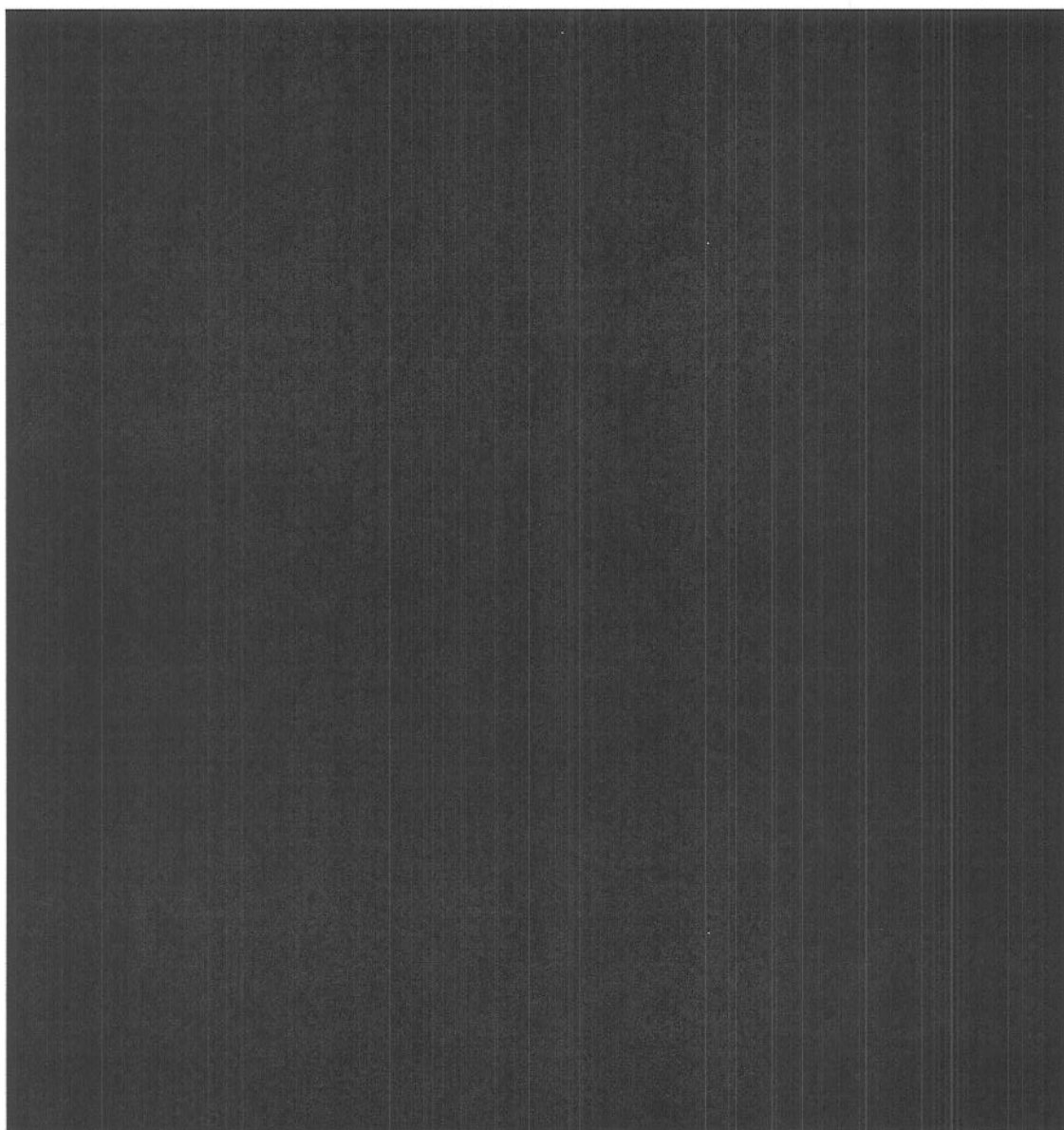
[REDACTED]

Your Affiant, [REDACTED] has been a duly sworn
Chicago Police Officer [REDACTED]

[REDACTED]

I, Police [REDACTED] along with detectives from [REDACTED]
[REDACTED] have been involved in the investigation of a subject named [REDACTED]
[REDACTED]

[REDACTED]



[REDACTED]

Based upon the foregoing information developed in this investigation, I, Police [REDACTED] request that an order for a pen-register be signed for the telephone number of [REDACTED]

Your affiant has contacted US CELLULAR and US CELLULAR confirmed the cell number is active.

Based on the above facts and information developed by this affiant and fellow detectives, this affiant believes that [REDACTED] [REDACTED] is in possession of this cellular telephone with the number [REDACTED] This Affiant, along with Fellow Detectives has exhausted all other investigatory tools as a means to locate the cellular telephone with the number [REDACTED] and [REDACTED] [REDACTED]. This information provided will assist in the apprehension and prosecution of the person responsible for the charge of [REDACTED] [REDACTED]

I, [REDACTED] having been duly sworn under oath, state that I have read the foregoing application and that it is true and correct to the best of my knowledge.

Applicant

Subscribed and sworn to before me this [REDACTED]

Judge of the Circuit Court of Cook County

Date:

Time:

STATE OF ILLINOIS)
) SS
COUNTY OF COOK)

IN THE CIRCUIT COURT OF COOK COUNTY
COUNTY DEPARTMENT, CRIMINAL DIVISION

IN THE MATTER OF)
APPLICATION OF THE PEOPLE)
OF THE STATE OF ILLINOIS)
FOR AN ORDER AUTHORIZING) NO.: 2011 PR
THE INSTALLATION AND USE)
OF A PEN REGISTER AND)
CALLER IDENTIFICATION TRAP)
AND TRACE DEVICE)

ORDER

THIS MATTER having come before the court pursuant to an application under Title 18 of the United States Code, Section 3122(a) (2) by [REDACTED] a State investigative or law enforcement officer, which application requests an order under Title 18, United States Code, Section 3123, authorizing the installation and use of a pen register and caller identification trap and trace device and **in support of the request for an order under Section 3125 (a) (1) (A) of Title 18 of the United States Code authorizing a Law Enforcement Officer to activate a Emergency pen register and caller identification trap and trace device on telephone number [REDACTED]** the court finds that the applicant has certified that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation into possible violation of [REDACTED] of the Illinois Compiled Statutes, by a unknown subject and that the records concerning electronic communication service listed below are also relevant to this ongoing criminal investigation,

IT APPEARING that the numbers dialed or pulsed from and to telephone number [REDACTED] being used by [REDACTED], and the records listed below are relevant to an ongoing criminal investigation of the specified offenses and that disclosure to any person of this investigation or of this application and order would seriously jeopardize the investigation,

1. IT IS ORDERED, pursuant to Title 18, United States Code, Section 3123, that agents of the Chicago Police Department may install and use a pen register to register numbers dialed or pulsed from cellular telephone number [REDACTED] and a caller identification trap and trap device to display numbers dialed or pulsed to cellular telephone number [REDACTED] to record the date and time of such pulsing or recordings, and to record the length of time the telephone receiver in question is off the hook for incoming or outgoing calls for a period of 60 days; and include previous cell site tower and incoming & outgoing phone records from the [REDACTED]

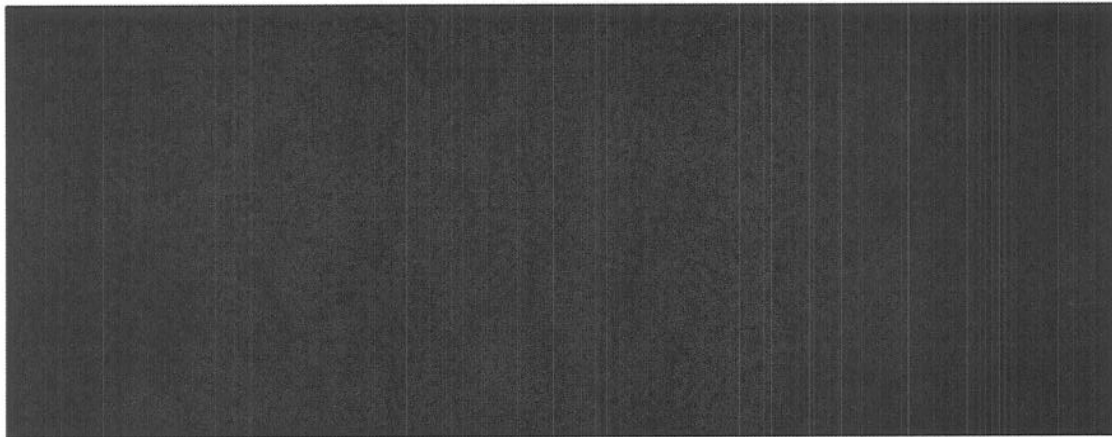
through the duration of this Pen Register, a [REDACTED]

3. IT IS FURTHER ORDERED that the Chicago Police Department use technology reasonably available to it to restrict the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing so as not to include the contents of any wire or electronic communications.

5. IT IS FURTHERED ORDERED, pursuant to Title 18, United States Code, section 3123 (b) (2), that **US CELLULAR**, shall furnish agents of the Chicago Police Department forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register and caller identification trap and trace

device unobtrusively and with minimum interference with the services that are accorded persons with respect to whom the installation and use is to take place; and IT IS FURTHER ORDERED, that **US CELLULAR** be compensated by the Chicago Police Department for reasonable expenses incurred in providing this information, these facilities, and this technical assistance; and

6. IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 2703(c) and (d), that **US CELLULAR** shall furnish agents of the Chicago Police Department and the Cook County State's Attorney's Office with subscriber information concerning the cellular telephone numbers dialed or pulsed from and to the subject telephone, including subscriber names and addresses, electronic serial number (ESN) and credit and billing information for the subject telephone and for telephone numbers dialed or pulsed from and to the subject telephone.

