UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
----------X

UNITED STATES OF AMERICA	:	14 Cr. 68 (KBF)
- against -	:	(Electronically Filed)
ROSS ULBRICHT,	:	
Defendant.	:	

----------X

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT ROSS ULBRICHT'S PRE-TRIAL MOTIONS TO SUPPRESS EVIDENCE, ORDER PRODUCTION OF DISCOVERY, FOR A BILL OF PARTICULARS, AND TO STRIKE SURPLUSAGE

JOSHUA L. DRATEL
JOSHUA L. DRATEL, P.C.
29 Broadway, Suite 1412
New York, New York 10006
(212) 732-0707

Attorneys for Defendant Ross Ulbricht

– Of Counsel –

Joshua L. Dratel
Lindsay A. Lewis
Whitney Schlimbach

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER

Introduction

This Memorandum of Law is submitted on behalf of defendant Ross Ulbricht, in support of his motion(s) to suppress certain evidence, to strike surplusage from the Indictment, and for discovery, a Bill of Particulars, and exculpatory material pursuant to *Brady v. Maryland*, 373 U.S. 83 (1963) and its progeny.

As discussed below, during the course of its investigation in this case, the government conducted a series of 14 searches and seizures of various physical devices containing electronically stored information ("ESI"), and of ESI itself from Internet providers and other sources. Some of the ESI was obtained via search warrant, but other ESI was obtained via court order, and still other ESI was obtained without benefit of any warrant at all.

Pursuant to the "fruit of the poisonous tree" doctrine, *see Wong Sun v. United States*, 371 U.S. 471 (1963), the admissibility of any of that material obtained at the various junctures of the investigation is dependent not only on the validity of the search and seizure through which a particular item of ESI or other evidence was acquired, but also on the validity of the searches and seizures that preceded such acquisition, and upon which any subsequent search and seizure were based.

Here, at the origin of the investigation, and again at multiple points along its path, the searches and seizures were unlawful in violation of the Fourth Amendment to the U.S. Constitution, and/or statutes regulating the acquisition of ESI. As set forth below, certain of the serial searches repeated prior defects; others suffered from separate, independent flaws.

As a result, the ESI and other material seized and searched has been contaminated at its source, and at several later points along the way, rendering the direct and indirect product of

those searches and seizures – in essence, the entire product of the investigation itself – inadmissible. Thus, the Fourth Amendment and relevant statutes require suppression of the fruits of the searches and seizures, and any evidence or other information derived therefrom.

All of the searches and seizures are predicated upon the government's infiltration of the alleged "Silk Road Servers." Each of the applications for warrants begin the tale of the investigation with the statement that "[e]arlier this year [2013], the FBI located the server hosting the Silk Road website in a foreign country." *See, e.g..*, *Affidavit in Support of a Search Warrant,* Eastern District of Pennsylvania, September 9, 2013, at ¶ 12 (a copy of which is provided with this motion as part of Exhibit 1). *See also* **post**, at 5-11.

However, that event – location of the Silk Road Servers – is shrouded in mystery, as the means and manner in which that discovery was accomplished has not been disclosed – indeed, it was not disclosed in any of the applications for warrants or other orders to search and seize ESI and other material in this case.

That presents a threshold issue: whether locating the Silk Road Servers was the result of legitimate investigative technique(s), or the product of some unlawful intrusion, digital or otherwise. It also presents the issue whether the magistrate judges who approved the searches and seizures were remiss in not at least satisfying themselves that the information upon which the warrant was based was lawfully obtained and/or reliable.

In addition, the subsequent searches, whether pursuant to warrant or court order (issued on information establishing less than probable cause) each suffer from similar and in some instances individual defects that render them invalid. For example, the pen register and trap and trace orders should have required a warrant, not only because of the relevant recent case law that

has transformed the application of the Fourth Amendment to digital devices and information, but also because of the use to which the pen register and trap and trace devices were put, and the information they gleaned.

In addition, many of the warrants – in particular, those directed at Mr. Ulbricht's laptop, and his gmail and Facebook accounts – constitute the general warrants abhorred by the Framers, and which led directly to the Fourth Amendment. The wholesale collection and study of Mr. Ulbricht's entire digital history without limitation – expressly sought in the warrants and granted – represent the very type of indiscriminate rummaging that caused the American colonists so much consternation.

Regarding the case law, three recent cases in particular, *Riley v. California*, ___ U.S. ___, 134 S. Ct. 2473 (2014), *United States v. Jones*, ___ U.S. ___, 132 S. Ct. 945 (2012), and *United States v. Davis*, ---- F.3d ----, 2014 WL 2599917 (11th Cir. 2014), have set a course for the Fourth Amendment in the digital age. The evolving and emerging jurisprudence those cases have pioneered is consistent with traditional, fundamental Fourth Amendment values, and harmonizes longstanding legal principles with technological advancement and its impact on the law.

These motions, like much of this case as recognized by the Court in its opinion on the previous pretrial motions directed at the Indictment, "raise novel issues as they relate to the Internet . . ." Slip op. at 1, Dkt. # 42. They are on the cusp of developing law in the digital era, yet they are capable of resolution by time-honored Fourth Amendment principles applied – as they have been in *Riley*, *Jones*, and *Davis* – to contemporary circumstances in a manner that preserves and vindicates vitally important Fourth Amendment protections in the face of government surveillance capability and collection of digital material that threatens to eliminate

privacy altogether.

This Memo of Law will endeavor to avoid repetition of certain legal principles and facts as they apply to the various searches and seizures challenged in this motion. As a result, the structure of the motion to suppress, POINT I, will first provide a review of specific Fourth Amendment principles that apply generally to all of the issues raised in this motion. Following that presentation, certain searches and seizures will be grouped to the extent they suffer from identical or substantially similar constitutional or statutory deficiencies and/or present the same or substantially language in the warrant or order at issue. In addition, the Statement of Facts catalogs chronologically the warrants and orders at issue, but certain additional specific facts regarding the warrants and orders, either collectively or individually, are integrated throughout POINT I where relevant.

These motions also make several discovery demands enumerated in POINT II (as well as demands for *Brady* material), and a demand for a Bill of Particulars in POINT III. In addition, POINT IV moves to strike certain surplusage from the Indictment.

Accordingly, for all the reasons detailed in this Memorandum of Law, it is respectfully submitted that the Court should:

(1) suppress all of the material and information obtained through the invalid searches and seizures, and suppress all fruits therefrom;

(2) order the government to produce the discovery demanded;

(3) order the government to provide a Bill of Particulars as demanded herein;

(4) strike the designated surplusage from the Indictment; and

(5) conduct any evidentiary hearings necessitated by these motions.

Statement of the Facts

As noted above, the government's investigation in this case proceeded through a series of 14 searches and seizures of digital storage devices and the digital information stored therein. As each affidavit submitted in support of each search warrant states, *all* of the searches and seizures were premised upon the government's location of the Silk Road Servers, and the government's subsequent access to the ESI contained therein.

Thus, each affidavit states in identical language:

> Earlier this year [2013], the FBI located the server hosting the Silk Road website in a foreign country. Through a Mutual Legal Assistance Treaty request, the FBI received an image of the contents of the Silk Road Web Server on or about July 29, 2013.

See, e.g., *Affidavit in Support of a Search Warrant,* Eastern District of Pennsylvania, September 9, 2013, at ¶ 12 (Exhibit 1); *see also Affidavit in Support of a Search Warrant,* Eastern District of Pennsylvania, September 9, 2013 at ¶ 10 (Exhibit 2).[1]

Following forensic analysis of the Silk Road Servers by an "FBI computer forensic team[,]" *see, e.g.*, *Affidavit in Support of a Search Warrant,* Eastern District of Pennsylvania, September 9, 2013, at ¶¶ 12-13 (Exhibit 1), the government commenced its applications for warrants and orders based on the information obtained from those servers.

Those 14 warrants and orders proceeded chronologically as follows:

(1) the government applied September 9, 2013, to the District Court for the Eastern District of Pennsylvania, for a warrant to search the contents of the server maintained on behalf of JTAN.com stored in the second position from the top of a

[1] All of the warrants, orders, and supporting materials produced in discovery are provided with this motion as Exhibits.

rack at Windstream Communications Conshohocken Data Center, 1100 East Hector Street, Lee Park, Suite 500, a storage facility in Conshohocken, Pennsylvania. United States Magistrate Judge David R. Strawbridge issued a search and seizure warrant September 9, 2013, for the search of the contents of the server maintained on behalf of JTAN.com in the second position from the top of the rack (Exhibit 1);

(2) one minute later (4:51 p.m.) that same day, Magistrate Judge Strawbridge, in response to an application made September 9, 2013, to the District Court for the Eastern District of Pennsylvania issued a second warrant for the search and seizure of the contents of another server, maintained by JTAN.com, headquartered at 1302 Diamond Street, Sellersville, Pennsylvania. The warrant application noted that while the target server was located in Windstream Communications Conshohocken Data Center, in Conshohocken, Pennsylvania, JTAN.com was believed to have administrative access to the target server, had electronically preserved its contents in response to an FBI inquiry regarding the server, and could therefore produce a digital copy of the contents of the target server (Exhibit 2);

(3) the government applied September 16, 2013, to the District Court for the Southern District of New York for a Order directing Comcast to install a trap and trace device to identify the IP address of any Internet communications directed at a Comcast account assigned an Internet Protocol (hereinafter "IP") address as of September 14, 2013, and a pen register to determine the destination IP addresses

of any communication originating from that Comcast account, as well as the date, time, duration and port of transmission of such communications. By Order dated September 16, 2013, United States Magistrate Judge Henry Pitman Ordered the installation of the requested trap and trace device and pen register (hereinafter "pen-trap") for a period not to exceed 60 days from the date of the Order (Exhibit 3);

(4) the government applied September 17, 2013, to the District Court for the Southern District of New York, for another Order directing Comcast to install a trap and trace device to identify the IP address of any Internet communications directed at the Comcast account assigned an IP address as of September 15, 2013, and a pen register to determine the destination IP addresses of any communication originating from that Comcast account, as well as the date, time, duration and port of transmission of such communications. By Order dated September 17, 2013, Magistrate Judge Pitman Ordered the installation of the pen-trap for a period not to exceed 60 days from the date of the Order (Exhibit 4);

(5) the government applied, September 19, 2013, to the District Court for the Southern District of New York for an Order authorizing the FBI to use a pen register and trap and trace device to identify the source and destination IP addresses, as well as dates, times, durations, port of transmissions, and also any Transmission Control Protocol (hereinafter "TCP") collection data, associated with any electronic communications sent to or from the wireless router maintained at 235 Monterey Boulevard, San Francisco, California, 94131, assigned an IP

address, as of the date of the application. By Order dated September 19, 2013, Magistrate Judge Pitman authorized the requested pen-trap for a period not to exceed 60 days from the date of the Order (Exhibit 5);

(6) that same day, September 19, 2013, the government also applied to the District Court for the Southern District of New York for a warrant to search a computer server assigned two different IP addresses, maintained at a premises controlled by Voxility LLC, headquartered at 580 California Street, 12th Floor, Suite #1243, San Francisco, California, 94104. Magistrate Judge Pitman issued a warrant for the search September 19, 2013 (Exhibit 6);

(7) the following day, September 20, 2013, the government applied to the District Court for the Southern District of New York for an Order authorizing the FBI to use a pen register and trap and trace device to identify the source and destination IP addresses, as well as dates, times, durations, port of transmissions, any TCP collection data, and any other dialing, routing, addressing and signaling information associated with any electronic communications sent to or from the computer devices associated with four different MAC addresses. Magistrate Judge Pitman authorized the requested pen-trap by Order dated September 20, 2013 (Exhibit 7);

(8) also on September 20, 2013, the government applied for an Order authorizing the FBI to use a pen register and trap and trace device to identify the source and destination IP addresses, as well as dates, times, durations, port of transmissions, any TCP collection data, as well as any MAC addresses, or other dialing, routing,

addressing and signaling information associated with any electronic communications sent to or from the wireless router maintained at 235 Monterey Boulevard, San Francisco, California, 94131, assigned an IP address, as of the date of the application. By Order dated September 20, 2013, United States Magistrate Judge Debra Freeman authorized the requested pen-trap for a period not to exceed 60 days from the date of the Order. The application and subsequent Order were almost identical to the application and Order issued by Magistrate Judge Pitman a day prior, but were broader in scope in terms of what the application and Order permitted the FBI to identify by means of the pen-trap (Exhibit 8);

(9) the government applied October 1, 2013, to the District Court for the Southern District of Pennsylvania for a warrant to search Windstream Communications Conshohocken Data Center, 1100 East Hector Street, Lee Park, Suite 500, a storage facility in Conshohocken, Pennsylvania, and seize three servers, assigned three different IP addresses, and located therein at server rack "R2-16" with the customer ID "ggb" and assigned host number 418, server rack "R2-15" with customer ID "alsa," and assigned host number 421, and rack "R2-15" with customer ID "beggy" and assigned host number 420, respectively. The contents of one of the target servers was also the target of a previous September 9, 2013, search warrant and application (Exhibit 2; *see* ¶ 2 above). United States Magistrate Elizabeth T. Hay issued a warrant October 1, 2013, authorizing the FBI to seize and remove the servers in the above-described locations (Exhibit 9);

(10) also on October 1, 2013, the government applied to the District Court for the Southern District of New York for a warrant to search the contents of a computer server assigned two different IP addresses, maintained at a premises controlled by Voxility LLC, headquartered at 580 California Street, 12th Floor, Suite #1243, San Francisco, California, 94104. The contents of those servers were also the target of a previous September 19, 2013, search warrant and application (Exhibit 6; *see* ¶ 6 above). The government stated in its application that the purpose of the October 1, 2013, search warrant application was "to obtain a more current image of the TARGET server and, thereby, to obtain more current information concerning the balances and contents of the Silk Road Bitcoin Wallets contained therein." October 1, 2013, Application, at 9, ¶ 21. United States Magistrate Judge James L. Cott issued a warrant for the search October 1, 2013 (Exhibit 10);

(11) in addition, the government applied October 1, 2013, to the District Court for the Northern District of California for a warrant for a silver Samsung laptop computer, containing a network adapter with a MAC address, allegedly known to be used by Ross William Ulbricht, and any peripheral devices, storage media, or data security devices attached to or contained in the computer. That same day, United States Magistrate Judge Nathanael Cousins signed the warrant for the search of the Samsung laptop (Exhibit 11);

(12) the government also applied October 1, 2013, to the the District Court for the Northern District of California for a warrant for the search of Mr. Ulbricht's residence located at 235 Monterey Avenue, San Francisco, California, 94131, and

for the seizure of items constituting evidence, contraband, fruits, or instrumentalities of violations of 21 U.S.C. §846, 18 U.S.C. §1030, 18 U.S.C. §956, and 18 U.S.C. §1958. That same day, Magistrate Judge Cousins signed the warrant for the search of 235 Monterey Avenue, and seizure of the above-described items (Exhibit 12);

(13) the government applied October 8, 2013, to the United States District Court for the Southern District of New York for a warrant for all information associated with the Facebook account for username "rossulbricht." That same day, United States Magistrate Judge Gabriel W. Gorenstein signed the warrant for the search of the above-described target account, including the name "Ross Ulbricht," (Exhibit 13); and,

(14) also that same day, October 8, 2013, the government applied to the United States District Court for the Southern District of New York for a warrant to search all content associated with the e-mail account "rossulbricht@gmail.com." That same day, Magistrate Judge Gorenstein signed the warrant for the search of the above-described target account (Exhibit 14).

ARGUMENT

POINT I

THE MATERIALS AND INFORMATION OBTAINED VIA VARIOUS SEARCHES AND SEIZURES IN THE COURSE OF THE INVESTIGATION IN THIS CASE SHOULD BE SUPPRESSED BECAUSE THEY WERE OBTAINED AS A DIRECT OR INDIRECT RESULT OF UNLAWFUL SEARCHES AND SEIZURES CONDUCTED IN VIOLATION OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION

As detailed below, a vast trove of material and information, including ESI, should be suppressed because the government obtained it as a result of unlawful searches and seizures – either directly because the specific warrant or order authorizing the search and/or seizure was unlawful, or because the search and seizure constituted the "fruit of the poisonous tree" of a previously conducted invalid search and/or seizure – that violated the Fourth Amendment to the U.S. Constitution, as well as certain applicable statutes.

