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

REPLY 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 G. Schlimbach
Joshua J. Horowitz

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

Introduction

This Reply Memorandum of Law is submitted on behalf of defendant Ross Ulbricht, and in support of his motions to suppress evidence, discovery, a Bill of Particulars, and to strike surplusage from the Indictment. As many of the government's arguments in opposition (Dkt # 56) (hereinafter "Government's Memo of Law") were anticipated in Mr. Ulbricht's initial Memorandum of Law (Dkt #48), much does not require rejoinder.[1]

Indeed, the government's response is remarkable for what it *fails* to confront at all: an entire current class of Supreme Court opinions that have adapted and updated Fourth Amendment jurisprudence to accommodate the essential privacy imperatives of the digital age. Thus, the government does not even mention or cite, much less address, the Court's decision and opinions in *Riley v. California*, ___ U.S. ___, 134 S. Ct. 2473 (2014), or *United States v. Jones*, ___ U.S. ___, 132 S. Ct. 945 (2012), or even *Kyllo v. United States*, 533 U.S. 27, 32 (2001).

Yet pretending those cases do not exist, and that is still 1979, with the landscape governed only by *Smith v. Maryland*, 442 U.S. 735 (1979), fails to assist the government in defending the series of unconstitutional searches and seizures it conducted in its investigation of this case. As detailed in Mr. Ulbricht's initial Memo of Law, at 18-28, *Riley* and *Jones* augur a contemporary Fourth Amendment analysis that recognizes the privacy interests in electronically stored and communicated information. The government's inability even to discuss those cases, and their Fourth Amendment implications, simply demonstrates the bankruptcy of its arguments

[1] Mr. Ulbricht's additional motions aimed at the Superseding Indictment (Dkt #52) will raise any additional issues the Superseding Indictment has generated pertinent to his demand for a Bill of Particulars. In addition, the defense is still reviewing discovery produced by the government which may further inform those motions.

in opposition.

In its response, however, the government does devote significant space and effort to explaining and defending its initial access to the Silk Road Server overseas. Yet that, too, is unavailing, because, as discussed below and detailed in the accompanying September 30, 2014, Declaration of Joshua J. Horowitz, Esq. (hereinafter "Horowitz Declaration"), the government's explanation does not withstand technical scrutiny and/or analysis, or practical application.

In fact, as the Horowitz Declaration establishes, the discovery produced by the government in this case fatally undermines the government's account – provided in the Declaration by former Special Agent Christopher Tarbell (Dkt #57) (hereinafter "Tarbell Declaration") – of its initial access to the Silk Road Server, and raises additional material questions regarding the government's representations about its investigation. All of those questions beg the ultimate queries: what is the government hiding, and *why*?

Also, as an afterthought, nearly two weeks after it filed its opposition, the government, in its September 16, 2014, Supplemental Memo of Law (Dkt #63), raised the issue of Mr. Ulbricht's standing to challenge the government's acquisition of an image of the Silk Road Server. Yet to the extent there is any question that the Court can adjudicate Mr. Ulbricht's motion with respect to the Silk Road Server, the inadequacy of the government's version of how it gained access raises material issues of fact, relative to standing as well as the ultimate issues, that requires an evidentiary hearing.

That hearing is necessary to address not only the claims in the Tarbell Declaration, but also whether the U.S. government enlisted Icelandic authorities as the U.S.'s virtual agents in obtaining the image of the Silk Road Server. While the government contends its involvement

did not rise to that of virtual agency, that, too, is a case-specific, fact-specific evaluation that merits a hearing in this case.

Regarding its seizure and searches subsequent to imaging the Silk Road Server – in particular, those pertaining to Mr. Ulbricht's laptop, and his Facebook and Google accounts – the government acknowledges their unbridled breadth, but, in effect, asserts that because they were unlimited and indiscriminate *by design*, they somehow escape invalidation as general warrants. As detailed below, that argument is without merit.

Regarding Mr. Ulbricht's motion for discovery, while the government contends it is not obligated to comply with Mr. Ulbricht's discovery demands, and even that Mr. Ulbricht has failed to demonstrate a need for the materials requested, the Horowitz Declaration establishes the government's failure to provide adequate discovery, and/or an explanation of how it obtained access to the Silk Road Server, which is necessary and material to Mr. Ulbricht's preparation of his defense. Thus, as set forth in POINT II below, Mr. Ulbricht's discovery demands are tailored to fill the holes in the government's discovery and in its explanation of how the FBI was able to identify and locate the Silk Road Server.

In addition, as discussed **post**, in POINT III, the government's opposition to Mr. Ulbricht's motion for a Bill of Particulars relies on the avalanche of discovery that in many respects *creates*, rather than cures, the problem of identifying the specific criminal conduct alleged with respect to particular counts in the Indictment.

Accordingly, it is respectfully submitted that Mr. Ulbricht's motions to suppress should be granted in its entirety, or, in the alternative, an evidentiary hearing conducted, and that his motions for discovery, a Bill of Particulars, and to strike surplusage from the Indictment be

granted in their entirety as well.

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

A. *The Government's Claim of How It Gained Access to the Silk Road Servers Raises Several Material and Disputed Issues of Fact That Require An Evidentiary Hearing*

As noted **ante**, in its Memo of Law the government concentrates on explaining and defending its initial access to the Silk Road Server overseas. The explanation was provided in the Tarbell Declaration, but, as the Horowitz Declaration concludes, that account is "implausible" and contradicted by the very discovery produced by the government as well as the technical realities of the internet. As a result, since the government's version has raised several material disputed issues of fact, an evidentiary hearing is necessary.

As the Horowitz Declaration attests, the government's account suffers from several serious deficiencies:

(1) based on the Silk Road Server's configuration files provided in discovery, former Special Agent Tarbell's explanation of how the FBI discovered the Server's IP address is implausible;

(2) the account by former Special Agent Tarbell in his Declaration differs in important respects from the government's June 12, 2013, letter to Icelandic authorities. For example, that letter (which is Exhibit A to the government's

opposition papers) suggests the possibility of an alternative method for the government's identifying and locating the Silk Road Server;

(3) former Special Agent Tarbell's explanation is vague and lacks supporting documentary and forensic evidence that should exist if former Special Agent Tarbell had adhered to the most rudimentary standards of computer forensic analysis, but which he apparently did not follow, or failed to preserve evidence of his alleged work that could substantiate the government's account (and which the defense has now requested);

(4) several critical files provided in discovery contain modification dates predating the first date Special Agent Tarbell claims the Icelandic authorities imaged the Silk Road Server, thereby casting serious doubt on the chronology and methodology of Special Agent Tarbell's account; and

(5) the government's version contains additional inconsistencies, including items referred to and/or indicated by former Special Agent Tarbell's Declaration, but not produced in discovery.