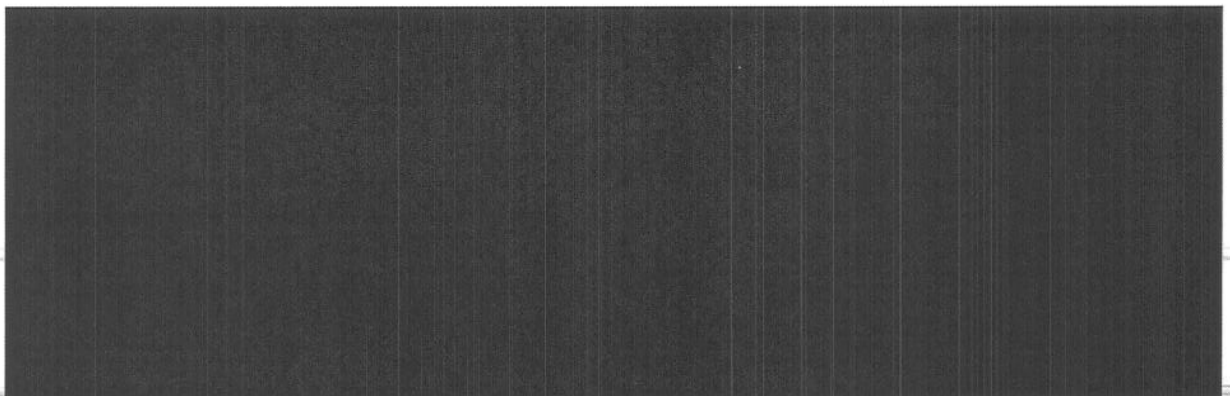


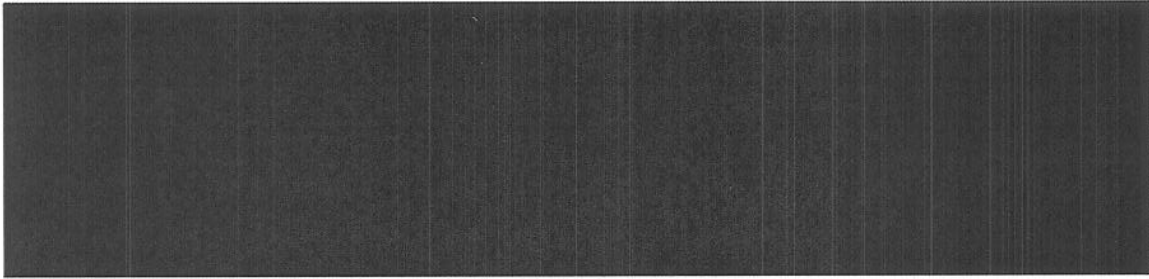
9. IT IS FURTHER ORDERED that in the event the pen register and caller identification trap and trace device discloses telephone numbers which belong to other telephone companies, namely to Ameritech, Ameritech Wireless, AT&T Wireless, Bell South, Bell South Wireless, Cingular, GTE, MCI, New Millennium Communications, Nextel Communications, Pacific Bell, Pacific Bell Wireless, Southwestern Bell Systems, Southwestern Bell Wireless, Southwestern Bell Mobile Systems, S.B.C. Ameritech,

S.B.C. Wireless doing business as Cellular One, Sprint Communications, Sprint Spectrum, T-Mobile, US Cellular, Verizon, Verizon Wireless, CellCo Partnership doing business as Verizon Wireless, Voice Stream Wireless, or any other providers of electronic communication service as defined in Title 18, United States Code, Section 2510(15), these companies are to furnish agents of the Chicago Police Department and the Cook County State's Attorney's Office with subscriber information concerning the telephone numbers dialed or pulsed from or to the telephone which is the subject of the pen register, including the name and address of the subscriber of record for each outgoing call from and each incoming call to the above listed telephone number. It is provided that said companies are to be compensated there for at the prevailing rates.



11. IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, section 3123 (d), that this order and the application be sealed until otherwise ordered by the court.





Judge of the Circuit Court of Cook County

Date:

Time:

STATE OF ILLINOIS)

(

SS

COUNTY OF COOK)

IN THE CIRCUIT COURT OF COOK COUNTY
COUNTY DEPARTMENT, CRIMINAL DIVISION

IN THE MATTER OF THE)
APPLICATION OF THE PEOPLE)
OF THE STATE OF ILLINOIS)
FOR AN ORDER AUTHORIZING)
THE INSTALLATION AND USE)
OF A PEN REGISTER AND)
CALLER IDENTIFICATION TRAP))
AND TRACE DEVICE)

NO.:

IMPOUNDING ORDER

THIS MATTER having come before the court pursuant to an application under Title 18 of the United States Code, Section 3122(a) (2) and under Title 18 of the United States Code, Section 3125 (a) (1) (A), and the court having issued the said order;

IT IS HEREBY FURTHER ORDERED that the original application and order, which I have placed in an envelope and signed and sealed, are to be impounded and held in the custody of the Clerk of the Circuit Court until otherwise ordered by the court.

Judge of the Circuit Court of Cook County

Date:

Time:

Received by:

Clerk of the Circuit Court

Date:

Time:

WARRANTLESS LOCATION TRACKING

IAN JAMES SAMUEL*

The ubiquity of cell phones has transformed police investigations. Tracking a suspect's movements by following her phone is now a common but largely unnoticed surveillance technique. It is useful, no doubt, precisely because it is so revealing; it also raises significant privacy concerns. In this Note, I consider what the procedural requirements for cell phone tracking should be by examining the relevant statutory and constitutional law. Ultimately, the best standard is probable cause; only an ordinary warrant can satisfy the text of the statutes and the mandates of the Constitution.

INTRODUCTION

Technological advances often result in new police investigation techniques. Some such developments, like heat detection, prove to be legally significant as well as professionally useful, and find their way into Supreme Court opinions.¹ Others, like forensic crime scene analysis, simply become routine parts of the ordinary police toolkit. Cell phones are emerging as an important but little-noticed investigative tool. In particular, the ability to track a phone's location has proven incredibly useful to the police, even as the legal status of such tracking has grown quite murky.

Tracking a suspect's precise movements may shatter a claimed alibi: In Scott Peterson's murder trial, for example, Peterson's cell phone records were introduced to establish his whereabouts on the morning of his wife's murder, belying his version of the events of that morning.² Retrospective analysis of cell phone records, however, is just the beginning. Real-time monitoring is even more powerful. When a Greek magnate was kidnapped by criminals who often changed locations to avoid the police, detectives monitored cell phone

* Copyright © 2008 by Ian James Samuel, J.D., 2008, New York University School of Law. Thanks to Samuel Issacharoff, Barry Friedman, Noah Feldman, Paul Monteleoni, Antoine McNamara, Benjamin Yaster, and Erik Paulsen for their help, and extraordinary thanks to Caroline Mello for being a constant source of patience and smart ideas.

¹ See, e.g., *Kyllo v. United States*, 533 U.S. 27, 40 (2001) (holding use of thermal imaging device aimed at private home from public street constitutes "search" within meaning of Fourth Amendment).

² Diana Walsh & Stacy Finz, *The Peterson Trial; Defendant Lied Often, Recorded Calls Show; Supporters Misled About Whereabouts*, S.F. CHRON., Aug. 26, 2004, at B1, available at <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2004/08/26/BAG458EJ3S1.DTL>.

records and were able to locate the victim.³ The kidnappers' phones were, in effect, converted into very accurate tracking devices, without the police needing physical access to them.

This technique isn't limited to investigating high profile cases like Peterson's or thwarting the kidnapping of foreign dignitaries. Cell phone tracking is used to solve more mundane crimes, such as car thefts never reported outside the local papers.⁴ It is even available to private citizens who want to monitor their children or spouses.⁵

Given the power of this technique, it's no surprise that its use has become routine.⁶ A common step in police investigations today is to secure a court order tracking the movements of a suspect or anyone else whose location the police believe useful. The flip side of this powerful tool, though, is how revealing and intrusive it is. Few people would be comfortable being followed by a police officer all day, even if they did nothing illegal or even interesting. Justice Brandeis once invoked the "right to be let alone,"⁷ and undetectable location tracking pressures the *alone* part: No one is "let alone" if the police may, without notice or probable cause, find out everywhere they go for a day or a month.

This tension is a familiar one in American criminal law: The usefulness of an investigative tool is always roughly proportional to its intrusiveness. Out of that simple tension grows a major portion of criminal procedure. Today, the federal district courts have divided on the proper procedural requirements for cell phone tracking,⁸ and no

³ Laurie Thomas Lee, *Can Police Track Your Wireless Calls? Call Location Information and Privacy Law*, 21 CARDOZO ARTS & ENT. L.J. 381, 381 (2003) (discussing kidnapping of Greek magnate).

⁴ See, e.g., *Girl, 5, Found Safe as Man Steals Car*, ROCKY MTN. NEWS (Colo.), Apr. 22, 2004, at 18A (reporting use of cell phone to locate car stolen with child inside).

⁵ Many such services are available. For a representative example, consider AccuTracking, which bills itself as the "[t]racking [s]ervice for [e]veryone." AccuTracking, <http://www.accutracking.com> (last visited Mar. 8, 2008).

⁶ See *In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info. (Orenstein Opinion II)*, 396 F. Supp. 2d 294, 318 n.21 (E.D.N.Y. 2005) (referring to cell phone tracking as "routine" technique for which judicial authorization requests have been drafted on "forms that have been in use for years").

⁷ Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

⁸ Compare *In re Application of the United States for an Order Authorizing the Disclosure of Prospective Cell Site Info. (Adelman Opinion)*, No. 06-MISC-004, 2006 WL 2871743, at *1, *7 (E.D. Wis. Oct. 6, 2006) (requiring probable cause and warrant for such tracking), and *In re Application of the United States for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device; (2) Authorizing the Release of Subscriber & Other Info.; & (3) Authorizing the Disclosure of Location-Based Servs. (Lee Opinion)*, Nos. 1:06-MC-6, 1:06-MC-7, 2006 WL 1876847, at *1, *5 (N.D. Ind. July 5, 2006) (same), with *In re Application of the United States for an Order for Prospective Cell*

court of appeals has yet addressed the issue. The magistrate judges who actually issue the orders have been similarly divided.⁹

This Note argues that before police may track a cell phone, they ought to be required to obtain an ordinary warrant founded on probable cause. After a brief explanation of the technical and legal mechanics of tracking in Part I, I turn to the relevant statutory law in Part II. All of the court decisions in this area thus far have relied exclusively on the electronic surveillance statutes.