As noted **ante**, the warrants and orders contain generally similar language, and build on each other in sequential, chronological fashion. As a result, many of the constitutional and/or statutory defects in a particular warrant or order apply to many of the other warrants and orders. Accordingly, in order to eliminate unnecessary repetition and organize the issues efficiently, the ensuing analysis is presented as follows: Part A will review particular and fundamental Fourth Amendment principles that apply across the board in this motion; Part B will discuss an important historical underpinning of the Fourth Amendment, and which has particular relevance to this motion; Part C will trace the evolution of Fourth Amendment jurisprudence from a doctrine based on property law and the concept of trespass to one that incorporated a person's reasonable expectation of privacy; Part D will review recent case law that demonstrates the

courts' recognition that technological progress, and the advent of ESI as a primary means of information storage and retrieval, and digital devices as a predominant means of communication (not only with other individuals, but with any and all global resources, whether political, personal, commercial, academic, medical, or recreational), requires Fourth Amendment doctrine to adjust, and how courts have adapted traditional constitutional principles to accommodate that technological change; and Part E will address the specific Fourth Amendment and/or statutory deficiencies in the warrants and orders used to obtain material and information in this investigation.

A. *Fundamental Fourth Amendment Concepts and Principles Relevant to This Case*

As the Supreme Court has instructed repeatedly, and most recently in *Riley v. California*, ___ U.S. ___, 134 S. Ct. 2473 (2014),[2] "[a]s the text makes clear, 'the ultimate touchstone of the Fourth Amendment is reasonableness.'" *Id*., at 2482, *quoting Brigham City v. Stuart,* 547 U.S. 398, 403 (2006) (other internal quotation marks omitted). In turn, "'reasonableness generally requires the obtaining of a judicial warrant.'" *Id*., *quoting Vernonia School Dist. 47J v. Acton,* 515 U.S. 646, 653 (1995).

As the Court explained in *Riley*, "'[s]uch a warrant ensures that the inferences to support a search are "drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime."' *Id*., *quoting Johnson v. United States,* 333 U.S. 10, 14 (1948). Thus, "[i]n the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement." *Id*., citing

[2] *Riley* was paired with *United States v. Wurie* (same citation), and decided together with that case. The opinion will be referred to herein as "*Riley*" even when discussing any facts relevant to *Wurie*.

Kentucky v. King, 563 U.S. ___, 131 S. Ct. 1849, 1856–1857 (2011).[3]

Also, the execution of a warrant is as critical to Fourth Amendment compliance as the underlying basis for it, or subsequent review thereof: the "manner in which the government executes [a] warrant must comport with the Fourth Amendment's reasonableness standard." *United States v. Metter*, 860 F. Supp.2d 205, 212 (E.D.N.Y. 2012) (citation omitted); *accord United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006).

> As Justice Breyer observed in *Whalen v. Roe*, 429 U.S. 589, 97 S. Ct. 869 (1977),the example of the Fourth Amendment shows the Constitution puts limits not only on the type of information the State may gather, but also on the means it may use to gather it. The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.

Id., at 607.

In addition, a Fourth Amendment violation is "fully accomplished" at that time of an unreasonable governmental intrusion, "whether or not the evidence seized is sought for use in a criminal trial." *United States v. Verdugo-Urquidez*, 494 U.S. 259, 264 (1990).

B. *The Importance of General Warrants and Writs of Assistance In the Formulation of the Fourth Amendment and the Protections It Affords*

The American colonists' viscerally negative reaction to the British practices of "general warrants" and "writs of assistance" provided an essential impetus for the Fourth Amendment. As the Supreme Court has explained for centuries now,

---

[3] Ironically, as the Court noted in *Riley*, "[i]ndeed, the label 'exception' is something of a misnomer in this context, as warrantless searches incident to arrest occur with far greater frequency than searches conducted pursuant to a warrant." 134 S. Ct. at 2482, citing 3 W. LaFave, Search and Seizure § 5.2(b), p. 132, and n. 15 (5th ed. 2012).

> [o]ur cases have recognized that the Fourth Amendment was the founding generation's response to the reviled "general warrants" and "writs of assistance" of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity. Opposition to such searches was in fact one of the driving forces behind the Revolution itself. In 1761, the patriot James Otis delivered a speech in Boston denouncing the use of writs of assistance. A young John Adams was there, and he would later write that "[e]very man of a crowded audience appeared to me to go away, as I did, ready to take arms against writs of assistance." 10 Works of John Adams 247–248 (C. Adams ed. 1856). According to Adams, Otis's speech was "the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born." *Id.,* at 248 (quoted in *Boyd v. United States,* 116 U.S. 616, 625 [] (1886)).

Riley, 134 S. Ct. at 2494.

As the Court elaborated in *Steagald v. United States*, 451 U.S. 204, 220 (1981),

> [t]he general warrant specified only an offense – typically seditious libel – and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched. Similarly, the writs of assistance used in the Colonies noted only the object of the search – any uncustomed goods – and thus left customs officials completely free to search any place where they believed such goods might be. The central objectionable feature of both warrants was that they provided no judicial check on the determination of the executing officials that the evidence available justified an intrusion into any particular home.

Id., at 220.[4]

---

[4] *See also* William J. Cuddihy, *The Fourth Amendment: Origins and Original Meaning: 602–1791*, at 538 (2009) ("[a] revulsion to general warrants ensued in the colonies that was among the prime causes of the specific warrant clause of the Fourth Amendment as nothing did more to alienate Americans from those warrants"); Tracey Maclin & Julia Mirabella, *Framing the Fourth*, 109 Mich. L. Rev. 1049, 1052 (2011), *available at* http://www.michiganlawreview.org/assets/pdfs/109/6/maclin___mirabella.pdf ("[t]he general warrant was the preponderant motivation behind the [Fourth A]mendment.") (*quoting* Cuddihy,

Just last month, the Second Circuit, in *United States v. Ganias*, ---- F.3d ----, 2014 WL 2722618 (2d Cir. June 17, 2014), reiterated that

> "The chief evil that prompted the framing and adoption of the Fourth Amendment was the 'indiscriminate searches and seizures' conducted by the British 'under the authority of general warrants.'" *United States v. Galpin,* 720 F.3d 436, 445 (2d Cir.2013) (*quoting Payton v. New York,* 445 U.S. 573, 583 (1980)) (internal quotation marks omitted). General warrants were ones "not grounded upon a sworn oath of a specific infraction by a particular individual, and thus not limited in scope and application." *Maryland v. King,* ___ U.S. ___, ___, 133 S.Ct. 1958, 1980 (2013). The British Crown had long used these questionable instruments to enter a political opponent's home and seize all his books and papers, hoping to find among them evidence of criminal activity. *See Stanford v. Texas,* 379 U.S. 476, 482–83 (1965). The Framers abhorred this practice, believing that "papers are often the dearest property a man can have" and that permitting the Government to "sweep away all papers whatsoever," without any legal justification, "would destroy all the comforts of society." *Entick v. Carrington,* 95 Eng. Rep. 807, 817–18 (C.P.1765).

2014 WL 2722618, at *7 (footnote omitted). *See also* Steven Schulhofer, *More Essential Than Ever: The Fourth Amendment In the Twenty-First Century*, 24-30 (2012) (describing another

---

supra, at 771); Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 Mich. L. Rev. 547 (1999), at 551 ("the historical concerns [animating the Fourth Amendment] were almost exclusively about the need to ban house searches under general warrants."); *cf.* Maclin & Mirabella, *supra*, at 1068 (noting that the Fourth Amendment focused on general warrants because at the time of the amendment's drafting, general warrants were perceived to be the only type of search posing a real danger to individual liberty, and observing that the "underlying vision of the amendment . . . is checking the discretionary power of law enforcement officials") (*citing* Davies, *supra*, at 741); *see also Marcus v. Search Warrants of Property at 104 East Tenth St., Kansas City, Mo.*, 367 U.S. 717, 727 (1961)(describing the use of general warrants to intimidate the press); *Herring v. United States*, 555 U.S. 135, 155 (2009) (Ginsburg, J., *dissenting*) (observing that "expansive, interconnected collections of electronic information" in government hands "raise grave concerns for individual liberty" and are "evocative of the use of general warrants that so outraged the authors of our Bill of Rights") (internal quotations omitted).

British case, *The North Briton No. 45*, that was pivotal to the Founders' perspective).[5]

C. *The Evolution of Fourth Amendment Jurisprudence from An Exclusively Property Law-Based Doctrine to One Including a Person's Reasonable Expectation of Privacy*

In *United States v. Jones*, ___ U.S. ___, 132 S. Ct. 945, 949-50 (2012), the Court traces the evolution of Fourth Amendment jurisprudence, from an exclusively property law-oriented analysis based on concepts of trespass, embodied in *Olmstead v. United States*, 277 U.S. 438 (1928), and continued through *Silverman v. United States*, 365 U.S. 404 (1961), to evaluation of a person's reasonable expectation of privacy, first enunciated formally in *Katz v. United States*, 389 U.S. 347 (1967). *See also Kyllo v. United States*, 533 U.S. 27, 32 (2001) (Court has "since decoupled violation of a person's Fourth Amendment rights from the trespassory violation of his property"), *citing Rakas v. Illinois*, 439 U.S. 128, 143 (1978).[6] Thus, while *Jones* was decided technically on a property-oriented basis, the Court added that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." 132 S. Ct. at 953 (cmphasis in original).

---

[5] In its footnote to that passage, the Court in *Ganias* pointed out that "[t]he Supreme Court has explained that *Entick* was 'undoubtedly familiar to every American statesman at the time the Constitution was adopted, and considered to be the true and ultimate expression of constitutional law with regard to search and seizure.'" *United States v. Jones*, ___ U.S. ___, ___, 132 S. Ct. 945, 949 (2012) (internal quotation marks omitted).

[6] In *United States v. Davis*, ---- F.3d ----, ----, 2014 WL 2599917 (11th Cir. 2014), the Court recounted that there exist "two distinct views of the interests protected by the Fourth Amendment's prohibition of unreasonable searches and seizures. The older of the two theories is the view that the Fourth Amendment protects the property rights of the people." *Id*., at *4. However, as the Court added, "in the twentieth century, a second view gradually developed: that is, that the Fourth Amendment guarantee protects the privacy rights of the people without respect to whether the alleged "search" constituted a trespass against property rights." *Id*., at *4; *see also id*., at 4-5 (tracing the evolution of the privacy theory).

In addition, the concurring opinions in *Jones* provided an alternate rationale for the result: that regardless whether there had been a trespass, the *Katz* "expectation of privacy" dictated application of the Fourth Amendment's protection in the context of 28-day long GPS monitoring of the defendant's movements. 132 S. Ct. at 954-57 (Sotomayor, J., *concurring*); *id*., at 957-64 (Alito, J., *concurring*).[7]

D. ***The Supreme Court's Recognition That Fourth Amendment Protections Must Adapt to and Accommodate the Predominance of Ever-Advancing Digital Technology***

Just as the Court in *Katz*, in response to technological change, moved beyond its unduly restrictive analysis of telephone privacy in *Olmstead*, the Court signaled in *Jones* (and foreshadowed previously in *Kyllo*) and demonstrated in *Riley* that the digital era – with respect to communication, storage, and surveillance capacity – augured the arrival of another critical evolutionary period in Fourth Amendment law and application.

While *Riley*'s factual context involved a search incident to arrest, the more profound relevance of the Court's multiple opinions (yet unanimous in result), especially in this case, is the Court's acknowledgment of the need for the Fourth Amendment to recognize and adapt to the technological advancement accompanying the digitization of communication, storage, and surveillance.

In many respects *Riley* moved beyond the pre-existing conceptual framework for the proper scope of searches incident to arrest, propounded more than 40 years ago in *Chimel v. California*, 395 U.S. 752 (1969) and *United States v. Robinson*, 414 U.S. 218 (1973), just as

---

[7] Justice Alito's concurrence in *Jones* was joined by Justices Ginsburg, Breyer, and Kagan. Thus, including Justice Sotomayor, who concurred separately, the number of Justices who would have grounded the result in an expectation of privacy outnumbered those who relied on the property law basis and refrained from reaching the *Katz*-based rationale.

Jones heralded a similar advance beyond the opinions in *United States v. Knotts*, 460 U.S. 276 (1983) and *United States v. Karo*, 468 U.S. 705 (1984), that addressed the use of tracking beepers. *See Jones*, 132 S. Ct. at 951-52.

Thus, while in 1928 Chief Justice Taft could, in *Olmstead*, write that the Fourth Amendment could not be "extended and expanded to include telephone wires reaching to the whole world[,]" at 465, by 1967 *Katz* would reject that limitation in favor of an analytical approach that would harmonize Fourth Amendment values with burgeoning technological mores. It is now another 35 years from the decision in *Smith v. Maryland*, 442 U.S. 735 (1979), and 38 years since *United States v. Miller*, 425 U.S. 435 (1976) was decided, and again during that interval technology has compelled re-evaluation of just what the Fourth Amendment protects.[8]

Many justices – often in dissent or concurrence – have been prescient with respect to the necessity for the Fourth Amendment to acknowledge the impact of technology on the concepts of privacy, surveillance, and government intrusion. For example, in his dissent in *Goldman v. United States*, 316 U.S. 125 (1942), Justice Murphy observed that "science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forbears." 316 U.S. at 139 (Murphy, J., *dissenting*); *see also Olmstead,* 277 U.S. at 474 (Brandeis, J., *dissenting*) ("[w]ays may some day be developed by which the government, without removing papers from secret drawers, can

[8] Thus has it been since enactment of the Fourth Amendment. It was not until the Pony Express, which began its service in 1860, became popular that the issue of mail privacy – personal papers existing outside the home – merited the Supreme Court's attention. *Ex Parte Jackson*, 96 U.S. 727,733 (1877) (holding that "[t]he constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be" such as "in the mail"). *See also United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the house."); *Lopez v. United States*, 373 U.S. 427, 441 (1963) (Warren, C.J., *concurring*) (warning that "the fantastic advances in the field of electronic communications constitute a great danger to the privacy of the individual," and that "indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments"); *Dow Chemical Co. v. U.S.*, 476 U.S. 227, 251 (1986) (Powell, J., *concurring in part and dissenting in part*) (observing that "privacy rights [c]ould be seriously at risk as technological advances become generally disseminated and available in our society"); *United States v. Garcia*, 474 F.3d 994, 998 (7th Cir. 2007) (Posner, J.) ("[t]echnological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive"); *Alliance to End Repression v. City of Chicago*, 627 F.Supp. 1044, 1054 (N.D. Ill. 1985) ("[i]t seems that there should come a point when, in tenaciously tracking and piecing together the details of a person's life from multifarious sources, the resulting probe becomes so intrusive as to amount to an invasion of privacy even if the individual pieces of the probe are from public sources"); *Nader v. General Motors Corp*., 25 N.Y.2d 560, 572 (N.Y. 1970) (Breitel, J., *concurring*) ("[a]lthough acts performed in 'public,' especially if taken singly or in small numbers, may not be confidential, at least arguably a right to privacy may nevertheless be invaded through extensive or exhaustive monitoring and cataloguing of acts normally disconnected and anonymous").

The future envisioned in those opinions has in many respects been realized. *See People v. Weaver*, 12 N.Y.3d 433, 442 (N.Y. Ct. App. 2009) (noting that *Knotts* reserved the question of "twenty-four hour surveillance of any citizen" for another day, and observing that "[t]o say that

that day has arrived involves no melodrama; 26 years after *Knotts*, GPS technology, even in its present state of evolution, quite simply forces the issue").

In that context, the Supreme Court has long recognized the need to apply the Fourth Amendment in a manner that maintains its purposes despite changes in the technological or other circumstances in which Fourth Amendment issues are presented.

For instance, in *United States v. Chadwick*, 433 U.S. 1 (1977), Justice Burger noted that while the Framers "focused on the wrongs of that day," they also "intended the Fourth Amendment to safeguard fundamental values which would far outlast the specific abuses which gave it birth." *Id*., at 9. *See also Goldman*, 139 U.S. at 138 (Murphy, J., *dissenting*) (Court assumes a "duty to see that this historic provision receives a construction sufficiently liberal and elastic to make it serve the needs and manners of each succeeding generation"); Andrew E. Taslitz, *Reconstructing The Fourth Amendment: A History of Search and Seizure*, 1789–1868 51 (2006) ("[t]he Framers' history ultimately matters most when revealing the *values* that originally animated adoption of the amendment . . . [to] allow us to refocus attention on the critical question of what a 'right to be secure' *should* mean").