Thus, the government's explanation has generated more questions than it has provided answers.[2] Unless the government can verify its account beyond the mere Declaration by a law

[2] Also, it is noteworthy that while the Silk Road web site was one of the most persistently monitored and attacked sites on the internet, and the subject of continued discussion in a variety of social media and other forums – including the success or lack thereof of attempts to penetrate it – the security flaw that permitted the FBI's purported intrusion, and which would have been available to the legions of hackers attempting continuously to gain access to or compromise the Silk Road Server, was never the subject of *any* internet discussion, in contrast to the extensive and intensive coverage attendant to prior security breaches the site had experienced. *See, e.g.*, Kadhim Shubber, "Infamous marketplace Silk Road brought down by DDOS attack," *Wired*, May 3, 2013, available at http://www.wired.co.uk/news/archive/2013-

enforcement agent, it cannot be accepted as dispositive. Former Special Agent Tarbell failed to maintain any record of his purported means of access to the Silk Road Servers. Indeed, by not preserving what he claims he did -- and preservation would have been a simple, automated task -- he violated the most rudimentary protocols of any forensic investigation, much less one involving digital data and communications. *See* Horowitz Declaration, at ¶ 35, and n.17. Accordingly, the government provides no corroboration or verification for its assertions. Certainly, the Horowitz Declaration identifies a series of material disputed issues of fact that require an evidentiary hearing on the issue.

In addition, and further casting doubt on the government's version, the government – conveniently in a footnote, *see* Government's Memo of Law, at 3, n. 1 – reveals that a fundamental representation made in each of its application(s) for a warrant in this investigation – that the Silk Road Server was imaged as a result of a request by the U.S. to Iceland pursuant to Mutual Legal Assistance Treaty (hereinafter "MLAT"), *see* Mr. Ulbricht's initial Memo of Law, at 30 – was "not technically correct[,]" which in this instance means it was *false*. The government has not, and evidently cannot, provide any explanation for that misrepresentation under oath, in affidavit after affidavit, by former Special Agent Tarbell, who was directly involved in the process of acquiring the image of the Server.

Consequently, when the government, in its Memo of Law, at 17, claims that the affidavits submitted in support of the serial applications for warrants "explained the legal mechanism

---

05/3/silk-road-ddos; Vitalik Buterin, "Silk Road Under DDOS Attack," *Bitcoin Magazine*, May 1, 2013, available at http://bitcoinmagazine.com/4387/silk-road-under-ddos-attack/; John Glenday, "Hackers take Silk Road website down in DDOS Attack," *The Drum*, May 2, 2013, available at http://www.thedrum.com/news/2013/05/02/hackers-take-silk-road-website-down-ddos-attack.

through which the government obtained a copy of the SR Server[,]" it omits that those affidavits did so *falsely*.

Also, the government attempts to create a straw man by contending, in its Memo of Law, at 2, that it was "not necessary to explain [in the warrant applications] how the Government located the Silk Road server in order to" establish probable cause. *See also id.*, at 15-16. However, the information the government withheld was not part of the probable cause determination, but rather the means by which it obtained evidence that contributed almost 100% to its probable cause presentation.

The government's position appears to be that if the government obtained evidence by patently illegal means, *i.e.*, torture, burglary, illegal eavesdropping, that would not be information relevant to a court's determination whether to issue the warrant. Yet a defendant is entitled to know whether the government's investigation was predicated on illegal government conduct, and for relief therefrom. *See, e.g., Gelbard v. United States*, 408 U.S. 41, 55 (1972) ("plac[ing] upon the Government an affirmative duty to answer a claim that evidence is inadmissible because of unlawful investigative conduct"). *See also United States v. Ghailani*, 743 F. Supp.2d 261, 287-88 (S.D.N.Y. 2010) (evidence obtained through torture was the subject of litigation, an evidentiary hearing, and a ground-breaking decision by the trial court: "[i]f the government is going to coerce a detainee to provide information . . . it may not use that evidence – or fruits of that evidence that are tied as closely related to the coerced statements as [the witness's] testimony would be [in Mr. Ghailani's case] – to prosecute the detainee for a criminal

offense").[3]

Constructing another straw man, the government states the unremarkable proposition that "[a] search warrant affidavit need not contain 'every piece of information gathered in the course of an investigation.'" Government's Memo of Law, at 15, *citing United States v. Awadallah*, 349 F.3d 42, 67-68 (2d Cir. 2003) (other citation omitted). However, in this instance, it is not just some extraneous piece of "information gathered" that was omitted – and to the extent provided, done so *falsely* – but the means by which the foundational evidence in the investigation was obtained.

Thus, contrary to the government's claim that warrant applications omitted merely a "*fact*[] learned during the investigation[,]" Government's Memo of Law, at 17, n. 4 (emphasis added), rather they omitted a methodology with potentially dispositive legal implications.

In citing *Wilson v. Russo*, 212 F.3d 781, 787 (3d Cir. 2000), the government, in its Memo of Law, at 16-17, quotes the Third Circuit's statement that "[a]ll storytelling involves an element of selectivity." Indeed, the issue here is *storytelling*, as the Tarbell Declaration does just that in a manner that, as demonstrated by the Horowitz Declaration, raises a series of material disputed issues of fact that can be resolved only by an evidentiary hearing.

---

[3] In its September 23, 2014, letter (Exhibit 4 to the Horowitz Declaration), at 6 (item 14), responding to Mr. Ulbricht's September 17, 2014, letter (Exhibit 3 to the Horowitz Declaration) seeking additional discovery, the government represents that it will not use at trial the images of the Silk Road Server created by Icelandic authorities June 6, 2013, thereby tacitly conceding that such imaging was performed in violation of Icelandic law. However, that disclaimer with respect to admission at trial does not answer the question whether the government reviewed those images, whether they were used or consulted in the course of the investigation, and/or whether any other evidence or information was derived from those June 6, 2013, images.

B. *The Government's Means of Access to the Silk Road Server Overseas Violated the Computer Fraud and Abuse Act, 18 U.S.C. §1030*

Even if the government's account of its initial means of access to the Silk Road Server overseas is accurate, the government doth protest too much, asserting "[t]here was nothing unconstitutional or otherwise unlawful in the FBI's detection of that leak." Government's Memo of Law, at 7. *See also id*., at 1, 17, 35.

The government's defensiveness is understandable given that it has *prosecuted* persons, under the Computer Fraud and Abuse Act (hereinafter "CFAA"), 18 U.S.C. §1030 (ironically, a violation of which is charged in Count Five), for essentially the same conduct described in former Special Agent Tarbell's Declaration.