The deep disagreement about the meaning of those statutes, however, makes it worthwhile to analyze what the Constitution has to say about the matter. In Part III, I argue that warrantless location tracking raises serious and difficult questions of constitutional law. For that reason, I invoke the statutory canon of “constitutional doubt” and argue that the ambiguous statutes should be read in a way that will not require those difficult constitutional questions to be confronted. Because the doubts are grounded in the Fourth Amendment, the easiest way to avoid these hard questions is to read the statutes to require a warrant, founded on probable cause, to track a person’s cell phone. In making this move, I part company with other judges and commentators who have written on the topic and who generally have focused entirely on the simple “yes/no” question of constitutionality or statutory legality, without much consideration of how the two interact.

Site Location Info. on a Certain Cellular Tel. (*Kaplan Opinion*), 460 F. Supp. 2d 448, 450 (S.D.N.Y. 2006) (permitting such searches absent probable cause), and *In re* Application 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. (*Rosenthal Opinion*), 433 F. Supp. 2d 804, 805–06 (S.D. Tex. 2006) (same).

⁹ A complete list of published magistrate opinions on this topic would exhaust the space available for discussion of them; only a representative few need be considered. See, e.g., *In re* Application of the United States for an Order Authorizing (1) Installation & Use of a Pen Register & Trap & Trace Device or Process, (2) Access to Customer Records, & (3) Cell Phone Tracking (*Smith Opinion*), 441 F. Supp. 2d 816, 836–37 (S.D. Tex. 2006) (concluding that less than probable cause showing for cell phone location tracking might violate Fourth Amendment); *In re* Application of the United States for an Order for Disclosure of Telecomms. Records & Authorizing the Use of a Pen Register & Trap & Trace (*Gorenstein Opinion*), 405 F. Supp. 2d 435, 448–49 (S.D.N.Y. 2005) (allowing such tracking without probable cause); *Orenstein Opinion II*, 396 F. Supp. 2d at 295, 327 (E.D.N.Y. 2005) (requiring probable cause and warrant for such tracking); *In re* Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info. 384 F. Supp. 2d 562, 564 (E.D.N.Y. 2005) (same, but on different grounds). For an overview of the case law available on cell phone location tracking, see Deborah F. Buckman, Annotation, *Allowable Use of Federal Pen Register and Trap and Trace Device to Trace Cell Phones and Internet Use*, 15 A.L.R. FED. 2d 537, 547–61 (2007) (collecting published cases).

I

HOW CELL PHONE TRACKING WORKS

The technical details of cell phone tracking are not too complex, and are worth understanding to have a good grasp of the issue. This Part describes those details, gives a brief overview of the legal process currently used to secure the tracking orders, and describes how the issue was first considered by magistrate judges.

A cell phone is “a radio—an extremely sophisticated radio, but a radio nonetheless.”¹⁰ To send and receive calls, text messages, or e-mail, cell phones communicate with radio towers, known as cell towers.¹¹ The cell towers are distributed throughout a coverage area; cell phone users are often in range of more than one.¹²

The quality of the signal to and from these towers is what’s measured by the characteristic “bars” on cell phones. As users of cell phones know, the signal quality bars are present whether or not a call is in progress, as the phones remain in regular contact with nearby cell towers.¹³ By comparing the phone signal’s time and angle of arrival at several cell towers, the location of the broadcast can be figured out.¹⁴ This is known as radio triangulation.¹⁵ The more densely placed the phone towers, the more accurate the location data will be. This location information, originating as it does from the physical cell towers, is often called “cell site information.”¹⁶ The upshot is that “[i]t is now possible to locate a person using a cellular phone down to a range of a few meters, anywhere on the globe.”¹⁷

The technical possibility of tracking cell phone location, by itself, would not be much of an investigative tool. The owners of the cell towers (usually phone companies), not the police, possess the relevant

¹⁰ Julia Layton et al., *How Cell Phones Work*, HOW STUFF WORKS, <http://electronics.howstuffworks.com/cell-phone.htm/printable> (last visited Mar. 8, 2008).

¹¹ *Id.*

¹² *Id.*

¹³ See *Kaplan Opinion*, 460 F. Supp. 2d at 450 (describing every cell phone as “periodically transmit[ting] a unique identification number to register its presence and location in the network”).

¹⁴ For example, Apple’s iPhone relies in part on this technique to show its user her location on the map software. See John Markoff, *Jobs Returns to His Mac Roots with a Thin, Ultralight Laptop*, N.Y. TIMES, Jan. 16, 2008, at C4 (discussing map feature’s introduction at 2008 Macworld Expo).

¹⁵ *Kaplan Opinion*, 460 F. Supp. 2d at 451 & n.3; see also JOHN CLAYTON TRACY, PLANE SURVEYING: A TEXT-BOOK AND POCKET MANUAL 191–200 (1906) (describing triangulation in another context).

¹⁶ See, e.g., *Kaplan Opinion*, 460 F. Supp. 2d at 451 (referring to location information as “cell site” data).

¹⁷ Marshall Brain & Jeff Tyson, *How Buying a Cell Phone Works*, HOW STUFF WORKS, <http://electronics.howstuffworks.com/cell-phone-buying6.htm> (last accessed Mar. 8, 2008).

information. To get the location data, police need a legal mechanism to compel its disclosure. The Pen Register Act provides this mechanism.¹⁸ It allows police to apply for a “pen register,” which initially referred to a mechanical device designed to record numbers dialed.¹⁹ Today, a pen register is defined much more broadly.²⁰ If the statutory requirements are fulfilled,²¹ a judge orders the phone company to disclose the information.²²

When new technology emerges, the first applications of the law try to build on old paradigms, generally without contemplating whether the new tools challenge the implicit assumptions of the past. So it was during most of this particular tracking technique’s history; police tracking requests were approved wholly without comment by the magistrate judges who actually issued the orders.²³ Justice Department attorneys assured the magistrates of the legality of their requests, and the magistrates acquiesced without opinion.²⁴ The failure to issue any opinions on this topic has many possible explanations, but the simplest is probably right: Most likely, the magistrate judges trusted the claims of U.S. Attorneys about what the law required on this subject, and since these proceedings are *ex parte*, no one else pressed the issue.

Judge Orenstein upset the apple cart in an August 2005 opinion that admitted to granting many of these orders in the past,²⁵ but simultaneously concluded that such orders were illegal without probable cause.²⁶ It was the first opinion to raise the issue, and it came as an enormous shock to the lawyers involved who had come to regard such

¹⁸ 18 U.S.C. §§ 3121–3127 (2000).

¹⁹ *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 161 n.1 (1977).

²⁰ See *In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info. (Orenstein Opinion II)*, 396 F. Supp. 2d 294, 318 (E.D.N.Y. 2005) (noting Patriot Act’s expansion of pen/trap definitions).

²¹ These requirements are set out generally in 18 U.S.C. § 3123(b) (2000). What exactly the statutory requirements are for this type of pen register—particularly, what evidentiary showing must be made—is the topic of this Note.

²² 18 U.S.C. § 3127(3) (2000).

²³ See *In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info. (Orenstein Opinion I)*, 384 F. Supp. 2d 562, 566 (E.D.N.Y. 2005) (describing absence of law on topic despite magistrates in other jurisdictions confronting issue).

²⁴ *Id.*

²⁵ *Id.* (citing *Henslee v. Union Planters Nat’l Bank & Trust Co.*, 335 U.S. 595, 600 (1949) (Frankfurter, J., dissenting) (“Wisdom too often never comes, and so one ought not to reject it merely because it comes late.”)).

²⁶ *Id.* at 564 (cell site data “is *not* information that the government may lawfully obtain absent a showing of probable cause”).

requests as routine.²⁷ The opinion touched off a minor firestorm within the broader community of American magistrate judges. Very soon after Judge Orenstein's initial opinion, Judge Smith of the Southern District of Texas issued an opinion on the topic, grounded in different reasons but reaching the same conclusion.²⁸ Judge Orenstein then issued a much longer opinion on a motion for reconsideration, citing Judge Smith extensively.²⁹ Other magistrates soon followed suit.³⁰

It looked for a moment as if the issue was going to be settled by consensus, but that was not to be. Magistrate judges soon published opinions reaching the opposite conclusion and affirming the legality of these orders, the first of whom was Judge Gorenstein of the Southern District of New York.³¹ Other judges followed Judge Gorenstein's lead, and it rapidly became clear that appellate resolution of this issue was unlikely, since the Department of Justice (DOJ) has not sought district court review in most cases, and has never sought appellate court review.³² When the DOJ loses, the matter ends; when the DOJ wins, there is no one else in court to appeal.

As a result, there is a live statutory disagreement amongst judges regarding an enormously important tool used in police investigations, a disagreement whose contours cannot even be fully mapped by a close study of the published opinions. It's likely that some judges continue to issue these orders without comment, either because they are unaware of the disagreement regarding their legality or because,

²⁷ Cf. *In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info. (Orenstein Opinion II)*, 396 F. Supp. 2d 294, 318 n.21 (E.D.N.Y. 2005) (referring to this technique as "routine," and having been submitted on "forms that have been in use for years").

²⁸ See *In re Application of the United States for an Order Authorizing (1) Installation & Use of a Pen Register & Trap & Trace Device or Process, (2) Access to Customer Records, & (3) Cell Phone Tracking (Smith Opinion)*, 441 F. Supp. 2d 816, 836–37 (S.D. Tex. 2006).

²⁹ See *Orenstein Opinion II*, 396 F. Supp. 2d at 294.

³⁰ See *supra* note 8.

³¹ *In re Application of the United States for an Order for Disclosure of Telecomms. Records & Authorizing the Use of a Pen Register & Trap & Trace (Gorenstein Opinion)*, 405 F. Supp. 2d 435 (S.D.N.Y. 2005). This prompted *amicus curiae* the Electronic Frontier Foundation to remark on its website: "What a difference a G makes." Electronic Frontier Foundation: DeepLinks, Bad Ruling on Cell Phone Tracking, <http://www.eff.org/deep-links/2005/12/bad-ruling-cell-phone-tracking-what-difference-g-makes> (last visited Mar. 8, 2008).

³² The magistrate judges have encouraged the government to seek review by a court of appeals. See, e.g., *In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info. (Orenstein Opinion I)*, 384 F. Supp. 2d 562, 566 (E.D.N.Y. 2005) (requesting appellate resolution of matter).

after considering the arguments on all sides, they understand the statutes to come down on one side or the other.

The open legal question concerns the evidentiary standard that must be met to justify using a pen register to track a phone's location rather than just record dialed numbers. Whether the police must show probable cause, something less, or perhaps even something more, is the debate to which I now turn.