In light of those principles, the prospect of untrammeled government access to ESI simply because it is technically in the possession of a third party, a commentator remarks, "this state of affairs poses one of the most significant threats to privacy in the twenty-first century." Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083, 1087 (July 2002).

Here, the context includes not only everything in or accessible via Mr. Ulbricht's laptop, but also the entire contents of his Facebook and Gmail accounts, as well as the entire contents of

servers. In both *Jones* and *Riley*, the Court presaged a Fourth Amendment jurisprudence sensitive to the evolving status of digital devices and ESI, and their multiple functionality not only for users, but also for law enforcement as tools for pervasive automated surveillance.

Thus, in *Riley*, the Court understood that regardless of the fact that *all* of the ESI resident on the defendant's cell phone (and that of the defendant in *Wurie* as well) was in the "possession" of (and accessible by) his service provider *by agreement*, "[t]hese cases require us to decide how the search incident to arrest doctrine applies to modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." 134 S. Ct. at 2485.

Expounding on the impact the difference over time technological advancement has had on customary behavior, the Court pointed out that

> [a] smart phone of the sort taken from Riley was unheard of ten years ago; a significant majority of American adults now own such phones. *See* A. Smith, Pew Research Center, Smartphone Ownership—2013 Update (June 5, 2013). Even less sophisticated phones like Wurie's, which have already faded in popularity since Wurie was arrested in 2007, have been around for less than 15 years. Both phones are based on technology nearly inconceivable just a few decades ago, when *Chimel* and *Robinson* were decided.

Id.

Conducting a balancing test – "assessing, on the one hand, the degree to which [a search] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests[,]" *id*., *quoting Wyoming v. Houghton,* 526 U.S. 295, 300 (1999) – frozen in a previous time, the Court realized, would not be consistent with Fourth Amendment values and protections. *See also id*., at 2496-97 (Alito, J., *concurring in the judgment*) ("we should not mechanically apply the rule used in the predigital era to the search of

a cell phone. Many cell phones now in use are capable of storing and accessing a quantity of information, some highly personal, that no person would ever have had on his person in hard-copy form. This calls for a new balancing of law enforcement and privacy interests").[9]

Consequently, while conceding that "a mechanical application of *Robinson* might well support the warrantless searches at issue here[,]" the Court nonetheless concluded that justifying a cell phone search based on "pre-digital analogues" would result in 'a significant diminution of privacy[,]'" *id*., at 2493, and held that ". . . officers must generally secure a warrant before conducting such a search." *Id*., at 2485.

The reasons for that determination apply to ESI and digital devices *en toto*, including to Mr. Ulbricht's laptop at issue. As the Court in *Riley* explained, "[c]ell phones . . place vast quantities of personal information literally in the hands of individuals." *Id*. Consequently, "[a] search of the information on a cell phone bears little resemblance to the type of brief physical search considered in *Robinson*." *Id*. *See also id*., at 2484 ("[b]ut while *Robinson*'s categorical rule strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones").

In *Riley*, the Court expanded its consideration to include the functionality of digital devices:

---

[9] *See also What's Old Is New Again: Retaining Fourth Amendment Protections In Warranted Digital Searches (Pre-Search Instructions and Post-Search Reasonableness)* A Report by the National Association of Criminal Defense Lawyers' Fourth Amendment Advocacy Committee, May 18, 2014 (hereinafter "*NACDL Report*"), available at <http://www.nacdl.org/NewsReleases.aspx?id=33866>, at 3 ("in light of today's digital realities[] . . . Courts are attempting to balance the competing needs for both citizens' privacy and effective law enforcement").

> [c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers. One of the most notable distinguishing features of modern cell phones is their immense storage capacity.

Id., at 2488-89.

Certainly that description applies even more so to laptops, with their enhanced storage capacity, internet access, and diverse functions, including GPS locating. Moreover (and also applicable to laptops), in *Jones*, Justice Alito, concurring, noted that "[p]erhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users . . ." 132 S. Ct. at 963 (Alito, J., *concurring*). *See also Riley*, 134 S. Ct. at 2490 ["[d]ata on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building. *See United States v. Jones,* 565 U.S. ___, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., *concurring*) ('GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations')].

The aggregation of information available from a trove of ESI available on digital devices also influenced the Court's decision in *Riley*:

> [t]he storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information – an address, a note, a prescription, a bank statement, a video – that reveal much more in

> combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.

Id., at 2489.[10]

The Court also disposed of the argument that a digital device such as a cell phone is merely a "container," pointing out that "the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen. That is what cell phones, with increasing frequency, are designed to do by taking advantage of 'cloud computing.' Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself." *Id*., at 2491.

Indeed, the government's attempts to analogize digital devices to traditional analog physical items were met with derision by the Court, which responded that the government's claim "that a search of all data stored on a cell phone is 'materially indistinguishable' from searches of these sorts of physical items . . . is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a

---

[10] *See also NACDL Report*, at 1 ("[w]hat is different is the amount of private information that can be improperly searched and the substantially greater intrusion upon privacy and Fourth Amendment interests that may result").

purse." *Id*., at 2488-89.

In addition, the Court noted that "there is an element of pervasiveness that characterizes cell phones but not physical records[,]" *id*., at 2490, finding it important that "[m]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" *Id*., at 2494-95, *quoting Boyd*, 116 U.S. at 630. Again stressing the need for continually updating Fourth Amendment doctrine to keep pace with a changing world, the Court stated that "[t]he fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple – get a warrant." *Id*., at 2495.

Moreover, the need to act now, rather than waiting, to modernize Fourth Amendment law, was not lost on the Court: "[w]e expect that the gulf between physical practicability and digital capacity will only continue to widen in the future." *Id*., at 2489. The pace of technological advancement has accelerated obsolescence with respect to products themselves, and threatens to do so legally if courts are not responsive. As the Court has recognized, and acted, in *Jones* and *Riley*, the answer is to adapt or become moribund just like any other part of society confronted by shifting circumstances.[11]

---

[11] For instance, media companies that failed to recognize the decline in print media, and did not quickly enough transition to include an online presence (if not abandoning print altogether), have not survived the rapid shift in consumer preferences. The examples in all fields, commercial or otherwise, abound. The law is not materially different in that regard. *See, e.g.*, *American Broadcasting Cos. v. Aereo*, 573 U.S. ___, 134 S. Ct. 2498 (2014) (rejecting notion that Aereo (and any imitators) could violate the spirit and purpose of the copyright act "provided they substitute [] new technologies for old[,]" and correcting the imbalance with an

In a trajectory that arcs at least as far back as *Jackson* and the Pony Express, changes in technology, transportation, and communication have required the courts to navigate a path for the Fourth Amendment that adheres to its fundamental purpose, and applies its fundamental protections. In *Jones* and *Riley*, the Court responded without ambiguity. It bypassed entirely the question whether a third party provider could gain access, or enjoyed possession (by the customer's tacit consent), to digital information, and instead proceeded to modernize Fourth Amendment jurisprudence to account for the new challenges – in degree and in kind – presented by a digital universe.[12] In both cases, a unanimous Court required a warrant and recognized important aspects of digital communication and storage that, as detailed below, are extraordinarily pertinent to the Fourth Amendment issues presented in this case.

In *Kyllo*, the Court framed the issue as follows: "the question [the Court] confront[s] today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy." 533 U.S. at 34. The same is true here in multiples. Also, true here as well, the Court in *Kyllo* cautioned that "the rule we adopt must take account of more sophisticated systems that

---

expansive statutory interpretation).

[12] These concerns are indeed global. Recently, the United Nations High Commissioner for Human Rights issued a Report, *The Right to Privacy In the Digital Age*, 30 June 2014 (hereinafter "*UN Report*"), available at <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf>, that noted ". . . there is universal recognition of the fundamental importance, and enduring relevance, of the right to privacy and of the need to ensure that it is safeguarded, in law and in practice[,]" *id*., at ¶ 13, citing both Article 12 of the Universal Declaration of Human Rights, which provides that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation[,]" *id*., at ¶ 12, and the International Covenant on Civil and Political Rights, to date ratified by 167 States, that provides in article 17 that "no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation." *Id*.

are already in use or development." *Id*., at 36 (footnote omitted).[13]

Last month, too, the Second Circuit articulated the courts' obligation to resolve these issues in a contemporary context. In *Ganias*, the Circuit remarked that "[a]pplying 18th Century notions about searches and seizures to modern technology, however, is easier said than done, as we are asked to measure Government actions taken in the 'computer age' against Fourth Amendment frameworks crafted long before this technology existed." 2014 WL 2722618, at *6 (footnote omitted). The Court in *Ganias* also recognized that "[b]ecause the degree of privacy secured to citizens by the Fourth Amendment has been impacted by the advance of technology, the challenge is to adapt traditional Fourth Amendment concepts to the Government's modern, more sophisticated investigative tools." Again, as set forth below, this case presents that challenge in manifold fashion.

E. ***The Searches and Seizures In This Case Failed to Satisfy the Fourth Amendment***

For several, sometimes overlapping, reasons, the searches and seizures in this case failed to satisfy the strictures of the Fourth Amendment. Those reasons, detailed below, include in broad terms:

(1) the failure to obtain a warrant to seize and search the information on the Silk Road Servers;

(2) the failure to obtain a warrant for purposes of implementing pen registers and/or trap and trace devices that were used to obtain location information regarding Mr. Ulbricht; and

---

[13] Even the dissent in *Kyllo* acknowledged that "the [majority] is properly and commendably concerned about the threats to privacy that may flow from advances in the technology available to the law enforcement profession." 533 U.S. at 51 (Stevens, J., *dissenting*).

(3) the failure to abide by the Fourth Amendment's "particularity" requirement, which demands that the items to be seized (and subsequently searched) be specified in the warrant, and that in the execution of the warrant the search and seizure be confined to those items for which there exists probable cause to seize and search.

Also, certain of the applications failed to apprise the issuing courts of material facts, and/or make misleading or false assertions. In addition, the issuing magistrate judges failed with respect to certain applications to ensure that the information that was used to establish probable cause was lawfully obtained and/or reliable. Moreover, in certain instances, the searches and seizures were conducted in a manner that violated the statutes pursuant to which the orders authorizing them were obtained.

For all these reasons, as well as the doctrine that the "fruit of the poisonous tree" contaminates subsequent searches and seizures, *see Wong Sun v. United States*, 371 U.S. 471 (1963), it is respectfully submitted that the materials and information obtained pursuant to the searches and seizures conducted in this investigation be suppressed because they violated the Fourth Amendment.

1. ***The Government's Location of the Silk Road Servers***

As set forth **ante**, all of the searches and seizures conducted pursuant to warrants and/or orders were based on the initial ability of the government to locate the Silk Road Servers, obtain the ESI on them, and perform extensive forensic analysis of that ESI. Thus, all subsequent searches and seizures are invalid if that initial locating the Silk Road Servers, obtaining their ESI, and gaining real-time continued access to those servers, was accomplished unlawfully.

a. ***Discovery of the Means By Which the Government Located the Servers***

A definitive answer as to whether the government gained access to the Silk Road servers lawfully or unlawfully is not possible at this stage because the government has not disclosed how it located the Silk Road Servers. However, it is apparent that the government did not seek or obtain a warrant to acquire the ESI on those servers, as the subsequent warrant applications note that the ESI was provided in response to a request pursuant to a Mutual Legal Assistance Treaty (hereinafter "MLAT").

As a result, Mr. Ulbricht seeks discovery of the means and methods employed by the government to locate the Silk Road Servers, and the contents of the MLAT request(s). Those discovery demands are set forth **post**, in POINT II, at 60.

The discovery demanded is essential to determine whether the entire series of warrants and/or orders are infected by the government's access to the Silk Road Servers, which included not only their ESI, but also an ability to monitor activity on those servers continuously and in real-time.

b. ***The Prospect of "Parallel Construction" In This Investigation***

In that context, the practice of "parallel construction" is relevant. "Parallel construction," first revealed in a *Reuters* article approximately a year ago, describes a practice by the National Security Agency ("NSA") and the Drug Enforcement Administration's Special Operations Division (hereinafter "DEA SoD") by which the former provides the latter with information about non-national security criminal activity collected via NSA electronic surveillance, and the latter transmits the substance of the information to federal and/or local law enforcement agencies, sometimes without disclosing the origin of the information, and always with the condition that

the NSA's involvement cannot be disclosed to defendants, their counsel, or even courts. *See* John Shiffman and Kristina Cooke, "U.S. Directs Agents to Cover Up Program Used to Investigate Americans," *Reuters*, August 5, 2013, available at <http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805>

The "parallel construction" is the *post hoc* contrived creation of an alternate, sanitized pathway of information or evidence acquisition designed deliberately to shield the NSA's (and DEA's SoD) involvement, and the origins and means of the genuine collection of the information. According to the *Reuters* article, in certain instances even prosecutors were not informed of the true source of the information. *Id*. ("[a]lthough these cases rarely involve national security issues, documents reviewed by Reuters show that law enforcement agents have been directed to conceal how such investigations truly begin – not only from defense lawyers but also sometimes from prosecutors and judges").

Any such sanitizing of an investigation's origins, or the basis for obtaining court authorization for searches (or anything else) cannot be considered legitimate, or a substitute for complete and accurate disclosure. *See* John Shiffman & Kristina Cooke, *U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, Reuters, Aug. 5, 2013, http://reut.rs/15xWJwH (describing parallel construction as "just like money laundering – you work it backwards to make it clean").[14]

[14] Such non-disclosure does not suggest that it is the prosecutors in this case that are at fault here. In fact, it may well be the case that the NSA or other agencies have deliberately concealed this information from the prosecutors as it did the public. *See, e.g.*, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, Reuters, August 5, 2013, available at http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805.

Given the massive breadth of the NSA's dragnet electronic surveillance,[15] this case is a prime candidate for "parallel construction," particularly in light of Silk Road's exclusive operation on the Internet, and its use of both the Tor network and Bitcoin, both designed to anonymize vendors and purchasers, as well as the intensity of the government's multi-year investigation aimed at finding the identity of those operating the web site (evident from the government's description of its investigation). In addition, the government's vague references to its locating of the Silk Road Servers only add to the possibility of "parallel construction." *See In the Matter of the Search of Information Associated with [Redacted] @mac.comthat is Stored at Premises Controlled by Apple, Inc*., not reported in F. Supp.2d, available at 2014 WL 1377793, at *8 n. 15 (D.D.C. April 7, 2014) (seizure and retention of an entire e-mail account pursuant to a search warrant "creates the problem that the data may be put into a larger database that would be ripe for abuse. Even if outright abuse does not occur, there is always the risk of troubling uses such as "parallel construction," where illegal or secret criminal investigations are recreated in a manner that is seemingly consistent with the Constitution without informing the accused or the court. *See* Hanni Fakhoury, *DEA and NSA Team Up to Share Intelligence, Leading to Secret Use of Surveillance in Ordinary Investigations,* Electronic Frontier Foundation, *available at* https://www.eff.org/deeplinks/2013/08/dea-and-nsa-team-intelligence-laundering (last visited

[15] The scope of NSA's electronic surveillance, in terms of both interception of communications, as well as bulk telephony metadata collection, is covered comprehensively in filings in two American Civil Liberties Union lawsuits, *Amnesty International USA, et al. v. Clapper*, 08 Civ. 06259 (JGK) (S.D.N.Y.), Docket #7, and *American Civil Liberties Union, et al. v. Clapper*, 13 Civ. 03994 (WHP) (S.D.N.Y.), Docket #26.

Mar. 30, 2014)).[16]

In addition, disclosures made by former NSA employee Edward Snowden with respect to collaboration between the U.S. and other governments – particularly the United Kingdom's General Communications Headquarters (hereinafter "GCHQ") – in conducting surreptitious warrantless electronic surveillance must be taken into consideration. *See, e.g.*, *UN Report*, at ¶ 4 (noting " . . . revelations in 2013 and 2014 that suggested that, together, the National Security Agency in the United States of America and General Communications Headquarters [GCHQ] in the United Kingdom of Great Britain and Northern Ireland have developed technologies allowing access to much global internet traffic, calling records in the United States, individuals' address books and huge volumes of the digital communications content").