For example, in *United States v. Auernheimer*, Docket No. 13-1816 (3d Cir. 2013), the government *repeatedly* argued in the Third Circuit, in response to the defendant's appeal from his conviction, that

> AT&T's server was not unprotected and openly available to the public. Bad or inadequate protection is not the same as no protection. . . . AT&T's security precautions were inadequate, and [the defendants] exploited for their own purposes the security flaw they discovered. The jury was entitled to find, as they did, that the conspirators' accessing of the AT&T servers was unauthorized.

Government's Brief, *United States v. Auernheimer*, Docket No. 13-1816 (3d Circuit), filed September 20, 2013 (Dkt #3111395511), at 20-21. *See also id*., at 26 ("[a]ll of Auernheimer's conversations with Spitler and others indicate that he knew they were exploiting a security flaw in AT&T's system") (record citations omitted); *id*. at 27 ("[t]he complicated steps that Spitler had to take to access the e-mail/ICC-ID pairings on the AT&T server support the jury's factual conclusion that Spitler's use of the server was unauthorized"); *id*., at 33 ("even discovering the

security flaw, not to mention exploiting it, required a level of sophistication unavailable to the vast majority of internet users").[4]

Indeed, the government posited an analogy that applies with equal force here:

> [l]ikewise, in using computers, people commit security lapses all the time. If a government employee, after properly signing in to her account, leaves her workstation unattended without logging out, that does not authorize the office's cleaning person to access her computer and start entering search requests for classified government information or even search requests for the government employee's personal e-mails. The government employee almost certainly failed to comply with proper security procedures by leaving her computer unattended, but the knowing and purposeful exploitation of that security breach by the cleaning person could be prosecuted as a violation of the CFAA because the access was unauthorized and any reasonable person would know that.

Id., at 34-35.

Moreover, the government based its position not merely on the technical statutory language of the CFAA, but also on accepted ethical norms adopted by society that would make anyone aware of the wrongfulness of such conduct:

---

[4] Also, as the government pointed out in its Brief in *Auernheimer*,

> [t]here was no search on Google, Bing, or any other search engine that a person could enter that would return the e-mail/ICC-ID pairings. Likewise, there was no link on any AT&T webpage that could be clicked on to return this information. No one could have stumbled upon this information inadvertently. Members of the general public who lacked expertise in reading and manipulating computer code could not have gained access to this information. Indeed, it was not easy for Spitler, an experienced computer hacker, to obtain this information from AT&T's servers.

Government's Brief, *United States v. Auernheimer*, Docket No. 13-1816 (3d Circuit), filed September 20, 2013 (Dkt #3111395511), at 27.

> [a]s the above example demonstrates, a person can improperly access a computer without violating a code-based restriction or without using someone else's password. There are norms of behavior that are generally recognized by society, and violating those norms of behavior – by taking unattended property or accessing a computer without authorization – can constitute a crime. *See U.S. v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007) (authorization is "typically analyzed on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user"); *U.S. v. Morris*, 928 F.2d 504, 510 (2d Cir. 1991) (defendant committed unauthorized access where he "did not use [certain computer] features in any way related to their intended function").

Id., at 35.[5]

Thus, in *Auernheimer*, the government advanced the position that obtaining information at the website addresses constituted unauthorized – and therefore criminal in violation of §1030 – access because AT&T had not intended for the public to see that information, and it was in a place where an ordinary computer user would not likely find it.

Yet, here, the government has assumed the diametric position: data on a server is unprotected by law if the system administrator configured the network incompetently so that an FBI expert could find the data. *See, e.g.*, Orin Kerr, "Does Obtaining Leaked Data From a

---

[5] Again, in a passage applicable here, the government argued in *Auernheimer* that:

> AT&T's servers were tricked into returning information that its system was designed to return only to the actual iPad owners, and only when they were accessing AT&T's servers through their iPads. Auernheimer's suggestion that this access was legal since AT&T's system was in fact responding to the URLs as it was designed to do, is as absurd as arguing that picking a lock to commit trespass is legal simply because the lock responded to a configuration of lock picks in the exact way that it was mechanically designed to respond.

United States v. Auernheimer, Government's Brief, at 42.

Misconfigured Website Violate the CFAA?" *The Washington Post*, September 8, 2014 (available at <http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/08/does-obtaining-leaked-data-from-a-misconfigured-website-violate-the-cfaa/>).[6]

That tension in the government's position(s) is irreconcilable, and is not ameliorated by the CFAA provision (not cited by the government herein) that grants an exception for "lawfully authorized investigative . . . activity of a law enforcement agency of the United States[.]" 18 U.S.C. §1030(f).[7] Certainly illegal conduct that invades privacy – either tangibly or intangibly – is not "lawfully authorized." Indeed, the government could not commit a burglary, or warrantless electronic surveillance, or a home invasion and claim it was "lawfully authorized" simply because the illegal activity was performed as part of a criminal investigation. Here, there is no basis to conclude that the government's conduct – a criminal violation of §1030 under the government's own definition of the offense – was "lawfully authorized." As a result, the exception in §1030(f) does not apply.

Nor are the cases cited by the government apposite. For example, in *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010) (cited in the Government's Memo of Law, at 8), the

---

[6] *See* Government's Memo of Law, at 8 ("[i]t does not matter that Ulbricht *intended* to conceal the IP address of the SR Server from public view. He failed to do so competently, and as a result the IP address was transmitted to another party – which turned out to be the FBI – who could lawfully take notice of it").

[7] In *New Hampshire v. Maine*, 532 U.S. 742, 749 (2001), the Court declared that "[w]here a party assumes a certain position in a legal proceeding, and succeeds in maintaining that position, he may not thereafter, simply because his interests have changed, assume a contrary position." Here, since in *Auernheimer* the Third Circuit decided the appeal (in the defendant's favor) on venue grounds, the government's theory underlying the substantive offense, which resulted in a conviction, ostensibly stands.

information in IP addresses that was deemed "voluntarily turned over in order to direct the third party's servers[]" was limited to packet headers, and not the content – which in this instance the IP address itself represented. Also, the "voluntariness" aspect of the opinion in *Christie* completely undercuts the government's claim that "[i]t does not matter that Ulbricht intended to conceal the IP address of the SR Server from public view."

Similarly, contrary to the government's characterization of the holding in *United States v. Post*, ___ F. Supp.2d ___, 2014 WL 345992 (S.D.Tex. Jan. 30, 2014), cited in the government's Memo of Law, at 8, the Court therein did not hold that a legitimate privacy interest does not exist in metadata generally. Rather, the Court found that the defendant's lacked a privacy interest in the image containing the metadata because he had *voluntarily posted the image* on the Internet. 2014 WL 345992, at *4.