II

STATUTORY DISAGREEMENT

Despite its enormous value to the police, evident ubiquity, and the potential consequences for individual privacy, the legality of cell phone tracking was not addressed in a published opinion until 2005.³³ The courts that have addressed this issue since have focused on the electronic surveillance statutes, which is where this Part begins. These statutes are strangely written, however, and ambiguous about the key question: what law enforcement must show to a neutral magistrate to track a person's location using her cell phone. This Part argues that the ambiguity cannot be resolved by reference to the text alone. In Part III, the ambiguity will be resolved by resort to other means.

A. *The Content/Envelope Distinction*

The statutory disagreement centers on only a few statutory provisions, the text of which will be explored shortly. First, however, it is helpful to understand why pen registers are treated differently from wiretaps, a difference in treatment that runs through all of the statutory and constitutional law on this topic.

The level of process required for different types of surveillance falls along a continuum.³⁴ At one end is a total absence of any legal process requirements—the police can get certain information without any process or order from a judge. (Consider, for example, the information an officer learns by simply walking around the local neighborhood.) At the other end is the “super-warrant” of Title III,³⁵ the federal wiretap statute, which requires probable cause, restricts who may request a wiretap, and requires that alternatives to wiretaps be unsuccessfully tried or too dangerous to attempt.³⁶ In between are

³³ See *id.* (stating that Judge Orenstein's research “failed to reveal any federal case law directly on point”).

³⁴ On the continuum of surveillance process, see Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 Nw. U. L. REV. 607, 620–21 (2003), available at <http://ssrn.com/abstract=317501>.

³⁵ 18 U.S.C. §§ 2510–2522 (2000).

³⁶ § 2518.

several intermediate levels of process commonly found in surveillance law, as illustrated in the chart below.³⁷

Evidentiary Burden	Requirement	Example
<i>Nothing</i>	Nothing.	Walking the Beat
<i>Relevance</i>	Certify to judge that the information is “relevant.”	Pen Register ³⁸
<i>Articulable Facts</i>	Offer specific facts that give reasonable grounds to believe information is relevant and material.	Stored Communications ³⁹
<i>Probable Cause</i>	Show likelihood that evidence of a crime will be revealed in the location to be searched.	Search of a Home ⁴⁰
<i>Super-Warrant</i>	Show probable cause and comply with other procedures.	Wiretap ⁴¹

Where a surveillance technique falls on this spectrum often depends on what kind of information it discloses. Every communications network “features two types of information: the contents of communications, and the addressing and routing information that the networks use to deliver the contents of communications.”⁴² The former is “content information,” and tends to be associated with high procedural requirements. The latter is “envelope information,” and tends to be associated with the opposite.⁴³

The federal wiretap statute,⁴⁴ for example, concerns itself explicitly with endeavors to “intercept . . . any wire, oral, or electronic communication,”⁴⁵ and prohibits the use of those communications as evidence except as the statute provides.⁴⁶ The statute defines “intercept” as “acquisition of the contents of any wire, electronic, or oral communication,”⁴⁷ and “contents” as “any information concerning the substance, purport, or meaning of that communication.”⁴⁸ The super-warrant requirement is triggered by a wiretap’s interception of content.⁴⁹

³⁷ This chart owes much to Kerr, *supra* note 33, at 620–21.

³⁸ 18 U.S.C. § 3123(a).

³⁹ 18 U.S.C. § 2703(d).

⁴⁰ FED. R. CRIM. P. 41(d)(1).

⁴¹ 18 U.S.C. § 2518.

⁴² Kerr, *supra* note 33, at 611.

⁴³ *Id.*

⁴⁴ 18 U.S.C. §§ 2510–2522 (2000).

⁴⁵ § 2511(1)(a).

⁴⁶ § 2515.

⁴⁷ § 2510(4).

⁴⁸ § 2510(8).

⁴⁹ § 2518 (describing super-warrant requirements for intercepting wire, oral, and electronic communications).

By contrast, an ordinary pen register discloses nothing about a phone call other than that it occurred and what the phone numbers involved were. A pen register is defined 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.”⁵⁰ This is envelope information, and is governed by low procedural requirements.⁵¹

What makes location tracking interesting is that it does not fit neatly along the spectrum between interception of content and envelope information. In a literal sense, the location of a call is “signaling information,” and might properly be regarded as “envelope information.” After all, an objector might state, doesn’t the post office stamp the time and location on envelopes when letters are mailed?⁵² And didn’t the “classic” pen register, which recorded only phone numbers, disclose the location of the call—the house to which the phone line was attached? Yes.

The exact details of one’s movements, however, seem intuitively more revealing than the zip code on a birthday card. Location tracking of one’s cell phone can, for example, reveal visits to places one might wish to keep private: the local gay bar, the abortion clinic in the next city over, or union headquarters. By contrast, the post office’s envelope information reveals only a visit to the post office. What is essential is not whether the information is “content” or “envelope,” but rather what the information reveals; the old “content/envelope” line is probative on that question, but not determinative. Bolstering this conclusion are statutes, discussed below, that explicitly place limits (albeit unclear in their substance) on pen registers that might disclose location information.

It’s worth analyzing the statutes with a clear understanding that the “content/envelope” distinction upon which they rely doesn’t translate easily to this new era. There’s no reason that we should anticipate finding all information easily divided into “content” and “envelope”; our data is no longer wrapped in paper and transmitted by Pony Express. It’s natural to expect that the old assumptions about how information is packaged will fall away as technology advances.

⁵⁰ 18 U.S.C. § 3127(3) (2000).

⁵¹ See 18 U.S.C. § 3123(a) (requiring law enforcement to certify that pen register information “likely to be obtained by such installation and use is relevant to an ongoing criminal investigation”).

⁵² I am grateful to Professor Kerr for raising this objection.

B. The Ambiguous Statutory Text

Against that background, let's consider the statutory provisions at the core of the dispute. The question is not "*whether* the government can obtain cell site information," but rather what "*standard* it must meet before a court will authorize such disclosure."⁵³ The Pen Register Act sets out a legal process for obtaining pen register orders,⁵⁴ which include cell phone tracking orders.⁵⁵ A separate statute, the Communications Assistance for Law Enforcement Act (CALEA), says that no order issued "solely pursuant" to the Pen Register Act may disclose the physical location of the subscriber.⁵⁶ This places a limit on the use of the Pen Register Act to track cell phones, certainly. The statutory disagreement is: If location information cannot be gotten "solely pursuant" to the Pen Register Act, what combination of statutory authority is acceptable? That is, the Pen Register Act plus what other law equals authority to track cell phones?

This is a very odd question of statutory interpretation. Statutes do not often require themselves to be combined, chimera-like, with other statutes to achieve their effects; it is even rarer that one statute should require another statute to be combined with an *unspecified* third statute to do something. In fact, the phrase "solely pursuant" is used in this way only once in the entire United States Code.⁵⁷

Analytically, CALEA could mean one of three things. First, the Pen Register Act may never authorize an order that would disclose location information. Second, the Pen Register Act in combination with *any* other law may authorize such an order. Third, the

⁵³ *In re* Application of the United States for an Order Authorizing the Installation & Use of a Pen Register Device, a Trap & Trace Device, & for Geographic Location Info. (*McGiverin Opinion*), 497 F. Supp. 2d 301, 304 (D.P.R. 2007) (quoting *In re* Application of the United States for an Order Authorizing the Disclosure of Prospective Cell Site Info. (*Adelman Opinion*), No. 06-MISC-004, 2006 WL 2871743, at *1 (E.D. Wis. Oct. 6, 2006)).

⁵⁴ The Pen Register Act states that "no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title." 18 U.S.C. § 3121(a).

⁵⁵ See, e.g., *In re* Application of the United States for an Order for Disclosure of Telecomms. Records & Authorizing the Use of a Pen Register & Trap & Trace (*Gorenstein Opinion*), 405 F. Supp. 2d 435, 438–39 (S.D.N.Y. 2005) (noting that under Pen Register Act, "the term 'signaling information' includes information on the location of cell site towers used by a cellular telephone").

⁵⁶ 47 U.S.C. § 1002(a)(2) (2000). The provision states: "[W]ith regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices . . . 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)." *Id.*

⁵⁷ *Gorenstein Opinion*, 405 F. Supp. 2d at 442.

Pen Register Act in combination with some laws (but not others) may authorize such an order.

The first possibility, that no location tracking order may ever issue pursuant to the Pen Register Act, is foreclosed by the text of CALEA. Though “solely pursuant” is not a phrase that receives much usage in the United States Code, the rule against surplusage suggests that some statutory combination must authorize a location tracking order.⁵⁸ This alternative “requires reading the word ‘solely’ out of the statute entirely.”⁵⁹ If Congress intended to ban the use of pen registers for location tracking, it simply could have said “pursuant.”

The second possibility, that CALEA simply requires any other statute to be used in combination with the Pen Register Act, has a certain sort of textual logic. After all, CALEA’s only prohibition is against issuing a certain type of order “solely” pursuant to the Pen Register Act. If the request to the judge relies on any other authority at all, then the order is not being issued “solely” pursuant to the Pen Register Act, and CALEA isn’t offended.

The other authority relied on, of course, would have to be germane to the information sought, and whatever process it imposed would have to be followed. Otherwise CALEA’s requirement would be nonsense. How could one combine the Pen Register Act and the tax code, for example? Once these constraints are admitted, though, “any law at all in combination with the Pen Register Act” starts to look more like “certain laws but not others.” This is the third choice for interpreting CALEA’s prohibition, and has come to be known as the “hybrid theory.”⁶⁰

Even this third understanding, though the best alternative, is strange. If another law is germane to the information sought, and its procedural requirements are satisfied, then what “work” is the Pen Register Act doing? Why not simply seek the order pursuant solely to that other statute?

The likely answer is that cell phone tracking requires the use of a pen register, and the Pen Register Act is the only procedural means

⁵⁸ The rule against surplusage is a canon of statutory construction that discourages interpretations of a statute that render some words meaningless. See, e.g., *United States v. Menasche*, 348 U.S. 528, 538–39 (1955).

⁵⁹ *In re Application of the United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel. (Kaplan Opinion)*, 460 F. Supp. 2d 448, 458 (S.D.N.Y. 2006).