That cooperative electronic surveillance could very well constitute a joint venture that would make the U.S. accountable for the conduct of the foreign government (here, in the context of assisting in locating the Silk Road Servers), and subject that foreign government's conduct to Fourth Amendment scrutiny and standards. *See, e.g., United States v. Paternina–Vergara*, 749 F.2d 993, 998 (2d Cir.1984) (when cooperation with foreign law enforcement officials may

---

[16] As noted by a law professor specializing in Fourth Amendment issues, "[t]he NSA program is representative of a number of other domestic law enforcement efforts – for instance, the seventy-plus "fusion centers" that have been set up to collect and fuse together information from public and private sources – that also involve government accumulation of vast amounts of data." Christopher Slobogin, "Cause to Believe What?: The Importance of Defining A Search's Object – Or, How the ABA Would Analyze the NSA Metadata Surveillance Program," 66 OKLAHOMA L. REV. 2 (2014), *citing* THE CONSTITUTION PROJECT, RECOMMENDATIONS FOR FUSION CENTERS: PRESERVING PRIVACY AND CIVIL LIBERTIES WHILE PROTECTING AGAINST CRIME AND TERRORISM, 4-7 (2012), *available at* http:// constitutionproject.org/pdf/fusioncenterreport.pdf. *See generally*, Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 318-322 (2008) (describing a number of "large-scale" federal data mining programs).

implicate constitutional restrictions, evidence obtained by foreign officials may be excluded); *United States v. Maturo*, 982 F.2d 57, 60-61 (2d Cir. 1992) [regarding suppression of evidence, constitutional requirements may attach in two situations: (1) when the conduct of foreign law enforcement officials rendered them agents, or virtual agents, of United States law enforcement officials, *see United States v. Busic*, 592 F.2d 13, 23 n. 7 (2d Cir.1978); or (2) when the cooperation between the United States and foreign law enforcement agencies is designed to evade constitutional requirements applicable to American officials. *See United States v. Bagaric*, 706 F.2d 42, 69 (2d Cir. 1983)].

The prospect of parallel construction is also present with respect to the Canadian Customs official's July 10, 2013, interception of a package allegedly from a Silk Road vendor and addressed to Mr. Ulbricht. While that interception could have been a coincidence, there were a mere thirteen days between the interception and the FBI's viewing of the first image of the Silk Road Servers (no date is provided for when the Silk Road servers were first located), and provided a convenient basis for Department of Homeland Security investigators to make a controlled delivery of the package and then interview Mr. Ulbricht about it. *See* Complaint, at ¶ 22, 42.

As a result, the government should be compelled to disclose any and all information about that incident as well, and/or to inquire of U.S. law enforcement and intelligence agencies with respect to whether any parallel construction has occurred in this investigation.

c. ***The Government Was Required to Obtain a Warrant to Gain Access to the Silk Road Servers***

According to the warrant applications, the Silk Road Servers the government first gained

access to were located overseas. *See, e.g.*, Exhibit 10, at ¶ 14.[17] Yet even by the government's own arguments in another case, that did not obviate the requirement of seeking a warrant to obtain those servers' ESI.

In *In the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corporation* , 13 MJ 02814 (S.D.N.Y.), the government obtained a warrant for ESI stored by Microsoft. However, Microsoft responded by noting that the ESI sought in the warrant is stored overseas, thereby placing it outside the territorial reach of the warrant.

In reply, the government has asserted that the warrant is not extraterritorial because the statutory provision under which it was obtained, 18 U.S.C. §2703(c), confers jurisdiction over data stored outside the United States. *See id*., at Dkt # 60 ("[t]he warrant properly requires Microsoft to disclose data under its control regardless of where Microsoft has chosen to store the data").

The government's rationale was that in an era in which "email and other electronic communications are used extensively by criminals of all types in the United States and abroad, from fraudsters to hackers to drug dealers, in furtherance of violations of U.S. law," territorial limitations should not apply. *Id*., at Dkt #60. *See also* Mark Hamblett, "Government Rebuts Microsoft Challenge to Email Subpoena," *The New York Law Journal*, July 14, 2014, available

[17] Relevant to Mr. Ulbricht's discovery requests, and the validity of the government's acquisition of the content of the Silk Road Servers, and the subsequent series of warrants, is whether the government knew when it obtained access to the overseas servers that other alleged Silk Road Servers, which were the subject of subsequent warrant applications, were located in the United States, but declined to seek warrants for them, instead opting for a warrantless acquisition via the MLAT process.

at <http:www.newyorklawjournal.com/printerfriendly/id+120662768052>.

The government has not provided any reason why it could not have pursued, and why it was not obligated under its own theory of the scope of §2703(c)'s jurisdiction, to pursue the same avenue – a warrant – for obtaining the ESI on the Silk Road Server and, once it possessed the image of the servers, and monitored them in real time in the U.S., to obtain a warrant to perform its forensic analysis and monitoring of the servers' activity.

Accordingly, the warrantless acquisition of the Silk Road Servers' ESI, and the forensic analysis and effective operation of those servers by the government within the U.S. once an image was obtained, was unlawful. Consequently, any evidence emanating from the locating, acquisition, analysis and monitoring of, the Silk Road Servers should be suppressed. In the alternative, the government should be ordered to produce the discovery demanded in POINT II.

d. ***The Issuing Magistrate Judges Should Have Inquired About the Means Through Which the Government Located the Silk Road Servers***

As noted **ante**, each of the warrant applications included the reference to locating the Silk Road Servers overseas. Yet the government did not disclose in those applications the means of such locating, and there is no evidence that any of the issuing magistrate judges inquired of those means, or satisfied themselves with respect to the lawfulness and/or reliability of the source for the entire probable cause determination.

That represents an abdication of the duty of a "neutral, detached magistrate" occupying the role of constitutional gatekeeper. As the Supreme Court instructed in *Illinois v. Gates*, 462 U.S. 213 (1983), discussing the standard set forth in *Aguilar v. Texas,* 378 U.S. 108 (1964) and *Spinelli v. United States,* 393 U.S. 410 (1969),

> [f]indings of probable cause, and attendant intrusions, should not be authorized unless there is some assurance that the information on which they are based has been obtained in a reliable way by an honest or credible person. *As applied to police officers, the rules focus on the way in which the information was acquired.* As applied to informants, the rules focus both on the honesty or credibility of the informant and on the reliability of the way in which the information was acquired. Insofar as it is more complicated, an evaluation of affidavits based on hearsay involves a more difficult inquiry. This suggests a need to structure the inquiry in an effort to insure greater accuracy. The standards announced in *Aguilar,* as refined by *Spinelli,* fulfill that need. The standards inform the police of what information they have to provide and magistrates of what information they should demand. . . . *By requiring police to provide certain crucial information to magistrates and by structuring magistrates' probable cause inquiries, Aguilar and Spinelli assure the magistrate's role as an independent arbiter of probable cause*, insure greater accuracy in probable cause determinations, and advance the substantive value identified above.

Id., at 283 (emphasis added).

Here, with respect to the means by which the FBI located the Silk Road Servers, the issuing magistrate judges failed to fulfill their crucial role in the warrant process.

2. *The Pen Register and Trap and Trace Orders Were Unlawful Because They Required a Warrant and Also Failed to Adhere to Statutory Limitations*

The pen register and trap and trace Orders (hereinafter "pen-trap"), provided as parts of Exhibits 3 - 5 and 7 - 8, essentially request the following:

> this Court has, upon the application of the United States of America, entered an Order authorizing agents of the Secret Service to direct COMCAST to install a trap and trace device to identify the source Internet protocol ("IP") address of any Internet communications directed to, and a pen register to determine the destination IP address of any Internet communications originating from, the following Internet user account controlled by COMCAST (the "TARGET ACCOUNT"), along with the date, time, duration, and port of transmission, but not the contents, of such communications (the "Requested Pen-Trap"), in connection with a criminal investigation.

See Exhibit 3.[18]

The pen-trap devices were used on routers, IP addresses, and MAC addresses,[19] and the latter applications also referenced Transmission Control Protocols. *See, e.g.*, Exhibit 7, at ¶ 2.[20]

---

[18] According to the applications for the pen-trap Orders,

> [a] "pen register" is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C. § 3127 (3). A "trap and trace device" is defined as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." 18 U.S.C. § 3127 (4).

Exhibit 3, ¶ 4.

[19] According to the applications for the pen-trap Orders, "[e]very device on the Internet is identified by a unique number called and Internet Protocol ('IP') address. This number is used to route information between devices, for example, between two computers. Two computers must know each other's IP addresses to exchange even the smallest amount of information." *See* Exhibit 7, at ¶ 6. A MAC address is "a unique identifier that is hard-coded into a computer that can be used to physically identify the computer (similar to a vehicle identification number of a car)." *See* Exhibit 7, at ¶ 8.

[20] The pertinent applications explained Transmission Control Protocols as follows:

> [o]n the Internet, data transferred between devices is not sent as a continuous stream, but rather the data are split into discreet "packets." Generally, a single communication is sent as a series of packets. When the packets reach their destination, the receiving device reassembles them into the complete communication. Each packet has two parts: a "header," which contains routing and control information, and a "payload," which generally contains user data. The header contains non-content information such as the packet's source and destination IP addresses and the packet's size. The Transmission Control Protocol or "TCP" is a communications protocol used to process such data packets associated with popular Internet applications, such as Internet browser and e-mail applications.

Each of the Orders were for 60 days, although the full range of surveillance under the pen-trap orders lasted approximately two weeks. The applications also claimed that the pen-trap devices did not capture "content." *See, e.g.*, Exhibit 4, at ¶ 2.

While ostensibly a pen-trap reveals only identifying information, in fact these pen-traps had an ulterior purpose: to track Mr. Ulbricht's internet activity, coupled with his physical location, in an effort to connect him to access to the administrative section of the Silk Road Servers at particular times on particular dates. *See* Exhibit 11, at ¶¶ 41(a)-(g). That purpose extends well beyond that permissible for a pen-trap, and, because the devices were used absent a warrant based on probable cause, violates the Fourth Amendment as well as express statutory provisions.

As noted **ante**, in *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court held that a telephone subscriber does not have an expectation of privacy in the numbers he or she dials because the subscriber knows full well that the telephone company keeps records of that information (which the subscriber has at least tacitly "knowingly" provided to that third party). However, the pen-traps in this investigation are not "your grandfather's" pen-trap as was at issue in *Smith*.

For example, in *Smith*, the Court noted in support of its reasoning that a pen register "does not indicate whether calls are actually completed." *Id*., at 736 n. 1, *quoting United States v. New York Tel. Co.*, 434 U.S. 159, 161 n. 1 (1977). *See also id*., at 741 ("a law enforcement official could not even determine from a pen register whether a communication existed"). Also, again as part of its justification, the Court added that "[n]either the purport of any communication

---

Exhibit 7, at ¶ 7.

between the caller and recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers." 442 U.S. at 741, *quoting United States v. New York Tel. Co.*, 434 U.S. at 167.

Here, the pen-traps were implemented to do exactly what the Supreme Court said, "[g]iven a pen register's limited capabilities . . ." 442 U.S. at 742, the device could *not* do, and thus insulated them from constituting an invasion of private communications. The pen-traps here were sought in order to confirm the laptop's connection to the Internet at specific times and dates, their duration, and the laptop's physical location when it logged on and off.

Also, in *Smith*, the Court further based its decision on the fact that pen registers were "routinely used by telephone companies 'for the purpose of checking billing operations, detecting fraud, and preventing violations of law.'" 442 U.S. at 742, *quoting New York Tel. Co.*, at 174-75. *See also id*. (also "to check for a defective dial, or to check for overbilling) (citation omitted) (internal quotation marks omitted).

Again, the Internet provides an entirely different technical and privacy environment than a telephone circuit, particularly one in 1979. As explained by Julian Sanchez (a Research Fellow at the Cato Institute and contributing editor at *Reason* magazine),

> the Internet functions quite differently from the traditional circuit-switched telephone network. On the phone network, a binary distinction between "content" and "metadata" works well enough: The "content" is what you say to the person on the other end of the call, and the "metadata" is the information you send to the phone company so they can complete the call. But the Internet is more complicated. On the Open Systems Connections model familiar to most techies, an Internet communication can be conceptualized as consisting of many distinct "layers," and a single layer may simultaneously be "content" relative to the layer below it and "metadata" relative to the layer above it.

* * *

> The crucial point here is that the detailed "metadata" for a particular Internet communication, past the IP layer, typically wouldn't be processed or stored by the ISP in the way that phone numbers and other call data is stored by the phone company. From the ISP's perspective, all of that stuff is content.
>
> * * *
>
> Either way, the acquisition of "metadata" other than IP addresses from an ISP or off the backbone is pretty clearly dissimilar from the collection of call data at issue in *Smith* in every important respect. It is not information conveyed to the Internet provider for the purpose of routing the communication; it is routing information conveyed through the provider just like any other content. Nor is it information the Internet provider would otherwise normally retain for routine business purposes. Again, relative to the ISP, it's all just content.

Julian Sanchez, "Are Internet Backbone Pen Registers Constitutional?" *Just Security*, September 23, 2013, available at <http://justsecurity.org/1042/internet-backbone-pen-registers-constitutional/>.

Courts have reached the same conclusion with respect to certain internet information that is captured by a pen-trap, particularly that employed here. For example, in *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2007), the Court postulated that

> [s]urveillance techniques that enable the government to determine not only the IP addresses that a person accesses but also the uniform resource locators ("URL") of the pages visited might be more constitutionally problematic. A URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person's Internet activity. For instance, a surveillance technique that captures IP addresses would show only that a person visited the New York Times' website at http://www.nytimes.com, whereas a technique that captures URLs would also divulge the particular articles the person viewed. ("[I]f the user then enters a search phrase [in the Google search engine], that search phrase would

> appear in the URL after the first forward slash. This would reveal content . . . .").

Id., at 510 n. 6. *See also In re U.S. for an Order Authorizing the Use of a Pen Register and Trap on [xxx] Internet Service Account/User Name [xxxxxxx@xxx.com]*, 396 F. Supp. 2d 45, 49 (D. Mass 2005) ("[a] user may visit the Google site. . . . [I]f the user then enters a search phrase, that search phrase would appear in the URL after the first forward slash. This would reveal content . . . . The substance and meaning of the communication is that the user is conducting a search for information on a particular topic") (internal quotation marks omitted).

Indeed, even senior government intelligence officials concede that metadata *is* content. *See, e.g.,* Spencer Ackerman, "NSA Review Panel Casts Doubt On Bulk Data Collection Claims," *The Guardian*, January 14, 2014, available at <http://www.theguardian.com/world/2014/jan/14/nsa-review-panel-senate-phone-data-terrorism> (quoting former Deputy CIA Director Mike Morrell's testimony before the Senate Judiciary Committee that "[t]here is quite a bit of content in metadata"). *See also* Bruce Schneier, https://www.schneier.com/blog/archives/2013/09/metadata_equals.html (taking the position that metadata equals surveillance).

In fact, in *Smith*, Justice Stewart made that very point in his dissent, that phone numbers dialed constitute *content*. 442 U.S. at 750-51 (Stewart, J., *dissenting*). *See also Davis*, 2014 WL 2599917 (noting that aggregation of information can create content from otherwise non-substantive information, thereby invading privacy in a manner violative of the Fourth Amendment). Thus, even if *Smith* were not functionally eclipsed by *Riley*, *Jones*, and *United States v. Davis* (discussed in detail **post**), and therefore ripe for revisiting, it describes a primitive

methodology that bears little, if any genuine, resemblance to what the pen register and trap and trace accomplished in this case.

Moreover, the use of the pen-trap devices to establish Mr. Ulbricht's internet activity in conjunction with his physical location is the functional equivalent of geo-locating, which could violate the Communications Assistance for Law Enforcement Act (hereinafter "CALEA"), which at 47 U.S.C. §1002(a), in the context of requiring telecommunications carriers to make their equipment accessible for government electronic surveillance, provides the following caveat: "with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in 18 U.S.C. § 3127), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number[.]"

Here, the pen-trap Orders were "hybrids," procured through a combination of authorities – §3127 as well as 18 U.S.C. §2703(d) of the Stored Communications Act (hereinafter "SCA") – and were not authorized exclusively pursuant to §3127. However, that resort to the SCA constitutes mere semantics, and violates the spirit of CALEA, which was designed to foreclose real-time locating (as opposed to the SCA, which supposedly targets historical stored information).