In fact, the Court in *Post* specifically distinguished the situation therein from both the privacy issue resolved in *Riley*, and from the controversy over whether an individual has a privacy interest in telephone metadata in the context of the NSA's "bulk collection of telephone metadata." *Id*. The Court concluded that Post "had no cognizable privacy interest that the government needed to overcome to justify searching for metadata in the photo he placed on the internet," unlike the privacy interest in telephone metadata that is "necessarily disclosed" to third parties or in the contents of a cell phone when the warrantless seizure of the phone itself is justified. *Id*.

Also, in *United States v. Dreyer*, ___ F.3d ___, 2014 WL 4474295, at *1 (9th Cir. September 12, 2014), the Ninth Circuit recently reversed a conviction because a Naval Criminal Investigative Service (hereinafter "NCIS") violated the *Posse Comitatus* Act, 18 U.S.C. §1385,

that prohibits military involvement in civilian law enforcement.[8] In applying the exclusionary rule to a statutory violation, the Ninth Circuit explained,

> [t]hat a need to deter future violations exists is further supported by the government's litigation positions. The government is arguing vehemently that the military may monitor for criminal activity all the computers anywhere in any state with a military base or installation, regardless of how likely or unlikely the computers are to be associated with a member of the military. Such an expansive reading of the military's role in the enforcement of the civilian laws demonstrates a profound lack of regard for the important limitations on the role of the military in our civilian society.

Id., at 8.

Here, the same is true, as the government's contradictory litigation position(s) manifest its belief that it can blithely commit the very same conduct it considers illegal – and worthy of federal prosecution – under the CFAA. As a result, the deterrent purpose of the exclusionary rule is necessary here as it was in *Dreyer*.[9]

---

[8] While the NCIS investigator's violation of the PCA was sufficiently objectionable to require the conviction be reversed, perhaps the more disturbing aspect of the case was the revelation that the NCIS investigator had conducted surveillance of all of the civilian computers in the entire state of Washington to determine whether any contained child pornography. *Id*., at *8. That type of electronic dragnet provides a window, albeit limited, on the government's vast, heretofore inconceivable, investigative capabilities in the digital age, and the correspondingly limitless prospect for abuse of that capacity.

[9] In addition, any involvement of the National Security Agency – a military agency, *see* October 24, 1952, Memorandum from President Harry S. Truman to the Secretary of Defense and Secretary of State establishing the NSA, available at https://www.nsa.gov/public_info/declass/truman.shtml – in the investigation of this case would also constitute a violation of the Posse Comitatus Act for the same reasons set forth in *Dreyer*.

C. *The Imaging of the Silk Road Server Overseas – In Effect, Its Seizure – Was the Result of a Virtual Agency Between U.S. and Icelandic Authorities, and Therefore Subject to Fourth Amendment Review and Analysis*

While former SA Tarbell's Declaration maintains that "[t]he FBI was not involved in obtaining that court order [to search the SR Server located in Iceland] or ever given a copy of it . . . [n]or was the FBI present or otherwise involved in the imaging of the server" and that [a]t no time did the FBI possess any authority to direct or control the RMP's actions," Tarbell Declaration, at ¶ 12, it concedes *in that very same paragraph* that the FBI "asked the RMP, which coordinated with the FBI on the timing of the search of the [Silk Road] Server, to proceed with covertly imaging the server." *Id.*

Former SA Tarbell also admits, in his Declaration, at ¶ 14, that "September 26, 2013 . . . a supplemental request was issued to Iceland [by the FBI], asking Icelandic authorities to seize the SR Server at a time to be chosen in consultation with the FBI and to re-image its contents, in order to ensure collection of any data added or modified since the initial imaging of the server in July 2013." *Id.* [10]

Obviously, that sequence of events was neither accidental, coincidental, nor spontaneous. Nor can attempts at linguistic distinction – the FBI agents were not "present," obfuscate the truth.[11] Instead, it was just as obviously planned, orchestrated, directed, and implemented by and/or at the behest and for the benefit of the U.S. Having set that inexorable course in motion,

---

[10] Also, as set forth in former Special Agent's Tarbell's Declaration, at ¶ 9 n. 7, the FBI had previously made a similar request to Icelandic authorities for traffic data and an image of "Server-1," the Silk Road Server assigned IP address 193.107.84.4.

[11] The U.S.'s clear direction to seize and image the Silk Road server renders inexplicable former SA Tarbell's assertion that "at no time did the FBI possess any authority to direct or control the RMP's actions." *See* Tarbell Dec., at ¶ 12.

the U.S. cannot suggest that enlisting surrogates to perform the seizures and imaging somehow shields the U.S. from accountability for any violations of Mr. Ulbricht's Fourth Amendment rights as a result of those warrantless searches and seizures.

In fact, the Second Circuit has held that U.S. constitutional standards apply in two situations: "(1) where the conduct of foreign law enforcement officials rendered them agents, or virtual agents, of United States law enforcement officials;" and/or "(2) where the cooperation between the United States and foreign law enforcement agencies is designed to evade constitutional requirements applicable to American officials." *United States v. Maturo*, 982 F.2d 57, 61 (2d Cir. 1992), *citing United States v. Busic*, 592 F.2d 13, 23 n. 7 (2d Cir.1978) (suggesting Fourth Amendment could apply if foreign authorities acted "as agents of American authorities"); *United States v. Bagaric*, 706 F.2d 42, 69 (2d Cir. 1983).[12] *See also United States v. Karake*, 281 F. Supp.2d 302, 308 (D.D.C. 2003); *United States v. Getto*, 729 F.3d 221, 230 (2d Cir. 2013).

As a result, the government cannot evade judicial scrutiny pursuant to U.S. constitutional standards simply by delegating the performance of the conduct itself to foreign agents and authorities. In a weak effort to support its contention that the actions of the FBI in directing the RMP to conduct a search, seizure and imaging of the Silk Road server did *not* fall within one of the two "narrowly limited circumstances" in which U.S. constitutional restrictions attach, the

[12] Other circuit courts, as well as district courts within the S.D.N.Y., have similarly recognized that when U.S. agents are "substantially" involved in investigative activities with foreign law enforcement officials those acts constitute "a joint venture" and constitutional standards apply to the admission of evidence obtained as a result. *See, e.g., United States v. Peterson*, 812 F.2d 486, 490 (9th Cir. 1987) (finding "joint venture" and Fourth Amendment applicable to wiretap by Thai police agents given that U.S. law enforcement played a "substantial role" in assessing and utilizing fruits of wiretaps).

government relies on *United States v. Getto*, 729 F.3d at 227, 230-333, in which the Second Circuit held, in part, that "robust information-sharing and cooperation" does not rise to the level of virtual agency.