⁶⁰ See *In re Application of the United States for an Order Authorizing the Installation & Use of a Pen Register Device, a Trap & Trace Device, & for Geographic Location Info. (McGiverin Opinion)*, 497 F. Supp. 2d 301, 305 (D.P.R. 2007) (referring to theory by this name).

by which a court may approve the use of such a device. CALEA then provides, awkwardly, that even if the requirements of the Pen Register Act are satisfied, a pen register cannot be used to track physical locations until the substantive requirements of another statute are met. Why Congress would use this baffling method to express its intent is unclear, especially given the collateral uncertainty it creates, as I discuss below.

C. *The Candidates for Statutory “Partners”*

If some laws are permissible to combine with the Pen Register Act and some are not, there must be a nonarbitrary way of figuring out which are which. This question is a hard one to answer because CALEA simply does not say. CALEA provides neither a list of laws that may be acceptable statutory partners, nor any standards to provide guidance. Many possibilities have been proposed; each leads to differing evidentiary burdens.

Law enforcement has proposed using the Stored Communications Act.⁶¹ This law is ordinarily used to access data stored on computers. Some judges have instead suggested Rule 41 of the Federal Rules of Criminal Procedure as a statutory partner.⁶² This is the general authorization for magistrates to issue search warrants upon a showing of probable cause.⁶³ Advocacy groups that join litigation as amici have proposed that the only logical statutory partner for these orders is Title III.⁶⁴

The Stored Communication Act (SCA) is a plausible, but unlikely, partner to the Pen Register Act. As indicated by the chart above, the evidentiary burden it imposes is intermediate, somewhere between probable cause and an ordinary pen register. This is an odd choice, however: The SCA, by its terms, applies only to stored electronic communications.⁶⁵ Much cell phone tracking, however, is prospective rather than backward-looking.⁶⁶ To avoid this problem, the

⁶¹ 18 U.S.C. §§ 2701–2711 (2000).

⁶² See, e.g., *In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info. (Orenstein Opinion II)*, 396 F. Supp. 2d 294, 313–14 (E.D.N.Y. 2005).

⁶³ See FED. R. CRIM. P. 41(d)(1) (requiring judge to “issue the warrant” after receiving affidavit from law enforcement officer “if there is probable cause to search for and seize a person or property or to install and use a tracking device”).

⁶⁴ The Electronic Frontier Foundation is one example of such an advocacy group. See Brief for the Electronic Frontier Foundation as Amicus Curiae Opposing the Government at 6–9, *In re Application for Pen Register & Trap & Trace Device with Cell Site Location Auth.*, No. 05-1093 (E.D.N.Y. Sept. 23, 2005) (arguing that only warrant satisfying Title III’s requirements can authorize cell phone tracking).

⁶⁵ 18 U.S.C. § 2703(a).

⁶⁶ See *supra* text accompanying note 3.

government often argues that before the cell site data is provided, it has been stored for a few moments in the computers of the cell service provider.⁶⁷ This reading has convinced some judges to issue the orders,⁶⁸ but stretches credulity very near to its breaking point.

Federal Rule of Criminal Procedure 41, the general rule providing for a search warrant upon probable cause,⁶⁹ is unobjectionable as a potential partner for the Pen Register Act. The government concedes that probable cause is sufficient to track a cell phone; it simply disagrees that it is necessary. While it is possible to argue that the more rigorous requirements of Title III apply,⁷⁰ the fact that the statute deals only with content, not envelope, information suggests that the requirements of Title III remain confined to traditional wiretaps.⁷¹

A textual analysis does reveal that some interpretations of the Pen Register Act and CALEA are better than others. There is still quite a bit of ambiguity remaining, however, and it is impossible to reach a firm conclusion based on pure, "internal" statutory reasoning. It is worth exploring alternative sources of meaning, particularly the Constitution, to see if any progress can be made toward the best understanding of this confusing patchwork of laws.

III

CONSTITUTIONAL DOUBT

This Part argues that the Constitution is a useful source of meaning for this question. Considering the extent to which the Fourth Amendment already regulates police investigations, it is logical to expect it to bear on the statutory analysis of procedural requirements for cell phone tracking. Indeed, the legal norms of that Amendment ought to bear on one of the most significant investigative tools of the new century. In particular, the Fourth Amendment can inform

⁶⁷ The particular magistrate's tolerance for this form of wordplay often decides the case. Cf. *In re Application of the United States for an Order Authorizing the Installation & Use of a Pen Register Device, a Trap & Trace Device, & for Geographic Location Info.* (*McGiverin Opinion*), 497 F. Supp. 2d 301, 309 n.3 (D.P.R. 2007) ("[T]he fact that there may be momentary storage of cell site data before disclosure to the government does not address the SCA's lack of procedural safeguards.").

⁶⁸ See, e.g., *In re Application of the United States for an Order for Disclosure of Telecomms. Records & Authorizing the Use of a Pen Register & Trap & Trace* (*Gorenstein Opinion*), 405 F. Supp. 2d 435, 446–47 (S.D.N.Y. 2005) (holding that cell site information "is transmitted to the Government only after it has come into the possession of the cellular telephone provider in the form of a record" and that SCA is appropriate statutory partner with Pen Register Act under CALEA).

⁶⁹ FED. R. CRIM. P. 41(d)(1).

⁷⁰ See *supra* Part II.A and accompanying chart.

⁷¹ See *supra* notes 37–47 and accompanying text.

CALEA's ambiguous statutory text via the canon of "constitutional doubt."

This Part will first explore what "constitutional doubt" or "constitutional avoidance" is, as an interpretive technique, and how it operates. Second, it will explain why the issuance of cell phone tracking orders without probable cause raises constitutional doubts. Finally, this Part will argue that constitutional doubt is more than simply a workable approach to this problem; it is positively required and evinces respect for the statutory text without neglecting the task of judging under a constitution. Much of the statutory law on this topic was written in direct response to constitutional concerns and decisions by the Supreme Court. In assessing the meaning of that statutory framework for completely new investigative techniques, consulting the Constitution is likely to yield a more organic understanding of all the relevant law. Constitutional avoidance is thus the *best* approach to this interpretive difficulty.

A. *What Constitutional Doubt Is*

Attempting to interpret statutes so that they are consistent with the supreme law of the land is an exercise with a long pedigree across boundaries of ideology and time. The canon has been invoked in opinions by Justices Brandeis,⁷² Brennan,⁷³ Scalia,⁷⁴ and Chief Justice Marshall.⁷⁵

Reduced to its essentials, the canon of constitutional avoidance goes as follows: If a statute admits two constructions, one of which is constitutionally uncontroversial and the other of which requires a major decision on a hard question of constitutional law, the former is better. Of course, sometimes a statute does not admit more than one meaning, and the constitutional issue must be decided. But courts have long assumed that "the legislature is loathe to come close . . . to the precipice beyond which a statute will fall athwart of the Constitution."⁷⁶

The canon does not require a conclusive determination that one construction of a statute is definitely unconstitutional. It only requires

⁷² *Ashwander v. Tenn. Valley Auth.*, 297 U.S. 288, 345–46 (1936) (Brandeis, J., concurring).

⁷³ *NLRB v. Catholic Bishop of Chi.*, 440 U.S. 490, 510 (1979) (Brennan, J., dissenting).

⁷⁴ *Almendarez-Torres v. United States*, 523 U.S. 224, 250 (1998) (Scalia, J., dissenting).

⁷⁵ *Murray v. The Charming Betsy*, 6 U.S. (2 Cranch) 64, 118 (1804). Avoidance of conflict with the "law of nations" referred to in this passage has been later used by the Court in constitutional avoidance cases. See *Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575 (1988).

⁷⁶ WILLIAM N. ESKRIDGE, JR. ET AL., *CASES AND MATERIALS ON LEGISLATION: STATUTES AND THE CREATION OF PUBLIC POLICY* 907 (4th ed. 2007).

a serious controversy about one interpretation, such that it would be impossible to avoid a major constitutional ruling were that interpretation embraced. Otherwise, as Justice Scalia has explained, the canon would “mean that our duty is to first decide that a statute is unconstitutional and then proceed to hold that such ruling was unnecessary because the statute is susceptible of a meaning, which causes it not to be repugnant to the Constitution.”⁷⁷

The burden on someone who would oppose an argument based on the constitutional avoidance canon is thus to do much more than simply defend the constitutionality of their preferred interpretation. Their burden is to demonstrate that their interpretation is so correct as to be *uncontroversial*, raising no hard questions of constitutional law at all.⁷⁸

B. Constitutional Doubts in This Case

In this Section, I focus on the most serious source of constitutional doubt for warrantless location tracking: the Fourth Amendment.⁷⁹

The Fourth Amendment places significant limitations on police investigation because of its blanket protection against “unreasonable searches and seizures.”⁸⁰ Despite this, constitutional law has not played a part in the holding of any judge confronting applications for cell phone tracking. One court dismissed the idea outright (and, worse, relegated the dismissal to a footnote).⁸¹ That dismissal was too hasty; I argue in this Section that location tracking absent a showing of probable cause does raise constitutional concerns serious enough to justify the invocation of constitutional doubt as an interpretive technique.

⁷⁷ *Almendarez-Torres*, 523 U.S. at 250 (Scalia, J., dissenting) (quoting *United States ex rel. Att’y Gen. v. Del. & Hudson Co.*, 213 U.S. 366, 408 (1909)).

⁷⁸ *Cf. id.* at 260 (“[A]ll that I need to establish . . . is that on the basis of our jurisprudence to date, the answer to the constitutional question is not clear. It is the Court’s burden, on the other hand, to establish that its constitutional answer shines forth clearly from our cases.”).

⁷⁹ In this Note, I focus on the Fourth Amendment in order to treat the issue in depth; the reader should not infer from this that there could not be other serious constitutional concerns. There is a colorable claim that cell phone tracking might restrict movement between states, for example. *Cf. Kent v. Dulles*, 357 U.S. 116, 126 (1958) (describing freedom of movement as “basic in our scheme of values”); *Paul v. Virginia*, 75 U.S. 168, 180 (1868), *overruled in part by* *United States v. Se. Underwriters Ass’n*, 322 U.S. 533 (1944) (holding that Constitution ensures free egress and ingress between states).

⁸⁰ U.S. CONST. amend. IV.