Indeed, such "hybrids" have been disfavored by a number of courts. *See, e.g., In re Application*, 396 F. Supp.2d 747 (S.D. Tex. 2005); *In re Application of U.S. for Order*, 497 F.Supp.2d 301, 302 (D.Puerto Rico 2007) (rejecting application by government for "orders under 18 U.S.C. §§2703 and 3122, . . . for the installation and use of pen register and trap and trace devices, Enhanced Caller ID special calling features, and the capture of limited geographic or cell

site information, all for a period of sixty days from the date of the order"). *See also In re Application*, 2006 WL 1876847 (N.D.Ind. July 5, 2006); *In re Authorizing the Use of a Pen Register*, 384 F. Supp. 2d 562, 564 *on reconsideration sub nom. In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005) (initial case holds cell site location information which the government seeks "*is* information that a pen register or trap and trace device does, by definition, provide, but it is *not* information that the government may lawfully obtain absent a showing of probable cause"); *In re Applications of U.S. for Orders Authorizing Disclosure of Cell Cite Info.*, 05-403, 2005 WL 3658531 (D.D.C. Oct. 26, 2005) (stating that Magistrate Judges will not "grant applications for orders authorizing the disclosure of cell site information pursuant to 18 U.S.C. § 2703, 18 U.S.C. §§ 3122 and 3123, or both" absent new authority and ordering any such applications to be returned to the attorneys).

Also, courts have been unreceptive to applications for pen-traps used for the purpose of ascertaining location. *See In re U.S. for an Order: (1) Authorizing Installation & Use of Pen Register & Trap & Trace Device; (2) Authorizing Release of Subscriber & Other Info.; (3) Authorizing Disclosure of Location-Based Servs.*No. 07-128, 2007 WL 3342243 (S.D. Tex. Nov. 7, 2007) ("Assistant United States Attorney 'request[ed] an Order authorizing the [DEA] to require the [cell phone] Provider to disclose location-based data that will *assist law enforcement in determining the location of the Target Device*[,]" (emphasis added), prompting Court to conclude that "[t]he information that the Government seeks clearly attempts to identify the exact location of the Target Device (and presumably the person holding the Target Device), and thus requires a finding of probable cause"); *In re U.S. For an Order Authorizing the Disclosure of*

Prospective Cell Site Info., 412 F. Supp. 2d 947, 958 (E.D. Wis. 2006) *aff'd,* 06-MISC-004, 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006) (disagreeing with a prior SDNY case, *In re Application of the United States of America for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace*, 405 F.Supp.2d 435 (S.D.N.Y.2005), that a pen-trap with some other authority like the SCA could be sufficient to allow for geo-locating, and stating that "[t]he bottom line is that the array of statutes invoked by the issues in this case, *i.e.*, the Pen/Trap Statute, the SCA, and CALEA present much more a legislative collage than a legislative mosaic. If Congress intended to allow prospective cell site information to be obtained by means of the combined authority of the SCA and the Pen/Trap Statute, such intent is not at all apparent from the statutes themselves.").

In addition, the applications for the pen-traps in this case did not reveal to the issuing magistrate judges the true purpose – attempting to triangulate Mr. Ulbricht's internet activity in conjunction with his physical location and administrative interaction on the Silk Road Servers – beyond the rudimentary certification that the information sought was relevant to a criminal investigation of Mr. Ulbricht. *See, e.g.*, Exhibit 3, at ¶ 10.

Ultimately, *Jones* now combined with *Riley* renders prior conflicting decisions moot, as here there is not any functional distinction between the information protected in *Jones* and *Riley* (or *Davis*) and that the government obtained here through the pen-traps without benefit of a warrant. The protection afforded cell phones in *Riley* is only amplified with respect to laptops, and the geo-locating sought in *Davis* under the very same authority as used here – the order, rather than warrant, provisions of the SCA – is in practical terms indistinguishable from what the government sought to achieve here with the pen-trap devices.

Also, as noted **ante**, the Courts in *Jones* and *Riley* did not consider *Smith* an obstacle despite the fact that in both cases a third-party provider had access to the information sought (including, in *Wurie*, call logs, *see* 134 S. Ct. at 2492-93), and the customer/defendant had "voluntarily" surrendered the privacy of that information to the provider.

More explicitly, Justice Sotomayor, in concurring in *Jones*, challenged the continued vitality of the third-party records doctrine underlying *Smith*:

> [m]ore fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. *E.g., Smith* [*v. Maryland*], 442 U.S. [735], at 742 [(1979)]; *United States v. Miller,* 425 U.S. 435, 443, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice Alito notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," *post,* at 962, and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

Jones, 132 S. Ct. at 957 (Sotomayor, J., concurring).

Already, in *Davis*, the lower courts are taking heed. In *Davis*, the Eleventh Circuit held that the government required a warrant to obtain historical cell-site information that previously

had been accessible simply by an order pursuant to 18 U.S.C. §2703(d) (as opposed to §2703(c)(A), which provides authority for obtaining a warrant).

As the Court in *Davis* pointed out, §2703(d) "does not require probable cause, but only a showing 'that there are *reasonable grounds to believe* that the . . . records or other information sought, are relevant and material to an ongoing criminal investigation.'" 2014 WL 2599917, at *3 (emphasis added).

In analyzing whether that standard was sufficient under the Fourth Amendment, the Court in *Davis* concluded that "[i]n light of the confluence of the three opinions in the Supreme Court's decision in *Jones,* we accept the proposition that the privacy theory is not only alive and well, but available to govern electronic information of search and seizure in the absence of trespass." *Id*., at *8.

Continuing its analysis, the Court in *Davis* reasoned that

> [t]herefore, it cannot be denied that the Fourth Amendment protection against unreasonable searches and seizures shields the people from the warrantless interception of electronic data or sound waves carrying communications. The next step of analysis, then, is to inquire whether that protection covers not only content, but also the transmission itself when it reveals information about the personal source of the transmission, specifically his location. The Supreme Court in *Jones* dealt with such an electronic seizure by the government and reached a conclusion instructive to us in the present controversy.

Id., at *5.

In *Davis*, too, the Court eschewed any constraint *Smith* might impose, even in a clearly non-trespassory context. Thus, even if *Smith* survives as a technical matter of *stare decisis* (because it has not been formally overruled), technology, time, and the trio of decisions – *Riley* and *Jones* in the Supreme Court, and *Davis* in the Eleventh Circuit – have superseded it for

practical purposes. *See Jones*, 132 S. Ct. at 954 ("[i]t may be that achieving the same [tracking] result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question").

Moreover, the results in those cases provide clear guidance rather than ambiguity and confusion that is generated by legal doctrine that fails to keep pace with technology and the prevailing social environment it creates. As the Court noted in *Riley*, the government's "proposals would conflict with 'our general preference to provide clear guidance to law enforcement through categorical rules. "[I]f police are to have workable rules, the balancing of the competing interests . . . 'must in large part be done on a categorical basis – not in an *ad hoc*, case-by-case fashion by individual police officers.'" 134 S. Ct. at 2491-92, *quoting Michigan v. Summers,* 452 U.S. 692, 705, n. 19 (1981) (in turn quoting *Dunaway v. New York,* 442 U.S. 200, 219–220 (1979) (White, J., concurring)). *See also* 134 S. Ct. at 2497 (Alito, J., *concurring in the judgment*) ("[w]hile the Court's approach leads to anomalies, I do not see a workable alternative. Law enforcement officers need clear rules regarding searches incident to arrest, and it would take many cases and many years for the courts to develop more nuanced rules. And during that time, the nature of the electronic devices that ordinary Americans carry on their persons would continue to change").

3. *The Warrants In the Investigation Constituted Impermissible General Warrants*

In *United States v. Kirschenblatt*, 16 F.2d 202 (2d Cir. 1926), Learned Hand pointed out that it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him." *Id*., at 203. *See also Riley*, 134 S. Ct. at 2490-91 (noting that if the person's pockets included a cell phone, there

would no longer be a difference except that the cell phone would expose *more* information to the government than a search of a residence).

Here, the government's seizures and searches represent the confluence of Judge Hand's observation and that of the Court in *Riley*: a wholesale, unlimited, and unrestrained rummaging through the entirety of Mr. Ulbricht's digital existence – and expressly and deliberately so. The result is nothing less than the paradigmatic, impermissible general warrant.

a. *The Facts Relevant to the Warrants At Issue*

The warrants that operated as general warrants can be categorized as follows:

(1) the warrants for the Jtan.com servers in Pennsylvania, alleged to be Silk Road's backup servers, did not include any limiting principles, thereby authorizing search of the *entire* server(s). Yet the applications failed to inform the issuing magistrate judge that (a) the commerce on Silk Road included legitimate transactions for legal goods and services, and these transactions were neither acknowledged nor segregated; and (b) many of the transactions in contraband did not violate U.S. law for jurisdictional or other, substantive reasons (for instance, involving buyer and seller operating in other countries, without any connection to the U.S., or in which the merchandise was not illegal at all).

(2) the pen-trap orders, discussed **ante**, too, failed to provide any minimization principles or attempts to confine the information collected to that for which there was an adequate basis;

(3) the warrants for the entirety of Mr. Ulbricht's laptop, and gmail and Facebook accounts expressly included materials and information for which probable cause

did not exist, and licensed the very type of unrestrained rummaging that motivated the Framers to create the Fourth Amendment.

This section will concentrate on the latter warrants, which, in the context of general warrants, are the most egregious. Indeed, they are the paradigm of a general warrant not only in execution, but also in design, language, and purpose. For example, the warrant for the laptop sought, and received, authorization to search for the following (with only the most patently offending paragraphs cited herein):

> 44. The SUBJECT COMPUTER is also likely to contain evidence concerning ULBRICHT relevant to the investigation of the SUBJECT OFFENSES, including evidence relevant to corroborating the identification of ULBRICHT as the Silk Road user "Dread Pirate Roberts," including but not limited to:
>
> a. any communications or writings by Ulbricht, which may reflect linguistic patterns or idiosyncracies associated with "Dread Pirate Roberts"[] or political/economic views associated with "Dread Pirate Roberts" *(e.g.,* views associated with the Mises Institute);
>
> c. any evidence concerning Ulbricht's travel or patterns of movement, to allow comparison with patterns of online activity of "Dread Pirate Roberts" and any information known about his location at particular times
>
> h. any other evidence implicating ULBRICHT in the SUBJECT OFFENSES.

See Exhibit 11, at ¶ 44 (footnote omitted).

The footnote to ¶ 44(a) provided the only detail, but even that did not provide a limiting principle, as it targeted something that would require detailed review of *everything* Mr. Ulbricht has ever written:

> For example, "Dread Pirate Roberts" is known often to begin sentences with "Yea" – distinct from the usual spelling of the word, "Yeah." ULBRICHT is also known to favor this spelling of the word; for instance, his username on YouTube is "ohyeaross." The SUBJECT PREMISES is expected to contain writings or

> communications that will allow for similar linguistic comparisons between ULBRICHT and "Dread Pirate Roberts."

Id., at ¶ 44(a) n. 21.

The deliberate intention to review *everything* was further manifest from Attachment B to the warrant, which included authority to search the laptop for

> 2. Any evidence concerning ROSS WILLIAM ULBRICHT relevant to the investigation of the SUBJECT OFFENSES, including but not limited to:
>
> a. any communications or writings by ULBRICHT;
>
> c. any evidence concerning ULBRICHT'S travel or patterns of movement;

Id., at Attachment B.

Moreover, the warrants for Mr. Ulbricht's gmail and Facebook accounts were similarly without boundaries. *See* Exhibits 13 and 14. Thus, the entirety of Mr. Ulbricht's private "papers," and more (*i.e.*, his internet history, political or other associations) were expressly targeted by the government.[21]

That *defines* the very general warrants that attracted the ire of the Framers. *See* **ante**, at14-17. As the cases discussed below demonstrate, the Fourth Amendment's particularity requirement was designed to prevent such searches. Here, the abrogation of the particularity requirement mandates suppression.

---

[21] In another high profile British case that attracted the colonists' attention, *Wilkes v. Wood*, 19 How. St. Tr. 1153, 1156 (1763), John Wilkes, a member of Parliament was subject to an unrestricted search in which those conducting it"fetched a sack and filled it" with Wilkes's private papers. The celebrated Lord Camden noted that when those performing the search balked at taking all of Wilkes's papers, Lord Halifax ordered that "all must be taken, manuscripts and all."

b. *Digital Communications Are Protected By the Fourth Amendment*

In *United States v. Warshak*, 631 F.3d 266, 285-86 (6th Cir. 2010), the Sixth Circuit concluded that email is "is the technological scion of tangible mail" and that it would "defy common sense to afford emails lesser Fourth Amendment protection." In so ruling, the court also explicitly rejected the argument that a service provider's ability or right to access the content of email should somehow defeat the communicants' Fourth Amendment privacy interest.

Instead, *Warshak* likened service providers to "the functional equivalent of a post office or a telephone company," which the police may not simply storm to read a letter. *Id*., at 286. The Sixth Circuit relied on the Supreme Court's decision in *City of Ontario v. Quon*, 560 U.S. 746, 762-63 (2010), involving text messages sent and received on a government employee's pager ("implying that 'a search of [an individual's] personal e-mail account' would be just as intrusive as 'a wiretap on his home phone line'"), and the Ninth Circuit's decision in *United States v. Forrester*, 512 F.3d 500, 511 (2008) ("holding that '[t]he privacy interests in [mail and email] are identical'").

Yet here the searches of Mr. Ulbricht's laptop and gmail and Facebook accounts were far *more* intrusive than a Title III wiretap, which requires minimization procedures aimed at limiting recording to those conversations that are pertinent to the investigation for which the wiretap was authorized.

c. *The Overriding Importance of the Particularity Requirement*

The critical importance of the particularity requirement in preserving Fourth Amendment rights and protections in the digital age has been recognized by the courts. In *United States v. Galpin*, 720 F.3d 436 (2d Cir. 2013), the Court observed that

> [w]here, as here, the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance. As numerous courts and commentators have observed, advances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain.

Id., at 447, *citing United States v. Payton,* 573 F.3d 859, 861–62 (9th Cir.2009) ("[t]here is no question that computers are capable of storing immense amounts of information and often contain a great deal of private information. Searches of computers therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers.") (other citation omitted) (footnote omitted). *See also United States v. Ganias*, ---- F.3d ----, 2014 WL 2722618 (2d Cir. June 17, 2014); *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009); Orin S. Kerr, *Searches and Seizures in a Digital World,* 119 Harv. L.Rev. 531, 569 (2005).

In fact, in *Ganias* and *Galpin* the Second Circuit has twice reversed convictions and suppressed evidence because of violations of the particularity requirement. In *Ganias*, the Court noted that the particularity requirement "makes general searches . . . impossible" because it "prevents the seizure of one thing under a warrant describing another." 2014 WL 2722618, at *7, *quoting Galpin*, 720 F.3d at 446 (*quoting Marron v. United States,* 275 U.S. 192, 196 (1927)) (internal quotation marks omitted). This restricts the Government's ability to remove all of an individual's papers for later examination because it is generally unconstitutional to seize any item not described in the warrant. *See Horton v. California,* 496 U.S. 128, 140 (1990).

Nor is the protest here about the initial seizure of hard drives via imaging for off-site

review. *Ganias* has already noted that such a procedure is "constitutionally permissible." 2014 WL 2722618, at *8. Rather, it is the lack of any limiting standards or procedures in that review. Indeed, the language cited above from the applications and warrants manifests the opposite intent: a detailed review of every piece of digital information.

Ganias addressed a limited issue, "whether the Fourth Amendment permits officials executing a warrant for the seizure of particular data on a computer to seize and indefinitely retain every file on that computer for use in future criminal investigations," *id*., at *10, but nevertheless recognized that "computer files may contain intimate details regarding an individual's thoughts, beliefs, and lifestyle, and they should be similarly guarded against unwarranted Government intrusion. If anything, even greater protection is warranted." *Id*., at *7, *citing* Kerr, *Searches and Seizures in a Digital World,* 119 Harv. L.Rev. at 569 (explaining that computers have become the equivalent of "postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more").

Here, the government expressly seeks unfettered access to precisely the type of "papers" cited by the Court in *Ganias*: intimate details regarding Mr. Ulbricht's "thoughts, beliefs, and lifestyle," without any demonstration of probable cause to search *any* of those "papers."

Ganias followed *Galpin*, which a year earlier had explained that the purpose of the particularity requirement "is to minimize the discretion of the executing officer . . ." 720 F.3d at 446 n. 5, and pointed out that "[m]indful of that purpose, . . . other Circuits have held that even warrants that identify catchall statutory provisions, like the mail fraud or conspiracy statutes, may fail to comply with this aspect of the particularization requirement." *Id*., *citing United States v.*

Leary, 846 F.2d 592, 594 (10th Cir.1988) (warrant authorizing search of export company's business records for violation of the "Arms Export Control Act, 22 U.S.C. § 2778, and the Export Administration Act of 1979, 50 U.S.C.App. § 2410," held overbroad); *Voss v. Bergsgaard,* 774 F.2d 402 (10th Cir.1985) (warrant specifying 18 U.S.C. § 371, the general federal conspiracy statute, held overbroad); *United States v. Roche,* 614 F.2d 6, 8 (1st Cir.1980) (concluding that a limitation of a search to evidence relating to a violation of 18 U.S.C. § 1341, the general mail fraud statute, provides "no limitation at all").