However, the relevant circumstances in *Getto* – that (1) "American law enforcement authorities filed a *request*, pursuant to the MLAT between the United States and Israel for the Israeli National Police *to investigate*;" (2) "American law enforcement agents . . . *shared the results of their preliminary investigation* (*e.g.*, telephone numbers and bank account information) with the INP;" and (3) the foreign law enforcement agency *conducted an independent, parallel investigation*," *id*., at 226, 231 (emphasis added) – are so disparate from the facts in Mr. Ulbricht's case as to render the government's reliance on it meaningless. *See* Government's Memo of Law, at 9-11.

Indeed, the relatively benign facts in *Getto* only demonstrate the stark contrast between cooperation that does *not* warrant the application of U.S. constitutional standards, and the conduct here, *i.e.*, directing Icelandic authorities to seize the SR Server at a time to be chosen in consultation with the FBI, and to re-imaging its contents, which is precisely the type of virtual agency relationship that triggers the application of the Fourth Amendment's exclusionary rule. *See* Tarbell Dec., at ¶ 12, 14.

Accordingly, the government cannot hide behind the principle that "the Fourth Amendment's exclusionary rule, which requires that evidence seized in violation of the Fourth Amendment must be suppressed, generally does not apply to evidence obtained by searches abroad conducted by foreign officials." Government's Memo of Law, at 9, *quoting Getto*, 729 F.3d at 227 n.7.

Despite the fact that Iceland performed the mechanical acts of seizing the Silk Road Server and imaging and then re-imaging its contents, as set forth in former SA Tarbell's Declaration, it was the U.S. that was pulling the strings and calling shots.

D. *Mr. Ulbricht Does Not Have to File An Affidavit In Order to Establish Standing to Challenge the Imaging, Seizure, and Search of the Silk Road Server Overseas*

The government asserts in its September 16, 2014, Supplemental Memorandum of Law in opposition to Mr. Ulbricht's motion to suppress evidence that Mr. Ulbricht cannot move to suppress evidence from the Silk Road Servers because he lacks standing to do so in the absence of a "sworn affidavit" from him stating that "he leased and administered the SR server – in other words, that he was the administrator of the Silk Road website, as the government alleges." *See* Government's Supplemental Motion, at 3-4. This argument fails because whether a standing issue, in fact, exists must first be resolved through an evidentiary hearing.

Second Circuit case law makes clear that whether or not Mr. Ulbricht must establish standing through a sworn affidavit is a question to be answered *only after* the Court has decided the threshold issues whether (1) a Fourth Amendment interest exists in the Silk Road servers (absent which such affidavit would be altogether irrelevant); and (2) the government's conduct could and/or should be excused by the good faith exception to the Fourth Amendment's warrant requirement.

As the Circuit instructed in *United States v. Pena*, 961 F.2d 333, 336 (2d Cir. 1992), "'the better analysis forthrightly focuses on the extent of a particular defendant's rights under the Fourth Amendment, rather than on any theoretically separate, but invariably intertwined concept of standing.'" *Id*., *quoting United States v. Paulino*, 850 F.2d 93, 96 (2d Cir.1988); *Rakas v. Illinois*, 439 U.S. 128, 139 (1978) (relevant "inquiry . . . requires a determination of whether the

disputed search and seizure has infringed an interest of the defendant which the Fourth Amendment was designed to protect" and noting that "by frankly recognizing that this aspect of the analysis belongs more properly under the heading of substantive Fourth Amendment doctrine than under the heading of standing, we think the decision of this issue will rest on sounder logical footing").

Therefore, in *Pena*, in which the item searched was not a server, but a car, the Court made plain that "whatever the status of the person asserting a Fourth Amendment claim . . . it is clear that in this circuit, the issue is whether the claimant 'had a reasonable expectation of privacy in the area of the vehicle searched'" and that "[t]his focus is faithful to the Supreme Court's ruling in *Rakas* that the determinative issue is 'whether [the defendant] had a legitimate expectation of privacy in the particular areas . . . [to be] searched." *Pena*, 961 F.2d 337, *quoting Paulino*, 850 F.2d at 97, and *Rakas*, 439 U.S. at 148. *See also United States v. Chuang*, 897 F.2d 646, 649 (2d Cir. 1990) ("we focus on whether defendant has established a legitimate expectation of privacy in the area searched"); *United States v. Smith*, 621 F.2d 483, 486 (2d Cir.1980) ("the threshold question . . . is whether the defendant had a legitimate expectation of privacy in the area searched or in the articles seized").[13]

Thus, the standing issue is in part dependent on the information disclosed in an evidentiary hearing which could reveal that an affidavit from Mr. Ulbricht is not required, either

[13] In seeking to minimize Mr. Ulbricht's expectation of privacy in digital data, the government, in its Memo of Law, at 12, contends that "[t]his is not a case where the overseas property searched consisted of a home or other living space occupied by a U.S. citizen; it consisted of a computer server housed at a commercial data center." The government, in effect denying decades of technological and social development that has made digital data probably the *most* sensitive element of personal privacy, also again fails to confront *Riley* and *Jones*, which indisputably recognize the changes wrought by technological advancement and its impact on personal privacy.

because a Fourth Amendment interest does not exist or, alternatively, because information about the Silk Road Servers was obtained through a means that would independently afford Mr. Ulbricht standing to suppress the Silk Road servers.

In that context, as the Horowitz Declaration establishes, the several versions the government has advanced to explain its identification and location of the Silk Road Servers simply do not pass muster – technically, temporally, or forensically. Thus, a determination regarding standing – and any requirement of an affidavit on Mr. Ulbricht's part – is decidedly premature.

Indeed, regarding the need for an evidentiary hearing to ascertain whether the Silk Road Servers were located through an illegal intercept (which could also resolve the standing issue), as codified in 18 U.S.C. §1304(a)(1), and subsequently held in *Gelbard*, 408 U.S. at 55, Mr. Ulbricht has a right to know whether he was ever the subject of illegal surveillance, and "it is clear both from the face of [§]3504 and from its legislative history that subsection (a)(1), impos[es] the . . . duty upon 'the opponent of the claim' to 'affirm or deny the occurrence of the alleged' illegal interception." *Id.*

Also, in *Gelbard* the Court explained that "subsection (a)(1) was supported [in Congress] on the ground that it would be beneficial to the victims of illegal interceptions" in that it "places upon the Government an affirmative duty to answer a claim that evidence is inadmissible because of unlawful investigative conduct" and thus "actually places or codifies a burden upon the Government, rather than the defendant." *Id.*

Accordingly, since the Court has not yet resolved the above described threshold issues which are central to Mr. Ulbricht's current round of motions, it would be premature for the Court

to decide the issue of standing without first holding an evidentiary hearing or directing the government to produce verifiable evidence of just how it identified and located the Silk Road Servers.