⁸¹ *In re Application of the United States for an Order Authorizing the Disclosure of Prospective Cell Site Info. (Adelman Opinion)*, No. 06-MISC-004, 2006 WL 2871743, at *5 n.6 (E.D. Wis. Oct. 6, 2006) (noting it is “doubtful that the government’s use of cell site information to track a suspect implicates the Fourth Amendment”).

The Fourth Amendment prohibits “unreasonable searches” by the state or its agents of “persons, houses, papers, and effects.”⁸² This means there are at least three constitutional inquiries necessary to answer a Fourth Amendment question: First, is the activity a search at all? Second, is it a search of “persons, houses, papers, [or] effects”? Finally, is the search “unreasonable”?

There is precedent on each of these points, naturally, and the remainder of this Part will consider it. It is worth noting, however, that no Supreme Court case speaks directly to this issue for a simple reason: The technique is new, enabled by a technology unforeseen in 1791 or even at the time of the Pen Register Act’s drafting. The assumption about investigation in 1791 was that for police to track someone’s movements, the police had to physically follow that person around or hire spies to do the same. That assumption was first relaxed when radio technology made police-installed “beepers” possible, but even then the police needed advance physical access to an object guaranteed to be in the suspect’s possession, as well as ongoing proximity to the suspect.⁸³ Today, the assumption has been completely obliterated, so the failure of existing law to adequately resolve this novel issue is unsurprising. Thus, this is an occasion to reexamine existing precedent as much as to apply it, because the predicate assumptions of the doctrine have changed. We cannot know what the ratifiers of the Fourth Amendment would have thought their document meant for remote location surveillance, but it is a safe bet that—if the possibility of British soldiers monitoring Sam Adams’ location from London was feasible in their time—they would have thought it meant *something*.

1. *Is This Police Activity a “Search”?*

The threshold question for warrantless location tracking is whether the constant monitoring of a citizen’s every move, both in public and elsewhere, is considered a search. I argue that it is.

The word “search” is not given its usual meaning⁸⁴ when interpreting the Fourth Amendment. Instead, the Supreme Court has crafted its own test for what a Fourth Amendment “search” is, a test that has subsequently spawned its own forest of opinions. In *Katz v. United States*,⁸⁵ Justice Harlan’s well-known concurrence read the Fourth Amendment to extend only to “expectation[s] of privacy . . .

⁸² U.S. CONST. amend. IV.

⁸³ See *infra* Part III.B.1.iii (discussing Fourth Amendment beeper cases).

⁸⁴ OXFORD ENGLISH DICTIONARY 804 (2d ed. 1989) (defining “search” as “examination or scrutiny for the purpose of finding a person or thing”).

⁸⁵ 389 U.S. 347 (1967).

that society is prepared to recognize as ‘reasonable.’”⁸⁶ Violating those expectations is permissible, but constitutes a Fourth Amendment “search.”

This definition is more than a little circular, and has prompted widespread criticism on this ground. The general tenor is captured by Professor Amsterdam’s argument that, if the test were taken seriously, the state could eliminate all privacy interests by announcing “that we were all forthwith being placed under comprehensive electronic surveillance.”⁸⁷ Being told the Fourth Amendment protects the things society regards as private does little more than unhelpfully reframe the question.⁸⁸ However, there are particular explications of “reasonable expectations” that are relevant to cell phone tracking. These explications are sufficient for our purposes, as they can guide application of the *Katz* standard. The remainder of this Section considers decisions about reasonable expectations of privacy in the context of pen registers, disclosure of information to third parties, and beepers.

i. Pen Registers and *Smith v. Maryland*

The first major area of precedent bearing on cell phone tracking is the Court’s initial application of *Katz* to pen registers. In *Smith v. Maryland*,⁸⁹ the Supreme Court held that the use of pen registers was not a “search” for Fourth Amendment purposes, and so the Fourth Amendment would not regulate their use.⁹⁰ At first glance, this would appear to settle the topic of this Note fairly decisively (and in the opposite direction of its thesis), so it is worth analyzing the opinion in greater depth.

It is a mistake to describe *Smith* too abstractly. In fact, all the case decided was that for Fourth Amendment purposes, police gathering of a list of dialed phone numbers was not a search. The difference between the pen registers at issue in *Smith* and the pen registers at issue in this Note is that, while the name of the device remains the same, the pen registers at issue in *Smith* did not disclose mobile tracking information. They simply “record[ed] the numbers dialed from the telephone at petitioner’s home,” and it was those dialed

⁸⁶ *Id.* at 361 (Harlan, J., concurring).

⁸⁷ Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1974). Though beyond the scope of this Note, Professor Amsterdam’s objection seems irrefutable.

⁸⁸ See *Minnesota v. Carter*, 525 U.S. 83, 97 (1998) (Scalia, J., concurring) (“[*Katz*’s ‘reasonable expectations’] bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable.”).

⁸⁹ 442 U.S. 735 (1979).

⁹⁰ *Id.* at 745–46.

numbers that the petitioner sought to suppress.⁹¹ The key to Justice Blackmun's opinion is its determination that Smith lacked "a 'legitimate expectation of privacy' regarding *the numbers he dialed* on his phone."⁹²

Thus, *Smith* does not place all conceivable uses of a pen register outside the purview of the Fourth Amendment.⁹³ This is quite sensible. A pen register is nothing more than a device or process. The Fourth Amendment regulates *searches*, not the equipment or technology with which searches are conducted. That some uses of a pen register raise Fourth Amendment concerns and others do not is unsurprising, just as some uses of a telescope might be regulated by the Fourth Amendment even though others are not.

Beyond simply contrasting the holding of *Smith* with the current facts, however, consider too that Justice Blackmun's analysis is animated by concerns inapplicable to mobile location tracking. Justice Blackmun noted that everyone knows "that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills."⁹⁴ The typical cell phone bill, however, does *not* contain the triangulated latitude and longitude information the police can calculate using today's pen registers, for a simple reason: Phone bills disclose only information about calls, whereas cell phones are in constant communication with radio towers whether or not a call is being made.

An advocate of extending *Smith* to this new type of pen register might analogize to Internet surveillance. Most commentators have generally assumed that *Smith*'s reasoning holds when applied to information like e-mail addresses, and thus reading such information is not a Fourth Amendment search.⁹⁵ In *United States v. Forrester*,⁹⁶ the Ninth Circuit became the first appeals court to explicitly so hold.⁹⁷ This thinking keys off of the familiar "content/envelope"⁹⁸ distinction:

⁹¹ *Id.* at 737.

⁹² *Id.* at 742, 745–46 (emphasis added).

⁹³ *See id.* at 745–46 ("We therefore conclude that petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not 'legitimate.' The installation and use of a pen register, consequently, was not a 'search,' and no warrant was required.").

⁹⁴ *Id.* at 742.

⁹⁵ *See, e.g.,* Orin Kerr, *No Fourth Amendment Protection in E-mail Addresses, IP Addresses, Ninth Circuit Holds*, THE VOLOKH CONSPIRACY, http://www.volokh.com/posts/chain_1184933802.shtml (July 6, 2007, 18:27 EST). It is also generally agreed that the *content* of those messages is protected except upon procurement of a Title III order. *Id.*

⁹⁶ 495 F.3d 1041 (9th Cir. 2007).

⁹⁷ *Id.* at 1048–50.

⁹⁸ *See supra* Part II.A.

The e-mail address on a message is like the postal address on a letter, which is like the phone number dialed to place a call, and so on.

Recall, though, that pen registers used to monitor one's location do not fit neatly into the "content/envelope" paradigm. Even if the cell site data is "envelope" information in a strict technical sense, for Fourth Amendment purposes, it is undeniably more intrusive than having the e-mail addresses of one's correspondence logged. It also violates one's "reasonable expectations of privacy" far more, to the extent that phrase is meaningful. The "content/envelope" distinction is often a helpful heuristic when determining Fourth Amendment reasonableness, but it is no more than that.

What *Smith* settles is the question of a "reasonable expectation of privacy" in dialed phone numbers, and perhaps analogous envelope information. But it is no help at all in assessing such an expectation in the location of one's phone (and, by extension, one's self). "Envelope" information or no, rote application of *Smith* would fail to capture its motivating principles.

ii. The Third-Party Doctrine

The third-party doctrine is the principle that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."⁹⁹ Another potential justification of warrantless mobile location tracking might go: The user of the phone voluntarily conveys his location to the phone company, ergo he enjoys no expectation of privacy in that information, ergo the Fourth Amendment is not implicated.

This is a strong argument, if one takes the third-party doctrine as seriously as it could possibly be taken. This is a useful occasion to consider the boundaries of the third-party doctrine: What does voluntarily conveying information really mean?

The third-party doctrine has grown over the course of many cases.¹⁰⁰ In *United States v. Miller*, for example, the Court held that a bank depositor has no "legitimate 'expectation of privacy'" in financial information "voluntarily conveyed to . . . banks and exposed to

⁹⁹ *Smith*, 442 U.S. at 743–44.

¹⁰⁰ See, e.g., *United States v. Miller*, 425 U.S. 435, 442–43 (1976) (holding that information voluntarily given to banks is not protected by Fourth Amendment); *Couch v. United States*, 409 U.S. 322, 335–36 (1973) (holding that information knowingly given to accountant is not constitutionally protected); *United States v. White*, 401 U.S. 745, 752 (1971) (holding that conversations voluntarily transmitted by one party to police are not constitutionally protected); *Hoffa v. United States*, 385 U.S. 293, 302–03 (1966) (holding that conversation recounted to police by government informant is not constitutionally protected); *Lopez v. United States*, 373 U.S. 427, 438 (1963) (holding that conversations voluntarily recounted by one party to police are not constitutionally protected).

their employees in the ordinary course of business.”¹⁰¹ Explaining why, the Court noted:

The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.¹⁰²

Because the depositor “assumed the risk” of disclosure, the Court held that it would be unreasonable for him to expect his financial records to remain private.

The strongest possible formulation of the third-party doctrine, though, cannot be correct. A person also voluntarily transmits the *contents* of his communication to the phone companies, and yet it is widely recognized that listening in on phone conversations is a search.¹⁰³ However, this point has been made unsuccessfully before:

The telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment. Yet we have squarely held that the user of even a public telephone is entitled “to assume that the words he utters into the mouthpiece will not be broadcast to the world.”¹⁰⁴

The boundaries of this doctrine are thus far from clear. Transmitting some information to a third party will result in the police being able to seize that information without implicating the Fourth Amendment, but not other information, without a clear mechanism to distinguish which is which. What result, when applied to cell phone tracking?