In *Galpin*, the Court also recounted that it has "emphasized that 'a failure to describe the items to be seized with as much particularity as the circumstances reasonably allow offends the Fourth Amendment because there is no assurance that the permitted invasion of a suspect's privacy and property are no more than absolutely necessary.'" 720 F.3d at 446, *quoting United States v. George,* 975 F.2d 72, 76 (2d Cir.1992).

In language particularly germane here, the Court in *Galpin* cautioned that "[t]he potential for privacy violations occasioned by an unbridled, exploratory search of a hard drive is enormous[,]" and that "[t]his threat is compounded by the nature of digital storage." 720 F.3d at 446-47. The Circuit has thus far declined to impose the type of search protocols enumerated by Judge Kozinski in his concurring opinion in *United States v. Comprehensive Drug Testing, Inc.,* 621 F.3d 1162, 1176 (9th Cir.2010) (en banc) (per curiam). However, the Court in *Galpin* recognized "'a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant[,]'" and that "[t]his threat demands a heightened sensitivity to the particularity requirement in the context of digital searches." 720 F.3d at 447-48, *quoting Comprehensive Drug Testing*, 621 F.3d at 1176, and citing *United States*

v. Burgess, 576 F.3d 1078, 1091 (10th Cir.2009) ("If the warrant is read to allow a search of all computer records without description or limitation it would not meet the Fourth Amendment's particularity requirement").

In that context, the Court in *Galpin* instructed that upon remand the district court's review of the plain view issue should take into account the degree, if any, to which digital search protocols target information outside the scope of the valid portion of the warrant. To the extent such search methods are used, the plain view exception is not available." 720 F.3d at 451.

Here, again, no such limiting principles were instituted at all. In fact, the warrants herein invert the analysis in a manner that dissolves Fourth Amendment protections. Rather than require the government to establish probable cause in advance of reviewing categories of electronic data, they would license the government to examine *every* file to assure that probable cause to seize it did *not* exist. Any more dramatic or patent example of the "rummaging" attendant to general warrants could not be envisioned, yet that is what the government has done in this case most demonstrably with respect to Mr. Ulbricht's laptop and gmail and Facebook accounts, but in fact with respect to *every* search of ESI in this investigation.[22]

Regarding seizures of entire e-mail accounts, recently Magistrate Judge Gorenstein issued an opinion to address two opinions that denied the government access to an entire e-mail account. *See In the Matter of A Warrant for all Content and Other Information Associated With the Email Account xxxxx@Gmail.com Maintained at Premises Controlled By Google, Inc.*, 14 Mag. 309 2014 WL 3583529 (S.D.N.Y. July 18, 2014) (hereinafter "*Gmail*").

---

[22] *See NACDL Report*, at 12 ("[e]ven if every nook and cranny of a digital device could *theoretically* contain evidence covered by the warrant, it does not mean that every nook and cranny may *reasonably* contain such evidence." (Emphasis in original).

The two opinions to which his opinion was directed were *In the Matter of the Search of Information Associated with [Redacted] @mac.comthat is Stored at Premises Controlled by Apple, Inc*., not reported in F. Supp.2d, available at 2014 WL 1377793, at *8 n. 15 (D.D.C. April 7, 2014) (hereinafter "*Apple*") and *In the Matter of Applications for Search Warrants for Information Associated With Target Email Accounts/Skype Accounts*, not reported in F. Supp.2d, available at 2013 WL 4647554 (D. Kansas August 27, 2013) (hereinafter "*Skype*").

In *Apple*, the Court concluded the government sought a warrant that would be "unconstitutional because [t]he government simply has not shown probable cause to search the contents of all emails ever sent to or from the account." 2014 WL 1377793, at *5 (citation and internal quotes omitted). As a result, the Court reasoned, if it "were to grant the Renewed Application as it is, the government would immediately seize a vast quantity of e-mails to which it is not entitled; in so doing, this Court would issue a general warrant, which it cannot do." *Id*., at *6.

The Magistrate Judge in *Skype* reached the same conclusion, noting that "a warrant must describe the things to be seized with sufficiently precise language so that it informs the officers how to separate the items that are properly subject to seizure from those that are irrelevant." 2013 WL 4647554, at *5. The Court in *Skype* further pointed out that the warrants "failed to set out any limits on the government's review of the potentially large amount of electronic communications and information obtained from the electronic communications service provider[,]" and "do not identify any sorting or filtering procedures for electronic communications and information that are not relevant and do not fall within the scope of the government's probable cause statement, . . ." *Id*., at *8. *See also id*. ("[t]he government simply

has not shown probable cause to search the contents of all emails ever sent to or from the accounts or for all the information requested from the Providers").

The "carte blanche" the government sought but was denied in *Skype*, *see id*., at *9, was nevertheless provided here, and violated the Fourth Amendment. Nor does Magistrate Judge Gorenstein's opinion alter that analysis. In his opinion, Magistrate Judge Gorenstein permitted a search "for certain specific categories of evidence." *Gmail*, 2014 WL 3583529, at *1. That was not the case as no specific categories of evidence were listed. Instead, there was no definition at all, but rather an omnibus license.

Similarly, the principles cited in *Gmail* simply reinforce the lack of particularity with respect to the warrants at issue herein. For example, the warrants here do not permit mere "perusal" to determine relevance, as in *United States v. Mannino,* 635 F.2d 110, 115 (2d Cir.1980) (quoting *United States v. Ochs,* 595 F.2d 1247, 1257 n. 8 (2d Cir.1979)).

Nor do the warrants here seek merely a "cursory" review for purposes of determining relevance, as in *Andersen v. Maryland,* 427 U.S. 463, 482 n. 11, 96 S.Ct. 2737, 49 L.Ed.2d 627 (1976) ("[i]n searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized").

Indeed, the government has announced in the applications that it intends to perform various detailed analyses of the entirety of Mr. Ulbricht's communications and digital history. That guarantees that every piece of digital information will be subject to a detailed search in the absence of any probable cause to search any specific piece of ESI.

Nor is the principle that a warrant can seek and seize "mere evidence" availing to the government with respect to these warrants. *See Warden v. Hayden*, 387 U.S. 294 (1967). *Warden* involved a discrete set of physical objects – clothing and weapons directly related to the offense charged – that were easily identifiable, not a fishing expedition into the entirety of someone's communications and research history.

Also, in *Warden* the Court cautioned that "[t]here must, of course, be a nexus – automatically provided in the case of fruits, instrumentalities or contraband – between the item to be seized and criminal behavior." 387 U.S. at 300. Nor does the doctrine dispense with the particularity requirement. *Id.*, at 309-10.

Moreover, the explicit concentration on political opinions and association, and other constitutional rights such as travel, *see* Exhibit 11, at ¶ 44 (**ante**, at 50) implicates First Amendment freedoms in a very tangible fashion. As Justice Sotomayor warned in her concurrence in *Jones*, "[a]wareness that the Government may be watching chills associational and expressive freedoms." 132 S. Ct. at 956 (Sotomayor, J., *concurring*).

Nearly 60 years ago, Justice Douglas wondered of the impact of the very practice the government has conducted in this case with respect to these warrants:

> [t]he time may come when no one can be sure whether his words are being recorded for use at some future time; when everyone will fear that his most secret thoughts are no longer his own, but belong to the Government; when the most confidential and intimate conversations are always open to eager, prying ears. When that time comes, privacy, and with it liberty, will be gone. If a man's privacy can be invaded at will, who can say he is free? If his every word is taken down and evaluated, or if he is afraid every word may be, who can say he enjoys freedom of speech? If his every association is known and recorded, if the conversations with his associates are purloined, who can say he enjoys freedom of association? When such conditions obtain, our citizens will be

> afraid to utter any but the safest and most orthodox thoughts; afraid to associate with any but the most acceptable people. Freedom as the Constitution envisages it will have vanished.

Osborn v. United States, 385 U.S. 323, 353–54 (1966) (Douglas, J., *dissenting*). *See also Alliance to End Repression v. City of Chicago*, 627 F. Supp. 1044, 1054, 1056 (N.D. Ill. 1985) (recognizing that even if all of the individual "details of a person's life" are available publicly – as could be the case in the not-too-distant future – the recording of those details, as with public cameras or other surveillance technologies, "can only serve to stifle the very sort of lawful, robust dissent that the first amendment, from its inception, was intended to protect"); *Boyd v. United States*, 116 U.S. at 623 ("The search for and seizure of stolen or forfeited goods, or goods liable to duties and concealed to avoid the payment thereof, are totally different things from a search for and seizure of a man's private books and papers for the purpose of obtaining information therein contained, or of using them as evidence against him").

Here, the warrants expressly – even deliberately – fail to adhere to the Fourth Amendment's particularity requirement, and constitute general warrants. As a result, it is respectfully submitted that all evidence seized and/or searched pursuant to those warrants and orders, and all the fruits therefrom, should be suppressed.

POINT II

THE COURT SHOULD COMPEL THE GOVERNMENT TO PRODUCE THE REQUESTED DISCOVERY

The following discovery and information is necessary to assist defense counsel in determining whether any information gathered during the course of the government's investigation was obtained in violation of Mr. Ulbricht's rights pursuant to the Fourth

Amendment to the United States Constitution. In addition, the documents and data requested below are necessary to ensure Mr. Ulbricht's Sixth Amendment right to prepare a defense, and their disclosure is required pursuant to Rule 16, Fed.R.Crim.P.

Accordingly, Mr. Ulbricht requests an Order compelling the Government to produce the following discovery and other materials:

1. A list of IP addresses the government, including any branch of law enforcement in the U.S. or in any other country working with or sharing information with the U.S., or any private contractor, used to access or attempt to access the Silk Road servers;
2. Identify the person, persons, entity or entities associated with each "government" IP address;
3. The results of any and all network testing including, but not limited to, trace routes, IP address pings, penetration tests, and/or port scans which the government, including any branch of law enforcement in the U.S. or in any other country working with or sharing information with the U.S., or any private contractor, used to verify the existence of the Silk Road servers and/or conduct analysis of the Silk Road servers, in regard to their physical location, identifying information, and/or for any other purpose;
4. Any data and/or communications obtained from and/or involving the server hosts from which server images were obtained, including, but not limited to, any e-mails, letters, and server traffic logs;
5. Specify whether the government including any branch of law enforcement in

the U.S. or in any other country working with or sharing information with the U.S., or any private contractor, ever ran any "who is" queries to determine the location, host, service provider or IP address of the servers;

6. Identify any vulnerability scanning utilities used to detect vulnerabilities in the Silk Road servers and,

   a. the name any such utilities used;

   b. the dates and times of any such scans; and,

   c. the names of any exploits used including but not limited to names of technology, malware and hacking tools used;

7. Specify whether the government including any branch of law enforcement in the U.S. or in any other country working with or sharing information with the U.S., or any private contractor, used denial of service attacks on the Silk Road website or servers;

8. Identify the names of any TOR hidden service vulnerabilities the government including any branch of law enforcement in the U.S. or in any other country working with or sharing information with the U.S., or any private contractor, utilized during the course of the investigation;

9. Identify any information pertaining to TOR servers deployed by the government including any branch of law enforcement in the U.S. or in any other country working with or sharing information with the U.S., or any private contractor, during the course of the investigation;

10. Identify any public keys or addresses for any bitcoin wallets that were used by the

government, including any branch of law enforcement in the U.S. or in any other country working with or sharing information with the U.S., or any private contractor, for conducting this investigation;

11. Identify the dates, times, and usernames associated with any controlled buys conducted by law enforcement on the Silk Road website;

12. Identify a list of usernames and/or aliases that were used by law enforcement in the U.S. or in any other country working with or sharing information with the U.S., or any private contractor, on the Silk Road website at any time during the course of the investigation;

13. Identify any bitcoin addresses that the government, including any branch of law enforcement in the U.S. or in any other country working with or sharing information with the U.S., or any private contractor, knew or suspected was directly associated with or belonged to Ross Ulbricht;

14. Identify the means and methods the government, including any branch of law enforcement in the U.S. or in any other country working with or sharing information with the U.S., or any private contractor, used for tracing bitcoin transactions;

15. Identify any documents relating to any block chain analysis conducted by the government, including any branch of law enforcement in the U.S. or in any other country working with or sharing information with the U.S., or any private contractor, during the investigation;

16. Identify any transaction information, including, but not limited to, shipping address information, transaction IDs, buyer and seller identifications, and/or payment information obtained from the Silk Road server MYSQL and/or other databases with regard to the package intercepted from Canada;

17. Identify any information regarding methods or procedures in place for monitoring data entered into Silk Road server MYSQL and/or other databases, including, but not limited to, any tools or software used for this purpose;

18. Specify whether the government**,** including any branch of law enforcement in the U.S. or in any other country working with or sharing information with the U.S., or any private contractor, was aware at any point *prior* to the location of the servers overseas that there were servers located in the U.S.;

19. Identify the means and methods the government, including any branch of law enforcement in the U.S. or in any other country working with or sharing information with the U.S., or any private contractor, used to locate the Silk Road servers overseas;

20. Identify the contents of any and all MLAT requests related to this investigation; and,

21. Inquire of U.S. law enforcement and intelligence agencies with respect to whether any "parallel construction" has occurred in this investigation, and disclose any and all information regarding "parallel construction."

POINT III

THE COURT SHOULD COMPEL THE GOVERNMENT TO PRODUCE THE REQUESTED BILL OF PARTICULARS

As the Second Circuit has explained, a bill of particulars:

> is appropriate to permit a defendant "to identify with sufficient particularity the nature of the charge pending against him, thereby enabling defendant to prepare for trial, to prevent surprise, and to interpose a plea of double jeopardy should he be prosecuted a second time for the same offense."

United States v. Davidoff, 845 F.2d 1151, 1154 (2d Cir. 1988), *quoting United States v. Bortnovsky*, 820 F.2d 572, 574 (2d Cir. 1987). *See also United States v. Nachamie*, 91 F. Supp.2d 565, 570 (S.D.N.Y. 2000) (*quoting Bortnovsky*, 820 F.2d at 574) (ordering a Bill of Particulars).

Without further elucidation of the generic descriptions of the charges against him in the Indictment, Mr. Ulbricht will be unable to prepare his defense as he will not be able to isolate the specific transactions that he must defend against. Thus, Mr. Ulbricht's request for a bill of particulars should be granted.

A. *A Bill of Particulars Is Necessary for the Preparation of Mr. Ulbricht's Defense*

Absent a bill of particulars, Mr. Ulbricht will proceed to trial without sufficient notice of precisely what charges he faces, and without ample time to identify and locate witnesses and/or conduct a meaningful investigation of the offenses alleged. The Indictment alleges that the Silk Road "underground website" was "designed to enable users *across the world* to buy and sell illegal drugs and other illicit goods and services *anonymously*" and that "[t]he website was used by *several thousand* drug dealers and other unlawful vendors to distribute *hundreds* of kilograms

of illegal drugs and other illicit goods and services to *well over a hundred thousand* buyers *worldwide*, and to launder *hundreds of millions* of dollars deriving from these unlawful transactions." *See* Indictment at ¶1, 2 (emphasis added).

Moreover, the discovery produced thus far demonstrates that witnesses may be located in a number of countries, including the United Kingdom, Australia, Iceland, and France, and "elsewhere," and that transactions that occurred on the Silk Road may have occurred in locations all over the world. In this case, ordinary and efficient investigation is impeded by a number of traditional factors (*i.e.*, language, culture, and governmental authority) beyond counsel's control, but also uniquely by the sheer volume and seemingly impenetrable anonymity of the transactions that took place on the Silk Road site and the persons involved in these transactions, which defy any effort counsel could make to determine the precise volume of transactions and potential witnesses involved, let alone the specifics of any of these transactions or the locations they occurred in, or in which their alleged participants reside. Consequently, learning important particulars immediately before, or even during trial, will effectively preclude *any* defense investigation, or ability to prepare adequately, with respect to those issues.

As a result, a bill of particulars is necessary to inform Mr. Ulbricht of the specific elements of the charged conspiracies and substantive offenses, including, in key part (1) particularization and enumeration of specific transactions the Indictment describes in undefined or only general terms; and (2) the manner of, contents of, and parties involved in, the communications alleged. If Mr. Ulbricht is not provided with a bill of particulars, his ability to prepare his defense will be irremediably impaired.