E. ***The Government's Legal Analysis With Respect to Electronically Stored Information Is Mired Hopelessly and Fatally In the Distant Past, and Fails Entirely to Address or Even Mention Either the Critical Series of Supreme Court Opinions Regarding the Fourth Amendment's Application to Digital Information Stored on Electronic Devices, and/or the Implications of Capturing Metadata That In Functional Terms* Is *Content***

The government's concentration on the manner in which it gained access to the Silk Road Server, and its discredited explanation for something it claims is impervious to court review altogether, is perhaps a diversionary tactic because it cannot offer a meaningful defense for the subsequent warrants, seizures, and searches it conducted in the case – of Mr. Ulbricht's laptop, of his Facebook and Google accounts – and the Pen Registers/Trap and Trace monitoring it instituted – for all of which Mr. Ulbricht indisputably possesses standing and a legitimate expectation of privacy.

In its opposition, the government fails even to mention, much less distinguish, *Riley* and *Jones*, the watershed Supreme Court decisions issued in the past two years, or the Eleventh Circuit's decision in *United States v. Davis*, ___ F.3d ___, 2014 WL 2599917 (11th Cir. 2014), *reh'g en banc granted*, ---- Fed.Appx. ----, 2014 WL 4358411 (11th Cir. Sept. 4, 2014), in which rehearing *en banc* has since been granted, but which still substantially informs the issue(s) and the direction of the courts in the context of seizures and searches of electronically stored information.[14]

[14] Stephen Treglia, "Decisions Limit Government's Access to Stored Digital Data," *New York Law Journal*, July 29, 2014, available at http://www.newyorklawjournal.com/id=1202664859137/Decisions-Limit-Governments-Access-to-Stored-Digital-Data?slreturn=20140830205541.

Unable to generate any argument to counter the position and analysis set forth in Mr. Ulbricht's initial Memo of Law, or the clear mandate for the courts implicated by both *Riley* and *Jones*, the government has chosen instead to ignore them. That omission constitutes surrender on a legal, doctrinal, and intellectual level, and by itself should be dispositive.

1. *The Government's Equating Telephone Number With Internet Routing Information Is Fallacious Factually and Insupportable Legally*

Also, even on a factual level, the government clings to an obsolete categorization that finds some delineating, but false, distinction between "content" and the information it collected. *See* Government's Memo of Law, at 5 (claiming Pen Registers "did not include the contents of any communications"); *id.*, at 18 ("[t]he Pen Registers did not collect the contents of Ulbricht's Internet communications, or anything that might arguably be characterized as contents"). Yet neither did the government collect what the government arbitrarily denominates as "content" in *Riley*, or *Jones*, or *Davis*. Nevertheless, Fourth Amendment protections applied in each case. *See* Mr. Ulbricht's initial Memo of Law, at 21-27.

The government's refrain regarding "content" would prevail if it were still 1979, when *Smith v. Maryland* was decided. Today, though, as *Riley*, *Jones*, and *Davis* [as well as *Kyllo* and *Florida v. Jardines*, ___ U.S. ___, 133 S. Ct. 1409 (2013), by extension, particularly in light of the subsequent cases], recognize that the government's collection of "the IP addresses to which Ulbricht was connecting, and the dates, times, and durations of those connections[,]" *see* Government's Memo of Law, at 18, implicates *content*, and deserves Fourth Amendment protection. *See also* Mr. Ulbricht's initial Memo of Law, at 45-48.

Indeed, what the government itself describes mirrors what the government collected in *Jones* via the GPS device employed in that case – the when, where, and how long – only more

so, as here the identity of IP addresses provides a significant measure of "content." *See Jones*, 132 S. Ct. at 955-56.

Similarly, while, in its Memo of Law, at 5, the government contends it "did not use the Pen Registers to track [Mr. Ulbricht's] physical location[,]" that is pure semantics. The information from the pen registers, which included monitoring routers at specific locations, and specific Mac addresses, had the effect of also providing Mr. Ulbricht's physical location. *See* Mr. Ulbricht's initial Memo of Law, at 39, 43. As described in the affidavits in support of the October 1, 2013, applications to search Mr. Ulbricht's laptop and residence, at ¶ 28 (in each), the locations of specific routers monitored via the pen registers enabled the government to geo-locate Mr. Ulbricht.

Moreover, the government's argument that "[t]his is data that any Internet user necessarily reveals to his Internet service provider, as the provider needs it to properly route the user's Internet traffic to and from his computer[,]" *see* Government's Memo of Law, at 18, simply ignores the past decade of jurisprudence. Conversely, the government's categorical reliance on *Smith v. Maryland* – despite all the evidence that it has been superseded by technology and social mores, as well as by the Supreme Court's recognition that *Smith*'s premise is outdated and does not reflect current Fourth Amendment culture.

Relying almost exclusively on *Smith* and *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008), the government begins with the premise that the Supreme Court "long ago affirmed that a warrant is not constitutionally required for pen register information." Government's Memo of Law, at 19-20.

However, in order to ignore the clear reasoning of the recent Supreme Court decisions in

United States v. Jones and *Riley v. California*, the government must parrot the untenable analogy, drawn in *Forrester*, that the routing information and IP addresses collected by the pen registers here provide the government no more information than the mere phone numbers dialed to and from a landline telephone, the focus of *Smith v. Maryland*, 442 U.S. at 745-46.

Indeed, that inapposite comparison is undermined even by the reasoning and facts in *Smith v. Maryland*, and is completely annihilated by the more recent Supreme Court decisions in *Jones* and *Riley*. For example, while the Court in *Smith* did hold that subscribers' expectation of privacy in the numbers dialed to and from a land line telephone was nil, the Supreme Court's comfort in this conclusion was buttressed by the fact that the collection of these numbers did not reveal any underlying information which could be characterized as "content," impermissible without a warrant under the Fourth Amendment. 442 U.S. at 742. The Supreme Court noted that information collected by the pen registers did not reveal even whether a phone call had been completed, let alone indicate anything about the "purport of any communication" between the callers. 442 U.S. at 741. *See also* Mr. Ulbricht's initial Memo of Law, at 39-40.