In the spirit of constitutional doubt and avoiding major constitutional issues when possible, there is a way out. A court could and should hold that because a cell phone *passively* communicates its location to the radio towers without user input, the third-party doctrine is

¹⁰¹ 425 U.S. at 442.

¹⁰² *Id.* at 443 (citation omitted).

¹⁰³ See, e.g., *Smith v. Maryland*, 442 U.S. 735, 746–47 (1979) (Stewart, J., dissenting); *Katz v. United States*, 389 U.S. 347, 353 (1967) (holding that wiretapping public phone is Fourth Amendment search) (“The telephone conversation itself must be electronically transmitted . . . and may be recorded or overheard . . . Yet we have squarely held that the user of even a public telephone is entitled ‘to assume that the words he utters into the mouthpiece will not be broadcast to the world.’” (quoting *Katz*, 389 U.S. at 352)).

¹⁰⁴ *Smith*, 442 U.S. at 746–47 (1979) (Stewart, J., dissenting) (quoting *Katz*, 389 U.S. at 352).

not implicated. If the phone is transmitting its location at all times no matter what its owner does, it can hardly be said that the user has voluntarily conveyed some information to the phone company; rather, it is the phone doing the conveyance, without the user doing anything at all.

A dedicated believer in the third-party doctrine might find this explanation unsatisfying. But it is the only way to deal with the issue coherently and also avoid a difficult constitutional decision harmonizing *Katz* and *Miller*.

iii. The “Beeper” Cases: *Knotts* and *Karo*

The Supreme Court, in the early 1980s, confronted a primitive form of the technology being used today: police tracking of suspects using “beepers.” In *United States v. Knotts*¹⁰⁵ and *United States v. Karo*,¹⁰⁶ the Court held that the installation of the beeper and subsequent tracking of the container into which it was installed was not a search for Fourth Amendment purposes, so long as the vehicle was monitored only on public roads and in public places.¹⁰⁷

Even stated at that level of generality, the combined holdings of *Knotts* and *Karo* argue that a warrant might be required to track a cell phone. Cell phones, after all, do not stay only on public roads or in public places. A cell phone generally stays in the pocket of its owner throughout the day, accompanying her to her private office, the homes of those she may visit, and around her own abode, perhaps even to “her daily sauna and bath.”¹⁰⁸ All of this suggests that obtaining location information using cell phones is a search.

Even location tracking while the phones remain in public is more problematic than a very general reading of *Knotts* and *Karo* might suggest. Unlike a cell phone, a beeper does not disclose specific location information, just relative distance. As Chief Judge Legg has explained, beepers “merely help the police stay in contact with the vehicle that they are actively ‘tailing.’”¹⁰⁹ Use of cell phone tracking,

¹⁰⁵ 460 U.S. 276 (1983).

¹⁰⁶ 468 U.S. 705 (1984).

¹⁰⁷ In *Knotts*, the Court held that it was not a search to use a beeper since it revealed only information that someone could observe from the public. “[H]e voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.” 460 U.S. at 281–82. In *Karo*, when the beeper was used to track items on private property that police could not have observed from outside the house, the Court held that it was a Fourth Amendment search. 468 U.S. at 715.

¹⁰⁸ *Kyllo v. United States*, 533 U.S. 27, 38 (2001) (discussing intimate details that can be revealed by certain intrusive searches).

¹⁰⁹ *United States v. Berry*, 300 F. Supp. 2d 366, 368 (D. Md. 2004).

“unlike a beeper, is a substitute for police surveillance.”¹¹⁰ It is doubtful indeed that tracking a cell phone—a highly precise, real-time substitute for police surveillance—would or should receive constitutional treatment as lenient as a beeper, a highly imprecise aid to ordinary visual surveillance. *Knotts* and *Karo* are among the strongest arguments that cell phone location tracking is a search.

iv. Synthesis

The threshold question of “is this a search?” turns out to be quite complex, because cell phone tracking sits at the intersection of the pen register decisions, the third-party doctrine, and the beeper cases. A cell phone tracking order is a super-pen register that installs a permanent super-beeper. The third-party doctrine provides the most support for the conclusion that gathering this information is not a search, but recall that this Note is advocating only a strategy of constitutional avoidance. The presence of strong counterarguments on the constitutional merits is actually an excellent reason to avoid a decision that would require engaging in those constitutional debates.

2. *Is This a Search of “Persons, Papers, Houses [or] Effects”?*

The Fourth Amendment does not regulate all searches. By its own terms, it applies only to searches of “people, papers, houses, and effects.”¹¹¹ The second question in a Fourth Amendment analysis of cell phone tracking is: Does such tracking achieve a search of anything on that list?

A literalist argument is that the tracking of the phone only searches the location of that phone. This is true, but there is no reason to embrace a failure of imagination so often rejected in other contexts. For example, the use of thermal imaging devices to monitor the external walls of a house “searches,” in a literal sense, only the exterior surface of the walls. Justice Stevens, in his *Kyllo* dissent, makes exactly this point: “All that the infrared camera did in this case was passively measure heat emitted from the exterior surfaces of petitioner’s home; all that those measurements showed were relative differences in emission levels, vaguely indicating that some areas of the roof and outside walls were warmer than others.”¹¹² One can imagine the parallel argument being made for cell phone tracking.

¹¹⁰ *Id.* Chief Judge Legg was discussing GPS sensors placed on a car, but the underlying issues are the same.

¹¹¹ U.S. CONST. amend. IV.

¹¹² *Kyllo*, 533 U.S. at 42–43 (Stevens, J., dissenting).

Justice Scalia's majority opinion in *Kyllo*, however, makes it clear that what a search "reveals," not what it literally monitors, is the relevant standard: "The dissent's repeated assertion that the thermal imaging did not obtain information regarding the interior of the home is simply inaccurate. A thermal imager reveals the relative heat of various rooms in the home."¹¹³

A thermal imager measures only the external temperature of the walls, much as cell phone tracking measures only the location of a phone. But what the technology in both cases *reveals* is private information about an item on the Fourth Amendment's list of regulated subjects. In *Kyllo*, it was the home; with cell phone tracking, it is the person. In fact, when a person is at home, location tracking of that person's cell phone achieves both a search of her home (by revealing that there is a person inside) and her person (by revealing her location). If one wanted to fight literalism with more of the same, it is also logically true that tracking a cell phone's location achieves a search of any container in which the phone resides: perhaps a jacket pocket, a briefcase, or some other container, which the police ordinarily must get a warrant to search.¹¹⁴

While it is true that the same information could be gained with a round-the-clock stakeout of the subject's front door, consider Justice Scalia's response to this argument:

The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment. The police might, for example, learn how many people are in a particular house by setting up year-round surveillance; but that does not make breaking and entering to find out the same information lawful.¹¹⁵

A bit of common sense will dispel any doubt that cell phone tracking is designed to search for a person and reveal her location. If that were not the point, such searches would be of little value to police. It is precisely because of the powerful intuition that a person tends to have her phone with her that this evidence is useful in police investigations and criminal trials.

3. *Is This Search "Unreasonable"?*

The final stage of Fourth Amendment inquiry is reasonableness. There can be no constitutional doubts about reasonable searches; the

¹¹³ *Id.* at 35 n.2 (majority opinion) (citation omitted).

¹¹⁴ *Cf. United States v. Chadwick*, 433 U.S. 1, 11 (1977) (holding that search warrant is required to search footlocker even if police have probable cause to believe that it contains contraband).

¹¹⁵ *Kyllo*, 533 U.S. at 35 n.2.

Fourth Amendment provides no freedom from them. It would certainly be reasonable to monitor a person's location if one had a warrant founded on probable cause.¹¹⁶ So the key question is: Is cell phone tracking a reasonable search even when done absent a warrant? In this case, the question is not really a close one.

Much as with the meaning of "search," the word "unreasonable" in the Fourth Amendment context has acquired a thick judicial gloss. There are generally two moves made when arguing about the reasonableness of a search: invocation of the presumption of unreasonableness for warrantless searches, followed by invocation of one of the laundry-list exceptions to this presumption.

First, the Supreme Court has stated many times that warrantless searches are presumptively unreasonable. "[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."¹¹⁷ The Supreme Court has referred to this as "a cardinal principle" of Fourth Amendment law.¹¹⁸

The Court has also established a raft of exceptions to this presumption, often invoked by those who wish to search without a warrant. This has been done over the vocal and persistent objections of some Justices, who would either prefer that the warrant presumption be truly categorical or be abandoned altogether in favor of a "reasonableness" inquiry grounded in historical practice.¹¹⁹

Despite the presence of this lively debate in the pages of the U.S. Reports, it is actually not particularly important for cell phone tracking. The established exceptions to the warrant requirement—such as arrests in public,¹²⁰ stop-and-frisk searches,¹²¹ searches incident to arrest,¹²² and so on—do not apply to cell phone tracking. Potentially, of course, the warrant requirement could be excused by

¹¹⁶ Doubters of this proposition should recall that, with a warrant, the police can do far more intrusive things than simply monitor a person's location. For example, with a warrant, the police could strip search a child. *Doe v. Groody*, 361 F.3d 232, 238 (3d Cir. 2004) (suggesting in dicta that search warrant could authorize said search).

¹¹⁷ *Katz v. United States*, 389 U.S. 347, 357 (1967) (footnote omitted).

¹¹⁸ *Mincey v. Arizona*, 437 U.S. 385, 390 (1978).

¹¹⁹ The most vocal critic of the current approach is Justice Scalia. According to him, the Court has "lurched back and forth between imposing a categorical warrant requirement and looking to reasonableness alone." *California v. Acevedo*, 500 U.S. 565, 582 (1991) (Scalia, J., concurring). The result is that the warrant requirement has become "so riddled with exceptions that it [is] basically unrecognizable." *Id.*

¹²⁰ *United States v. Watson*, 423 U.S. 411, 423–24 (1976).

¹²¹ *Terry v. Ohio*, 392 U.S. 1, 27 (1968).

¹²² *United States v. Robinson*, 414 U.S. 218, 235 (1973).

exigency, as it always can.¹²³ There is no worry that a burdensome warrant process will slow down the police in a true emergency that requires a cell phone to be tracked without any delay. But other than that, probably none of the exceptions to the warrant requirement are relevant to cell phone tracking.¹²⁴ The real question is the definition of “search.”