1. *The Government Must Particularize Transactions the Indictment Describes In Undefined or Only General Terms*

The Indictment in Mr. Ulbricht's case is scant on details and speaks only in broad and undefined terms, thus boiling a complex, multi-transactional case down to sweeping generalities that provide no specifics and no roadmap to the charges Mr. Ulbricht will be required to defend against. *See* Indictment at ¶ 2 ("[t]he website was used by several thousand drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs and other illicit goods and services to *well over a hundred thousand buyers worldwide*, and to launder hundreds of millions of dollars deriving from these unlawful transactions"); ¶ 12 ("violations were part of a continuing series of violations of the Controlled Substance Act"); ¶ 14 ("[w]hile in operation, the Silk Road website regularly offered hundreds of listings for [malicious software] products"); ¶ 21 ("the defendant, and others known and unknown . . . would and did conduct financial transactions, which in fact involved the proceeds of specified unlawful activity"). Descriptions in the Indictment routinely omit necessary details such as (1) locations, dates, times, and precision as to the volume of that transactions occurred; (2) the parties involved in transactions; and (3) the definitions of terms or words, such as "illicit goods and services," that characterize the transactions.

In *United States v. Bin Laden (El-Hage)*, 92 F. Supp.2d 225 (S.D.N.Y. 2000), Judge Sand explained that "a bill of particulars [was] necessary . . . to permit the Defendants to prepare a defense and to prevent prejudicial surprise at trial," based, in part, on the Court's conclusion that "several of the allegations contained in the 'Overt Acts' section of the Indictment are cast in terms that are too general, in the context of [that] particular case, *to permit the Defendants to conduct a*

meaningfully directed investigation of the relevant facts and circumstances and be prepared to respond to the charges." *Id*., at 235 (emphasis added).

In Mr. Ulbricht's case, only one of the conspiracies charged even contains a list of overt acts, and these, for Count One, do not relate to the multitude of transactions alluded to in that count and include entirely extraneous details, such as the "murder-for-hire" allegations that are the subject of Mr. Ulbricht's motion to strike irrelevant and prejudicial surplusage. Accordingly, the transactions described in Count One and the Indictment as a whole lack specificity, and without the details requested by Mr. Ulbricht, such as geographical locations, dates, times, participants, and particularization of acts alleged, it would be impossible for Mr. Ulbricht "to conduct a meaningfully directed investigation."

Moreover, due to the essentially global nature of the transactions in this case, if Mr. Ulbricht is not notified of these particulars sufficiently in advance of trial, he will be unable, at the eleventh hour, to mount a defense based on witnesses, documents, and/or other information that can be procured and produced only through rather challenging, if feasible at all, international investigation and travel. Under such circumstances, his ability to prepare and present a defense would be irreparably impaired. *See Bin Laden (El-Hage)*, 92 F. Supp.2d at 234-36.[23]

Nor does the albeit voluminous discovery in this case provide a roadmap for the alleged transactions that would obviate the need for a bill of particulars.

As this Court stated last year in *United States v. Mostafa*, 965 F.Supp.2d 451, 465 (S.D.N.Y. 2013), "a bill of particulars is . . . unnecessary when the Government has produced

[23] The unsatisfactory alternative, of course, is a last-minute delay of the trial, or substantial continuance(s) once it begins, in order to permit Mr. Ulbricht to rebut evidence he should be permitted to prepare for *now*.

materials in discovery concerning the witness and other evidence" and "[t]hus, in determining whether to order a bill of particulars a court must examine the totality of the information available to the defendant, both through the indictment and through pre-trial discovery." *See also Bin Laden*, 92 F. Supp.2d at 233.

Bortonovsky is instructive in conducting this examination in Mr. Ulbricht's case in that the defendant in *Bortonovsky* was faced with a similar situation to that which Mr. Ulbricht faces here: the government refused to respond to a bill of particulars request from the defendant in his insurance fraud case despite the fact that "[n]owhere in the indictment . . . d[id] the Government specify the dates of the staged burglaries or enumerate which of numerous documents were falsified" on the basis that "it fulfilled its obligation to inform [defendants] of the charges by being explicit in the indictment and by providing over 4,000 documents to defense counsel during discovery." *Id*., at 574.

In *Bortonovsky*, the Court found that the defendants "were hindered in preparing their defense by the district court's failure to compel the Government to reveal crucial information: the dates of the fake burglaries and the identity of the three fraudulent documents." *Id*., at 574. The Court also found that the "Government did not fulfill its obligation merely by providing mountains of documents to defense counsel who were left unguided as to which documents would be proven falsified or which of some fifteen burglaries would be demonstrated to be staged." *Id*., at 575. The Court in *Bortonovsky* ultimately concluded that as a result of the government's failure to reveal crucial information and the district court's failure to require it, "[i]n effect, the burden of proof impermissibly shifted to [the defendants]." *Id.*, at 575.

Indeed, if Mr. Ulbricht is not provided a bill of particulars in this case he will suffer the same fate. He cannot possibly be expected to parse through multiple terabytes of discovery in the hopes that he will guess correctly as to the transactions that the government intends to put before the jury, nor does the veiled nature of the case itself even allow for such an inquiry to take place.

Accordingly, "to avoid surprise at trial and give [Mr. Ulbricht] sufficient information to meet the charges against him" as this Court stated was the very purpose of a bill of particulars, the Court must Order the government to provide the requested bill of particulars to Mr. Ulbricht. *See Mostafa*, 965 F.Supp.2d at 465, *citing Bin Laden*, 92 F. Supp.2d at 233.

2. *The Government Must Identify the Contents Of, and Parties Involved In, the Communications Alleged*

The identification of the manner in which communications occurred, as well as the specific persons involved in them, and their contents, alleged in the Indictment, are equally critical to preparation of Mr. Ulbricht's defense. As with the transactions alleged in the Indictment, the global nature of charges and thus potentially of the alleged communications, present unique problems for Mr. Ulbricht's defense. Also, the precise nature by which communications were alleged to have occurred is equally important to preparation, as that requires investigation, and potentially acquisition of documentary evidence and expert forensic analysis.

In the absence of a bill of particulars providing the requested details of these communications, defense counsel will not have ample time to identify and locate necessary witnesses and other evidence that may be obtainable only through international investigation and travel, or subpoena.

It should also be noted that material disclosed pursuant to discovery demands and 18 U.S.C. §3500, does not serve as a substitute for a bill of particulars. *See, e.g., Davidoff*, 845 F.2d

at 1155. This is especially true with regard to communications, and the transactions discussed **ante**, since late notice (such as via production of "3500 material") might require postponement of the trial in order to allow Mr. Ulbricht's defense team to pursue the evidence in remote and difficult locations. *See also* **ante**, at n. 23.

B. ***The Requested Particulars***

The Court should compel the government to provide the following particulars:[24]

1. With respect to Count One, ¶ 1, please identify:

   a. "users across the world" by name, Silk Road username, any other identifier, and location; and

   b. the specific nature of the "other illicit goods and services."

2. With respect to Count One, ¶ 2, please identify:

   a. the specific dates upon which Mr. Ulbricht is alleged to have "owned" the Silk Road website;

   b. the specific dates upon which Mr. Ulbricht is alleged to have "operated" the Silk Road website ; and

   c. by name, Silk Road username, location, any other identifier, and item(s) distributed, the "several thousand drug dealers and other unlawful vendors."

3. With respect to Count One, ¶ 3, please identify:

[24] Counsel requested a Bill of Particulars from the government July 31, 2014, and attempted to informally resolve this discovery matter as required by Local Criminal Rule 16.1. The government conveyed to counsel that same day by e-mail that it would not provide any of the requested particulars on the basis that "you have all the particulars you need in the complaint, indictment, and discovery."

a. by name, Silk Road username, any other identifier, and role the "various paid employees" Mr. Ulbricht is alleged to have "managed and supervised" as well as the amounts, frequency, nature and dates of payment;

b. the type of "assistance" each of these "paid employees" allegedly provided;

c. the "aspects of Silk Road" Mr. Ulbricht is alleged to have "controlled;" and

d. the nature and amount of the "commissions" Mr. Ulbricht is alleged to have "reaped" from the "illicit sales conducted through the site" and the specific "illicit sale," including date, time and location, that each "commission" was for.

4. With respect to Count One, ¶ 4, please identify:

a. each of the "violent means" Mr. Ulbricht is alleged to have "pursued" by date, time, location and nature of the conduct;

b. the date, time, location and nature of any alleged "solicitat[ations]" to execute a "murder-for-hire;"

c. by name, Silk Road username if applicable, and any other identifier, the "several individuals" Mr. Ulbricht allegedly "solicit[ed] the murder-for-hire" of; and

d. the nature of the "threat" each of these individuals allegedly posed.

5. With respect to Count One, ¶ 5, please identify:

a. all locations encompassed by the term "elsewhere;"

b. the date on which it is alleged that Mr. Ulbricht first became a member of the conspiracy charged in Count One;

c. the "others" by name, name, Silk Road username, any other identifier and location; and

d. by date, time, location and nature, any specific acts performed by Mr. Ulbricht in furtherance of the conspiracy charged in Count One.

6. With respect to Count One, ¶ 6, please identify:

a. the "others" by name, Silk Road username, any other identifier, and location; and

b. the nature of the "controlled substances" allegedly "distributed."

7. With respect to Count One, ¶ 7, please identify:

a. the "others" by name, Silk Road username, any other identifier, and location;

b. the nature of the "controlled substances" allegedly "deliver[ed], distribute[d], and dispense[d];"

c. the precise "means" by which the "controlled substances" were allegedly "deliver[ed], distribute[d], and dispense[d];" and

d. any role played by Mr. Ulbricht in these alleged transactions, including date, time, location and nature of the role.

8. With respect to Count One, ¶ 8, please identify:

a. the nature of the "communication facility;" and

b. the date, time, location and nature of any specific "acts" that constituted the alleged felonies.

9. With respect to Count One, ¶ 9, please identify the "others" by nature of controlled substance and volume.

10. With respect to Count One, ¶ 10, please identify:

a. all locations encompassed by the term "elsewhere;"

b. the time, date and location of each of the overt acts committed in the Southern District of New York; and

c. the time, date and location of each of the overt acts committed "elsewhere."

11. With respect to Count One, ¶ 10(a), please identify:

a. by name, Silk Road username, any other identifier and location each of the "drug dealers around the world" that Mr. Ulbricht allegedly provided a "platform" for; and

b. by type the "variety of controlled substances" each "drug dealer" allegedly sold.

12. With respect to Count One, ¶ 10(b), please identify:

a. the specific date, time, location, medium, and nature of the alleged "solicit[ation];"

b. by name, Silk Road user name, and any other identifier the "Silk Road user" allegedly "solicited" to "execute a murder-for-hire of another Silk Road user;"

c. by name, Silk Road user name, and any other identifier, the "Silk Road user" that was the alleged target of the "murder-for-hire;"

d. the precise time, date, location and nature of the alleged "threat[] to release the identities of thousands of users of the site;" and

e. by name, Silk Road user name, and any other identifier the "thousands of users of the site."

13. With respect to Count One, ¶ 10(c), please identify the specific date, time, and location from which Mr. Ulbricht allegedly "logged on as a site administrator to the web server hosting the Silk Road website."

14. With respect to Count Two, ¶ 12, please identify:

a. all locations encompassed by the term "elsewhere;"

b. by time, date and location any alleged acts committed by Mr. Ulbricht in the Southern District of New York;

c. by time, date and location any alleged acts committed by Mr. Ulbricht "elsewhere;"

d. by time, date, location, participants, and controlled substance, the specific transactions that "were part of a continuing series of violations of the Controlled Substance Act" that were allegedly "undertaken by ULBRICHT;"

e. by name, Silk Road user name, and any other identifier, any and all of the "at least five other persons with respect to whom ULBRICHT occupied a position of organizer, a supervisory position, and a position of management;" and

f. whether Mr. Ulbricht "occupied a position of organizer, a supervisory position" and/or "a position of management with respect to each individual.

15. With respect to Count Three, ¶ 14, please identify:

a. by name, type, brand, and any other identifier the specific "malicious software" that the Silk Road website allegedly "provided a platform for the purchase and sale of;"

b. the specific details including date, time, location, participants, and type of product involved in each "purchase and sale" alleged to constitute a violation pursuant to Count 3; and

c. the nature of the "platform" provided.

16. With respect to Count Three, ¶ 15, please identify:

a. all locations encompassed by the term "elsewhere;"

b. the date on which it is alleged that Mr. Ulbricht first became a member of the conspiracy charged in Count Three;

c. the "others" by name, Silk Road username, any other identifier and location; and

d. by date, time, location and nature, any specific acts performed by Mr. Ulbricht in furtherance of the conspiracy charged in Count Three.

17. With respect to Count Three, ¶ 16, please identify:

a. the "others" by name, Silk Road username, any other identifier and location;

b. the time, date and location of any alleged unauthorized access of any computer and the identifying information for the computer accessed;

c. the precise nature of the "information" allegedly obtained "from protected computers;" and

d. the specific nature of the "commercial advantage" or "private financial gain" derived from each unauthorized access alleged.

18. With respect to Count Four, ¶ 18, please identify:

a. the specific nature of the "illegal commerce conducted on the site;" and

b. the "users" by name, Silk Road username, and any other identifier whose identities Mr. Ulbricht allegedly sought to conceal; and

c. the "users" by name, Silk Road username, and any other identifier who "transmitt[ed] and receiv[ed] funds through the site."

19. With respect to Count Four, ¶ 19, please identify:

a. all locations encompassed by the term "elsewhere;"

b. the date on which it is alleged that Mr. Ulbricht first became a member of the conspiracy charged in Count Four;

c. the "others" by name, Silk Road username, any other identifier and location; and

d. by date, time, location and nature, any specific acts performed by Mr. Ulbricht in furtherance of the conspiracy charged in Count Four.

20. With respect to Count Four, ¶ 20, please identify:

a. the "others" by name;

b. the specific nature, time, date and location of each of the "financial transactions" alleged to involve the "proceeds of specified unlawful activity;

c. the specific nature of the "unlawful activity" allegedly involved in each transaction;

d. the specific type of "property" involved in each transaction; and

e. the role, if any, that Mr. Ulbricht allegedly played in each and any transaction.

21. With respect to Count Four, ¶ 21, please identify:

a. the "others" by name;

b. the specific nature, time, date and location of each of the "financial transactions" alleged to involve the "proceeds of specified unlawful activity;

c. the specific nature of the "unlawful activity" allegedly involved in each transaction;

d. the specific type of "property" involved in each transaction; and

e. the role, if any, that Mr. Ulbricht allegedly played in each and any transaction.

22. With respect to the forfeiture allegations, at ¶ 22, please identify:

a. the amount and nature of the "property" subject to forfeiture and basis upon which it is subject to forfeiture; and

b. whether any such property was obtained "directly or indirectly, as a result of the offense."

23. With respect to the forfeiture allegations, at ¶ 23, please identify:

a. the value and nature of the "property" subject to forfeiture and basis upon which it is subject to forfeiture; and

b. whether any such property was obtained "directly or indirectly, as a result of the offense."

24. With respect to the forfeiture allegations, at ¶ 24, please identify:

a. the value and nature of the "property" subject to forfeiture and basis upon which it is subject to forfeiture;

b. the value and nature of any "real" property;

c. the value and nature of any "personal" property; and

d. the value and nature of "any property traceable to such property" and the precise "property" it is "traceable to."

POINT IV

THE COURT SHOULD STRIKE IRRELEVANT AND PREJUDICIAL SURPLUSAGE FROM THE INDICTMENT

The Indictment in this case contains surplusage that is both irrelevant to the charges and/or unduly prejudicial to the defendant, in that (1) Count One of the Indictment includes extraneous, inflammatory and unduly prejudicial references to uncharged "murder-for-hire" allegations contained only in a separate case against Mr. Ulbricht in the District of Maryland ; (2) Count

Three of the Indictment refers to "password stealers, keyloggers, and remote access tools" as "malicious software designed for computer hacking" which is both extraneous and highly prejudicial because it provides a biased and incomplete characterization of the true nature of those devices; and (3) the Indictment is peppered throughout with impermissible broadening phrases, such as "others known and unknown," "among others," and elsewhere."