Building precariously on that faulty foundation, the government adopts the conclusion in *Forrester* that an "educated guess" about a user's Internet activity based on routing information and IP addresses, "is no different from speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed." 512 F.3d at 503. Yet, even without the subsequent acknowledgment in *Jones* and *Riley* that the changing landscape of technology implicates the privacy expectations underlying the Fourth Amendment in unanticipated ways, that comparison is intolerably strained.

As a threshold matter, the scope of information that can be gleaned from Internet routing

information allows for a profile of an individual's activity far more concrete and comprehensive than the "speculation" to be made about a phone call, of undisclosed duration, to or from a number which *may* be identifiable as someone or something that could indicate the content of the communication. *Forrester*, 512 F.3d at 510.

While it may be true that the information collected is similarly, and necessarily, conveyed to a third party, the Supreme Court has time and again recognized that the Fourth Amendment's protection very rarely boils down to bright line rules that cannot account for changing or novel circumstances. *See e.g. United States v. Chadwick*, 433 U.S. 1, 9 (1977); *see also Riley*, 134 S. Ct. at 2485.

As noted in Mr. Ulbricht's initial Memo of Law, at 41-42, even the Court in *Forrester* cautioned that "techniques . . . enabl[ing] the government to determine not only the IP addresses . . . but also the uniform resource locators ('URL') of the pages visited might be more constitutionally problematic." *Id.*, at 510, n. 6.

The government response is simply to create a straw man, denying that the pen registers here collected "things like the website addresses of the 'New York Times . . . articles' Ulbricht viewed or the 'search phrases' . . . entered into Google," but as Mr. Ulbricht's initial Memo of Law points out, at 39-40, *Smith* justified its conclusion only *because of* the very limited and neutral nature of the information (*i.e.*, phone numbers) collected by the pen register at issue. In the context of the Internet, however, the complexity of the distinction between content and routing information renders it a blunt, imprecise, and outdated analysis, and implicates the very Fourth Amendment concerns articulated in *Riley* and *Jones*. *See* Mr. Ulbricht's initial Memo of Law, at 40-43.

Thus, the government's attempts to treat IP addresses and similar routing information as nothing more complicated than a telephone number, and the cases cited in support of that premise, serve only to demonstrate the inconsistencies inexorably generated by (the government's) treating Internet communications like the straightforward telephone landline networks analyzed in *Smith*. Government's Memo of Law, at 20.

First, although ultimately concluding that the collection of IP addresses does not implicate Fourth Amendment concerns, the District Court in *In re Application of the U.S. for an Order Authorizing Use of a Pen Register and Trap on [xxx] Internet Service Acc't*, 396 F. Supp.2d 45 (D.Mass. 2005), expressed wariness with respect to the ease of distinguishing content from addressing information in the context of the Internet. *Id*., at 47-49.

Despite the Court's "acknowledged dearth of technological savvy," it cited three examples of what it considered obvious blending of content and routing information, including the inclusion in a URL of search terms typed into a search engine, the information contained in a "subject" line of an e-mail, and typing a bank account or credit card number into a website. *Id*., at 49.

Furthermore, the other case cited by the government, *In re Nickelodeon Consumer Privacy Litigation*, 2014 WL 3012873 (D.N.J. Jul. 2 2014), although decided almost ten years later, does little to clarify the boundary between content and addressing information in the context of Internet communications. In that case, the District Court characterized content as "information the user intended to communicate, such as the spoken words of a telephone call." *Id*., at * 14, *citing In re: Google Inc. Cookie Placement Consumer Privacy Litigation*, 988 F.Supp.2d 434, 443 (D.Del. 2013). The Court thus concluded that a URL containing the title of

a video, which provides the location of a single video, was not content because the URL described the "physical" location of the video on the servers. *Id*. Drawing a comparison to an individual requesting a video title over the phone, which would be "the 'substance, purport, or meaning' of the call itself," the Court held that because URL's are "static descriptions" that do not change, they are "more akin to "identification and address information'." *Id*., at *15.

However, the title of a video, conveyed to a video store clerk over the phone, is also a "static description" used to identify one video from among thousands of other videos, and the fact that the title of a video was conveyed using words, rather than a URL, does not alter the communication in any significant way. The distinction the District Court makes is illusory, and only further illustrates that limiting the Fourth Amendment's application to a particular facet of Internet communications by using an analysis developed with telephone communications in mind is inappropriate.

Thus, the government's attempt to rely solely on an analogy between Internet and phone communications, as analyzed in *Smith*, only accentuates the importance of the message conveyed by *Jones* and *Riley*: of adapting Fourth Amendment jurisprudence to changing technology, rather than attempting to force the rapidly changing nature of communications into outdated categories of protection. *See e.g. Jones*, 132 S. Ct.at 957 (Sotomayor, J., concurring); *see also Riley*, 134 S.Ct. at 2484-85.

As set forth in more detail in Mr. Ulbricht's motion, at 45-48, the information obtained here through warrantless pen registers is protected under the Fourth Amendment for the same reasons that the information collected in *Jones* and *Riley* fell within the warrant requirement, even despite the "voluntary" disclosure of information to third party providers.

2. *The Government's Legal Analysis Fails to Understand the Intractable Problem with General Warrants, and That the Warrants In This Case Violated the Fourth Amendment Because They Were General Warrants* By Design

In addition, the warrants issued in this case did not simply authorize a "cursor[y]" search of documents, "in order to determine whether they are, in fact, among those papers authorized to be seized," as the government argues in its Response, at 23. *Andresen v. Maryland*, 427 U.S. 463, 482, n.1 (1976). Rather, the warrants impermissibly authorized the government to scour the entirety of the servers, Mr. Ulbricht's laptop, email and Facebook accounts, for any evidence implicating Mr. Ulbricht in the "subject offenses," in flagrant violation of the Fourth Amendment's particularity requirement.

As discussed in Mr. Ulbricht's initial Memo of Law, at 53, the objection to the unfettered discretion provided by the warrants in this case does not arise from the practice of permitting "the seizure or copying of hard drives and other storage devices in order to effectuate a proper search for the categories of documents or files listed in a warrant." *See* Government's Memo of Law, at 22, *citing In the Matter of a Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx gmail.com Maintained at Premises Controlled By Google, Inc.*, 14 MAG. 309, 2014 WL 3583529, at *5 (S.D.N.Y. July 18, 2014), as amended (Aug. 7, 2014).

This "routine practice," referenced by the government, is merely the initial seizure of a server or hard drive in order to perform an off-site search, executed within the bounds of a properly limited warrant. *Id*., citing *United States v. Burns*, 2008 WL 4542990, at *5 (N.D.Ill. April 29, 2008) ("[c]ourts have found that seizure of computer equipment before search is reasonable given the complexities of electronic searches, as long as the requirements of the Fourth Amendment are met").