4. *Synthesis of the Constitutional Doubts*

This Part has attempted to break the tie amongst the various possible procedural requirements for cell phone tracking, by testing whether such tracking would be constitutional absent probable cause. The most likely answer, certainly likely enough to raise major constitutional doubts about alternative statutory interpretations, is no. Thus, the proper statutory partner with the Pen Register Act under CALEA is Federal Rule of Criminal Procedure 41, which enshrines the Fourth Amendment’s probable cause and warrant requirements.¹²⁵

The tracking of a cell phone is very likely a Fourth Amendment search. The “beeper” cases establish a strong foundation for a reasonable expectation of privacy in one’s movements, at least when one is not in public places. Moreover, the third-party cases are inapposite, since it is the cell phone itself that passively transmits location at all times without interference from the user. This search is a search of the person and potentially the home, and without a warrant, such a search is unreasonable and thus unlawful.

There is room to argue, of course, against all of the points just made. But the job of a court in the interpretation of statutes is to *avoid* hard constitutional questions. Once it is clear that only one interpretation of the statutes is constitutionally uncontroversial, courts are duty bound to embrace that interpretation.

¹²³ See *Warden v. Hayden*, 387 U.S. 294, 298–99 (1967) (“The Fourth Amendment does not require police officers to delay in the course of an investigation if to do so would gravely endanger their lives or the lives of others.”).

¹²⁴ Of course, it is always possible that a court might decide to engage in Fourth Amendment “reasonableness” analysis and forgo the use of its ordinary presumption of unreasonableness. Cf. *Terry*, 392 U.S. at 20–27 (applying “reasonableness” analysis to uphold warrantless stop-and-frisk searches). However, the “reasonableness” inquiry would itself be a major and novel question of constitutional law—exactly the sort of thing the canon of constitutional doubt counsels against except when unavoidable. Thus, the outcome of a free-floating, no-presumptions inquiry into the reasonableness of cell phone tracking is beyond the scope of this Note; it’s only necessary that the reader believe such an inquiry would constitute a major question of constitutional law.

¹²⁵ See FED. R. CRIM. P. 41(d)(1); see also *supra* note 64 and accompanying text (describing contents and requirements of Federal Rule of Criminal Procedure 41).

As a result, the best reading of the electronic surveillance statutes is one that requires that CALEA be “combined with” Federal Rule of Criminal Procedure 41, the rule providing for a warrant upon showing of probable cause, if a cell phone’s location is to be tracked. This is the best reading because it is the only one that doesn’t raise hard constitutional questions. Once probable cause is shown and a warrant issued, there is no longer any doubt about the constitutionality of the search.

C. *Why Avoidance Is the Answer*

Despite the attractiveness of constitutional doubt as an interpretive tool in this case, none of the courts to address warrantless location tracking have relied on it to decide the case.¹²⁶ Moreover, though this topic has attracted attention in the scholarly literature, scholars have not explored this dimension either.¹²⁷ The two bodies of published opinion tend to head down completely different paths: The judges mostly interpret statutes, and the law review articles mostly go straight to the Constitution. This Section argues that constitutional avoidance is more than just a novel approach to this problem; rather, it is the best one.

It must, of course, be honestly admitted that the canon has prominent detractors. Judge Posner has argued that it is a “judge-made ‘penumbra’” that unnecessarily sharpens the tensions between the legislative and judicial branches and breeds judicial activism.¹²⁸ No less a voice than Judge Friendly conceded that while “questioning the doctrine . . . is rather like challenging Holy Writ,” constitutional avoidance has “almost as many dangers as advantages.”¹²⁹

More recently, Frederick Schauer has argued that “it is by no means clear that a strained interpretation of a federal statute that avoids a constitutional question is any less a judicial intrusion than the judicial invalidation on constitutional grounds of a less strained inter-

¹²⁶ Though the *Smith Opinion* mentions the issue in passing, it is not essential to the holding. *In re Application of the United States for an Order Authorizing (1) Installation & Use of a Pen Register & Trap & Trace Device or Process, (2) Access to Customer Records, & (3) Cell Phone Tracking (Smith Opinion)*, 441 F. Supp. 2d 816, 836–37 (S.D. Tex. 2006).

¹²⁷ See, e.g., Kevin McLaughlin, Note, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 HASTINGS COMM. & ENT. L.J. 421 (2007) (arguing for a major decision of constitutional law without mentioning avoidance doctrine).

¹²⁸ RICHARD A. POSNER, *THE FEDERAL COURTS: CRISIS AND REFORM* 285 (1985).

¹²⁹ Henry J. Friendly, *Mr. Justice Frankfurter and the Reading of Statutes*, in *BENCHMARKS* 196, 211 (1967).

pretation of the same statute.”¹³⁰ Though this is surely true, Professor Schauer’s criticism is presumably satisfied by interpretations that are not “strained.” Justice Kennedy has similarly urged caution, arguing that the canon “should not be given too broad a scope lest a whole new range of Government action be proscribed by interpretive shadows cast by constitutional provisions that might or might not invalidate it.”¹³¹

These critiques are all valid, and Justice Kennedy’s point in particular ought not to be taken lightly: Applied in bad faith, avoidance has substantial potential for mischief. The canon, however, also figures prominently in recent Supreme Court jurisprudence,¹³² and given how much of criminal procedure is constitutionalized, the technique is quite relevant in this particular area.

One might ask: Why not go all the way? If these searches are so constitutionally doubtful, why not have the magistrate judges simply declare them unconstitutional and be done with it? What does the avoidance doctrine bring to the table? And aren’t there, as Justice Frankfurter once conceded, “obvious advantages in knowing at once the legal powers of the government”?¹³³ Yes. However, unnecessary declarations of unconstitutionality are at odds with long American tradition. Before *Marbury v. Madison*¹³⁴ was decided, Justice Chase declared of the power to strike down statutes as unconstitutional: “I will never exercise it, but in a very clear case.”¹³⁵ Avoiding the exercise of this power is more than mere prudence; it is a rule that has “so long been applied by [the] Court that it is beyond debate.”¹³⁶

To “avoid, not seek out, a constitutional issue” is to recognize the essential nature of our separated powers.¹³⁷ “[A] just respect for the legislature requires, that the obligation of its laws should not be unnecessarily and wantonly assailed.”¹³⁸ Whatever one may think of a particular Congress, it is hard to dispute that the institution has a substantially better claim on “cherished principles of representation

¹³⁰ Frederick Schauer, *Ashwander Revisited*, 1995 SUP. CT. REV. 71, 74. For a general discussion of avoidance’s place in textualism generally, see John F. Manning, *Textualism and the Equity of the Statute*, 101 COLUM. L. REV. 1, 119–26 (2001).

¹³¹ Pub. Citizen v. U.S. Dep’t of Justice, 491 U.S. 440, 481 (Kennedy, J., concurring).

¹³² See, e.g., *INS v. St. Cyr*, 533 U.S. 289, 299–300 (2001) (invoking constitutional avoidance doctrine).

¹³³ *United States v. Cong. of Indus. Orgs.*, 335 U.S. 106, 124 (1948) (Frankfurter, J., concurring).

¹³⁴ 5 U.S. (1 Cranch) 137 (1803).

¹³⁵ *Hylton v. United States*, 3 U.S. (3 Dall.) 171, 175 (1796).

¹³⁶ *Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575 (1988).

¹³⁷ *Eldred v. Reno*, 239 F.3d 372, 378 (D.C. Cir. 2001).

¹³⁸ *Ex parte Randolph*, 20 F. Cas. 242, 254 (C.C.D. Va. 1833) (opinion by Marshall, C.J.).

and political equality” than does any judicial body.¹³⁹ It might thus be wise to exercise some modicum of caution before laying waste to congressional enactments under the banner of the Fourth Amendment, so long as there are other options available that do not compromise the values for which we hold the banner aloft.

Neither, though, should we shy away from insisting that our constitutional values may be on the line. While confining the reasoning purely to the text of the statutes has the virtue of modesty, it does a disservice to the citizenry. We have long come to expect more vigorous supervision of criminal procedure from the courts.¹⁴⁰ As technological advancement gives the police previously unimaginable tools, ours is neither a time to be gun-shy nor trigger-happy.

CONCLUSION

As a general matter, remote location tracking raises issues of what might be termed “location privacy.” This term does not appear in the Constitution or in any statute, but is a helpful conceptual lens through which to think about issues related to the narrow one discussed here. The “right to be let alone”¹⁴¹ does not mean much if, thanks to the vicarious presence of the state in one’s phone, solitude is an illusion.

Location tracking by the government, however, is only the beginning. Location-aware devices are increasingly demanded by consumers themselves: Some new phones can disclose teenagers’ location to their parents¹⁴² or alert users when their friends are nearby.¹⁴³ Low-cost, widely available location surveillance promises many interesting questions for the law, in the context of police investigation and elsewhere.

A robust public debate about location privacy is essential for good policy. That discussion should not occur without reference to shared constitutional norms about search; and in the reading of statutes, Congress should not be presumed ignorant of them.

Remote location tracking of criminal suspects is an investigative tool that could not have been imagined when the Fourth Amendment

¹³⁹ Jeremy Waldron, *The Core of the Case Against Judicial Review*, 115 YALE L.J. 1346, 1353 (2006).

¹⁴⁰ E.g., WILLIAM BLACKSTONE, 4 COMMENTARIES *255–77 (examining criminal procedure in chapter entitled “Of Courts of a Criminal Jurisdiction”).

¹⁴¹ Warren & Brandeis, *supra* note 7, at 193.

¹⁴² David Pogue, *Cellphones That Track the Kids*, N.Y. TIMES, Dec. 21, 2006, at C1, available at <http://www.nytimes.com/2006/12/21/technology/21pogue.html>.

¹⁴³ Ryan Kim, *Find Friends by Cell Phone*, S.F. CHRON., Nov. 14, 2006, at C1, available at <http://sfgate.com/cgi-bin/article.cgi?f=c/a/2006/11/14/BUGMMMC1KE1.DTL>.

was written. Nor could it have been imagined when the Pen Register Act was written nearly two centuries later. The doubtful constitutionality of engaging in such tracking without a warrant compels reading the electronic surveillance statutes to require one.