By inserting references in ¶¶ 4 & 10(b) of the Indictment, to the inflammatory and highly prejudicial "murder-for-hire" allegations charged in the separate District of Maryland case against Mr. Ulbricht, the government improperly seeks to tie Mr. Ulbricht to conduct that was not brought before a grand jury in New York, and thus to improperly influence the jury to convict him here on the basis of that uncharged conduct. Nor is this alleged conduct an element of Count One, or any crime charged in the Indictment. As established **post**, *any* reference to the "murder for hire" allegations is irrelevant to the offenses charged in Count One, and therefore unduly prejudicial.

The government's characterization of "password stealers, keyloggers, and remote access tools" as "malicious software designed for computer hacking" in Count Three, ¶ 14 of the Indictment, unduly prejudices Mr. Ulbricht by improperly suggesting to the jury that these devices can only be used nefariously, a fact which the government must prove at trial, and undermined by the government's recent endorsement of the use of malware.

Broadening phrases, such as "others known and unknown," "among others," and elsewhere" impermissibly expand the charges against Mr. Ulbricht.

Thus, this Court must strike language contained in ¶¶ 4 & 10(b) and ¶ 14 of the Indictment referring to the "murder-for- hire" allegations and "password stealers, keyloggers, and remote access tools" as "malicious software designed for computer hacking" respectively, pursuant to

Rule 7(d), Fed.R.Crim.P., as well as broadening phrases such as "others known and unknown," "among others," and elsewhere," to protect Mr. Ulbricht's right to due process and a fair trial as guaranteed by the Fifth and Sixth Amendments to the U.S. Constitution.

A. *The Applicable Law Regarding Surplusage*

Rule 7(d), Fed.R.Crim.P., provides that upon motion of a defendant, the Court may strike extraneous matter, or "surplusage," from an Indictment. Pursuant to Second Circuit case law "a defendant's motion to strike surplusage from an indictment will be granted so long as the language is not relevant to the offenses and is either prejudicial or inflammatory." *United States v. Malochowski*, 604 F.Supp.2d 512, 518 (N.D.N.Y. 2009) (granting defendant's motion to strike surplusage based on irrelevance and the "danger of unfair prejudice"), *citing United States v. Mulder*, 273 F.3d 91, 99 (2d Cir.2001) ("[m]otions to strike surplusage from an indictment will be granted only where the challenged allegations are not relevant to the crime charged and are inflammatory and prejudicial"); *United States v. Scarpa*, 913 F.2d 993, 1013 (2d Cir.1990) (reiterating that Rule 7(d) imposes an "exacting standard").

In addition, any surplusage that remains in an Indictment implicates the defendant's right to due process and to a fair trial under the Fifth and Sixth Amendments because, as is well-settled among the circuit courts, the government is under no obligation – to sustain a conviction – to prove statements in the Indictment that constitute surplusage. *See, e.g., United States v. Greene*, 497 F.2d 1068, 1086 (7th Cir. 1984) ("[t]he language of indictment, insofar as it goes beyond alleging elements of statute, is . . . surplusage . . [and] such surplusage in an Indictment need not be proved"); *United States v. Archer*, 455 F.2d 193, 194 (10th Cir. 1972) ("[i]t is not essential that everything in an Indictment be proved"); *Milentz v. United States*, 446 F.2d 111, 114 (10th Cir.

1971) ("mere surplusage . . . need not be proved"); *Gawne v. United States*, 409 F.3d 1399, 1403 (9th Cir. 1969) ("allegation of the indictment was surplusage [because it was not an element of the offense] and need not have been proved"). Accordingly, to leave such language in an indictment is inherently unfair and a denial of due process.

Indeed, in applying the "exacting standard," this Court recently addressed the type of language that constitutes surplusage, and therefore must be deleted from an indictment, in *Mostafa*, 965 F.Supp.2d at 466-67 (denying defendant's motion to strike surplusage with leave to renew).

In *Mostafa*, this Court acknowledged that pursuant to Rule 7(d), Fed.R.Crim.P., "the Court may strike extraneous matter or surplusage from an indictment . . . 'where the challenged allegations are not relevant to the crime charged and are inflammatory or prejudicial.'" *Id*., at 466, *quoting Mulder*, 273 F.3d at 99; *Scarpa*, 913 F.2d at 1013. The Court also established that "[a]s to broadening phrases, surplusage may be struck if it impermissibly expands the charge" and that "broadening phrases in charging paragraphs can enlarge specific charges." *Mostafa*, 965 F.Supp.2d at 467, *citing United States v. Kassir*, S2 04 Cr. 356 (JFK), 2009 WL 995139 (S.D.N.Y. Apr. 9, 2003), *United States v. Pope*, 189 F.Supp. 12, 25 (S.D.N.Y. 1960).

On the specific facts of that case, however, the Court identified some of the contested surplusage as "background information" that was on that basis "'relevant and need not be struck,'" and ultimately denied the defendant's motion with leave to renew on the basis that "Courts in this district routinely await presentation of the government's evidence at trial before ruling on a motion to strike." *Mostafa*, 965 F.Supp.2d at 466-67.

B. ***All References to "Murder-For-Hire" Allegations In Count One of the Indictment Are Irrelevant to the Charged Offenses and Must Be Struck as Unduly Prejudicial Surplusage, and to Protect Mr. Ulbricht's Right to Due Process and a Fair Trial Guaranteed by the Fifth and Sixth Amendments***

All references to Mr. Ulbricht "soliciting" the "murder-for-hire" of any individuals in Count One, at ¶¶ 4 and 10(b), also must be struck from the Indictment as irrelevant and prejudicial surplusage pursuant to Rule 7(d), Fed.R.Crim.P. in that (1) the allegation that Mr. Ulbricht solicited any murder-for-hire is not charged conduct in this case nor is it an element of Count One or any other count in the Indictment; (2) such language does not possess any probative value under Rule 403, Fed.R.Evid.; and (3) the inclusion of such language violates Mr. Ulbricht's Fifth and Sixth Amendment rights to due process and a fair trial in that it invites the jury to convict him in this jurisdiction on the basis of uncharged conduct, although he has already been charged with "murder-for-hire" in a separate Indictment in the District of Maryland.

1. ***The "Murder-For-Hire" Allegations Referenced in Count One are Irrelevant and Unduly Prejudicial Surplusage Pursuant to Rule 7(d), Fed.R.Crim.P.; in That They Are Not an Element of Either One Or Any Other Count***

It is well-settled that surplusage should be struck from an Indictment pursuant to Rule 7(d), Fed.R.Crim.P., when such language is both irrelevant and prejudicial. *See Mulder*, 273 F.3d at 99. Rule 401 of the Federal Rules of Evidence defines relevant evidence as evidence "having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence." Rule 401, Fed.R.Evid. Moreover, in criminal trials, all facts presented to the jury must be "strictly relevant to the particular offense charged." *Williams v. New York*, 337 U.S. 241, 247 (1949).

In this case, the crucial question the government must prove at trial with regard to Count One, is whether Mr. Ulbricht conspired to distribute and possess with intent to distribute controlled substances in violation of the narcotics laws of the U.S. It is clear that the allegation that Mr. Ulbricht "solicit[ed] the murder-for-hire of several individuals" is not an element of Count One, nor is it a fact making it more or less probable that Mr. Ulbricht engaged in a narcotics trafficking conspiracy as alleged in Count One. It is not admissible as background information as it has nothing to do with the charges in this Indictment, which relate *not* to any murder-for-hire plot, but are limited to the areas of drug trafficking, computer hacking, and money laundering.

For these reasons, this case can also be distinguished from *Mostafa*, and the related case *Kassir*, because in those cases the "references to al Qaeda being led by Bin Laden [that each of those defendants sought to strike] were relevant to the leadership and organization of the entity for which the defendant[s] w[ere] charged with providing support, and was also admissible as background information." *Mostafa*, 965 F.Supp.2d at 466*; citing Kassir*, F.Supp.2d, 2009 WL 995139, at * 2.

Accordingly, since there is no concrete link between the murder-for-hire allegations and the unrelated drug trafficking and other charges in this case, it is clear that all references to "murder-for-hire" are irrelevant to the charges, and their inclusion in the Indictment is highly prejudicial to Mr. Ulbricht.

2. *The "Murder-For-Hire" Allegations Referenced in Count One Must Also Be Struck Pursuant to Fed.R.Evid. 403 Because They Lack Any Probative Value and Are Therefore Unduly Prejudicial to Mr. Ulbricht*

The references to "murder-for-hire" must also be struck from the Indictment because that language is unduly prejudicial under the standard set forth in Fed.R.Evid. 403, which provides for the exclusion of even relevant evidence – which this is not – when its "probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues or misleading the jury." Rule 403, Fed.R.Evid. The danger of unfair prejudice is overwhelming in this case, because of the toxic impact the mere mention of murder allegations would have on a jury.

Correspondingly, the offending language also presents the jury with an improper basis for convicting Mr. Ulbricht, *i.e.*, solely based on his alleged association with a "murder-for-hire" plot that has never been charged in this District and is therefore beyond the scope of the Indictment returned by the grand jury here. Thus, the Indictment leads the jury to ignore the factual issue of whether Mr. Ulbricht engaged in a narcotics trafficking conspiracy and to instead focus on these more inflammatory, murder-for-hire allegations. The irrelevant and highly prejudicial nature of the references to the murder-for-hire allegations requires that such language be struck in its entirety from the Indictment, pursuant to Rule 7(d).

3. *References To The "Murder-For-Hire" Allegations Must Be Struck from the Indictment to Protect Mr. Ulbricht's Fifth and Sixth Amendment Rights to Due Process and a Fair Trial*

In addition, the inclusion in the Indictment of uncharged murder-for-hire allegations is not only irrelevant and inflammatory, but violates Mr. Ulbricht's constitutional rights to due process and a fair trial. Since it is undisputed that the government need not prove that Mr. Ulbricht solicited any murder-for-hire to convict him of Count One, as it is not an element of the crime(s)

charged, and because "[t]he language of the indictment, insofar as it goes beyond alleging elements of statute, is surplusage [and] . . .need not be proved[,]" the government, through its inclusion of this surplusage, invites the jury to convict Mr. Ulbricht in this district of conduct he has never been charged with here and is already charged with in the District of Maryland. *See, e.g., Greene*, 497 F.2d at 1086.

Accordingly, language in the Indictment referring to the "murder for hire" allegations must be struck to preserve Mr. Ulbricht's constitutional protections under the Fifth and Sixth Amendments, in so far as his right to due process and a fair trial.

C. *Reference In Count Three of the Indictment to "Password Stealers, Keyloggers, and Remote Access Tools" as "Malicious Software Designed for Computer Hacking,"Are Extraneous and Must Be Struck as Unduly Prejudicial Surplusage, and to Protect Mr. Ulbricht's Right to Due Process and a Fair Trial Guaranteed by the Fifth and Sixth Amendments to the United States Constitution*

The government's flawed and biased characterization in Count Three of the Indictment of "password stealers, keyloggers, and remote access tools" as "malicious software designed for computer hacking," must be struck as extraneous and unduly prejudicial surplusage because these devices have numerous legitimate uses and applications, despite having become associated with illegal activity because of their use in high profile cases or fictional universes. *See* Indictment, at ¶ 14.

Indeed, as set forth in Mr. Ulbricht's pre-trial motions challenging the face of the Indictment, even the FBI solicits malware. An FBI podcast dated March 14, 2014, announced that "Malware Investigator gives community of interest partners the ability to submit malware files." The podcast announcement explains that "Malware Investigator will determine the damage the file can inflict[,]" and "will provide a technical analysis report to the submitter." *See*

<http://www.fbi.gov/news/podcasts/thisweek/malware-investigator.mp3/view>. The FBI even intends to launch Malware Investigator as a web site this summer. *Id.*

Accordingly, under the standard set forth in Rule 403, Fed.R.Evid. which excludes even relevant evidence when its "probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues or misleading the jury," the language the government uses to describe software allegedly sold on Silk Road is unduly prejudicial, as well as entirely extraneous and inaccurate, and must therefore be struck from the Indictment.

Mr. Ulbricht also seeks to strike the government's conclusory language about the nature of the software allegedly sold on Silk Road because it threatens to violate his Fifth and Sixth Amendment rights. Indeed, the inclusion of the contested language in the Indictment relieves the government of its burden of proving that Mr. Ulbricht *did know* that the purchaser or ultimate user of the software allegedly purchased on the Silk Road website was *not* intending to use the software for proprietary research, academic study, security purposes, or to satisfy his or her own particular abstract interest, but instead to "intentionally access computers without authorization, and thereby...obtain[ing] information from protected computers, for purposes of commercial advantage and private financial gain, in furtherance of criminal and tortious acts in violation of the Constitution and the laws of the United States [and 18 U.S.C. §1030]," the very offense charged in Count Three.

D. ***Broadening Phrases, Such as "Others Known and Unknown," "Among Others," and Elsewhere," must Be Stricken Because They Impermissibly Expand the Charges Against Mr. Ulbricht***

It is well-settled in this district, as this Court has acknowledged, that ""[a]s to broadening phrases, surplusage may be struck if it impermissibly expands the charge" and that "broadening

phrases in charging paragraphs can enlarge specific charges." *Mostafa*, 965 F.Supp.2d at 467, *citing Kassir*, 2009 WL 995139, at *2, *Pope*, 189 F.Supp., at 25 (holding that "language impermissibly delegated to the prosecution the authority to enlarge the specific charges, which could have resulted in 'depriving [the] defendant of his constitutional right to be accused of a felony offense only on the basis of a grand jury indictment'"). In this case, the Indictment includes broadening language, including phrases such as "others known and unknown," "among others," and "elsewhere," which impermissibly expand the charges against Mr. Ulbricht beyond the specific charges returned by the grand jury. Accordingly, since these phrases insinuate crimes not charged, as well as untold numbers of transactions, locations and persons involved in each crime that are not otherwise specified in the Indictment, or even decipherable from the evidence, these phrases must be struck in their entirety.

Indeed, while Mr. Ulbricht is aware that this Court, in *Mostafa*, denied a motion to strike surplusage with leave to renew, that addressed these specific phrases, the particular usage of these phrases within the context of Mr. Ulbricht's case is distinguishable as are the specific circumstances in this case.

For instance, in *Mostafa*, the Court denied the defendant's motion to strike the term "among others" though in a co-defendant's case the court had struck the term "among other things" because "the phrase was not used in the same manner as in the indictment [in Mr. Mostafa's case]." *Mostafa*, 965 F.Supp.2d at 467, *citing Kassir*, 2009 WL 995139, at *4. In Mr. Ulbricht's case the phrase "among others," used only in ¶ 9 of the Indictment, is like the usage in *Kassir* because it describes other *things, i.e.,* types of controlled substances. Accordingly, this reference, which masks a potential host of substances the government alludes to but does not

name, and which a jury could insinuate were even more dangerous or illicit than the substances listed, must therefore be struck from the Indictment.

In addition, unlike in *Mostafa* where the defendant had some idea of who the "others known and unknown" were and where the "elsewhere" locales might be, because the case involved particular regions of the world and known entities, the allegations in this case revolve around transactions that took place between individuals on the Silk Road website, which had as its hallmark, according to the government, the ability to preserve anonymity and to hide any details concerning location or identity of "users across the world." *See* Indictment at ¶ 1 (describing Silk Road as "an underground website . . . designed to enable users across the world to buy and sell illegal drugs and other illicit goods and services anonymously").

Without any specific parameters in the Indictment which create limits, the charges, as a result of phrases such as "others known and unknown" and "elsewhere" and under the particular circumstances of this case and the unique nature of the Silk Road website, have thus been expanded to include anyone and everyone, in every location in the entire world. Therefore, this language must be struck as surplusage to avoid 'depriving [Mr. Ulbricht] of his constitutional right to be accused of a felony offense only on the basis of a grand jury indictment.'" *Pope*, 189 F.Supp., at 25.

Conclusion

Accordingly, for all the reasons set forth above, it is respectfully requested that the Court grant Mr. Ulbricht's pre-trial motions to suppress the fruits of the unlawful searches and seizures, and any evidence or other information derived therefrom, for discovery, for a bill of particulars, and to strike irrelevant and prejudicial surplusage from the Indictment, in their entirety.

Dated: 1 August 2014
New York, New York

Respectfully submitted,

/S/ Joshua L. Dratel
JOSHUA L. DRATEL
JOSHUA L. DRATEL, P.C.
29 Broadway, Suite 1412
New York, New York 10006
(212) 732-0707

Attorneys for Defendant Ross Ulbricht

– Of Counsel –

Joshua L. Dratel
Lindsay A. Lewis