Neither is the objection to the search warrants based on the failure to segregate documents and information related to legitimate activity from illegitimate activity, but rather the utter lack of guidance in the search warrant as to what fell within each category. *See* Mr. Ulbricht's initial Memo of Law, at 56. In that respect, the cases cited by the government are inapposite.

For instance, reliance on the "all records" doctrine cannot save a general warrant from constitutional infirmity. *See e.g. United States v. Bowen*, 689 F. Supp.2d 675, 685, n.6 (S.D.N.Y. 2010) ("[t]he principle is not so much an 'exception' to the particularity requirement of the Fourth Amendment as a recognition that a warrant-no matter how broad-is, nonetheless, legitimate if its scope does not exceed the probable cause upon which it is based"), *quoting United States v. Hickey*, 16 F. Supp.2d 223, 240 (E.D.N.Y. 1998). Even demonstrating that a business is "pervaded" by criminal activity does not authorize a search of every record for *any* evidence of the offenses in violation of the Fourth Amendment.

Regarding the constitutional objections to the warrants authorizing searches of Mr. Ulbricht's laptop, Google and Facebook accounts, the government responds by pointing to the "numerous categories of evidence" listed in the search warrants. *See* Government's Memo of Law, at 27. However, those lists are so "extensive" as to provide virtually "'no assurance that the permitted invasion of a suspect's privacy and property are no more than absolutely necessary.'" *United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013), *quoting United States v. George*, 975 F.2d 72, 76 (2d Cir. 1992).

Indeed, the expansiveness of the government's position, expressed in its Memo of Law, at 25, is breathtaking: "*all* of the transactions reflected in the database *are* relevant to the case[]"

(emphasis in original) – and that was before the government reviewed even a single transaction or piece of data.[15] While, the government, in its Memo of Law, at 26, acknowledges that a general warrant "fails to specify the scope of an authorized search *at all*[,]" it nevertheless proceeds to argue that somehow a search that simply announces that its scope is unlimited escapes categorization as a general warrant.

Yet a general warrant need not be surreptitious; a warrant that is overtly without limits is just as offensive as one that is written properly but executed in an unrestricted manner. Nor, contrary to the government's claim, in its Memo of Law, at 28, is "clear language" a solution, particularly when that "clear language" seeks a search without any boundaries.

The government nonetheless clings tightly to the notion that particularity is satisfied as long as the warrant does not altogether fail to provide limits, either as in *United States v. Buck*, 813 F.2d 588, 590 (2d Cir. 1987), which held insufficient a warrant that "gave no limitation whatsoever on the kind of evidence sought," *id*. at 592, or in *Galpin*, which referenced only violations of the criminal law, and included no further information regarding the offenses to which the evidence related. 720 F.3d at 447.

Yet here there were no such limits. For example, if searching a person's entire history of communications to compare when he wrote "yeah" and "yea" could justify an untrammeled search, then limitless searches will become commonplace. *See* Government's Memo of Law, at 29. Likewise, looking for *any* patterns in language, or *any* patterns of movement, are

---

[15] In defending the misrepresentations in the warrant applications, the government, in its Memo of Law, at 22, creates another straw man in contending that Mr. Ulbricht's "premise appears to be that a search or seizure of the records of a criminal enterprise cannot encompass records reflecting any aspect of the enterprise that is not inherently unlawful." That is *not* Mr. Ulbricht's point, which, instead, is *do not mislead the Magistrate Judge*.

functionally without definition, and therefore without limit.

In addition, the same result may be accomplished with too little information as with too much. Especially in the context of computer files and electronic information, which, for instance, "may contain intimate details regarding an individual's thoughts, beliefs, and lifestyle," leaving the determination of what may be searched and seized to the discretion of the officials executing the search is impermissible under the Fourth Amendment. *United States v. Ganias*, ___ F.3d ___, 2014 WL 2722618, at *7 (2d Cir. June 17, 2014); *see also Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 325 (1979).[16]

Similarly, avoiding "simply leaving it to the agents' discretion what may be seized," *see* Government's Memo of Law, at 28, *citing United States v. George*, 975 F.2d at 75, by having the *warrant itself* permit wholly indiscriminate search and seizure of *everything* (thereby certainly eliminating an agent's discretion) does not save a general warrant from invalidity. It merely amplifies that invalidity.

That discretion is impermissibly authorized just as completely by the language cited by the government in *Buck* ("any papers, things or property of any kind relating to [the] previously described crime"), as by the all encompassing lists in the warrants here, which were additionally prefaced with the language "including but not limited to." *Buck*, 813 F.2d at 590; *see also* Government's Response, at 27-28, n.7.

As is the case here, a warrant that provides "so vague a description of the material sought as to impose no meaningful boundaries" violates the Fourth Amendment. *United States v. Cioffi*,

---

[16] The government fails altogether to mention *Ganias*, another recent Second Circuit decision regarding the permissible scope of searches of electronically stored information. *See also* Mr. Ulbricht's initial Memo of Law, at 21-33.

668 F. Supp.2d 385, 390 (E.D.N.Y. 2009), *quoting United States v. Cohan*, 628 F. Supp.2d 335, 359 (E.D.N.Y. 2009).

Also, while the government cites, in its Memo of Law, at 30, the doctrine of deference to the issuing magistrate, such deference is not categorical; otherwise a district court's review, and the Fourth Amendment protections inherent therein, would be eviscerated and/or meaningless.

3. *The Good Faith Doctrine Cannot Save a General Warrant*

The good faith exception articulated in *United States v. Leon*, 468 U.S. 897 (1984), and cited in the Government's Memo of Law, at 31, is unavailable to salvage a deficient search warrant in four situations: "(1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable." *United States v. Clark*, 638 F.3d 89, 100 (2d Cir. 2011), *quoting United States v. Moore*, 968 F.2d 216, 222 (2d Cir.1992).

As the Second Circuit explained in *George*, 975 F.2d at 77-78, general warrants, which authorize impermissibly unlimited searches and seizures, are facially deficient, and therefore, cannot be saved by the good faith exception in *Leon*. 975 F.2d at 77-78; *see also Leon*, 468 U.S. at 923. The opinion in *George* specifically addressed warrants that do not sufficiently articulate the crime or criminal activity to which the seizable evidence relates, but the Court also pointed out that it "cautioned" in *Buck*, 813 F.2d at 593 n. 2, that after *Buck* "police officers may no longer invoke the reasonable-reliance exception to the exclusionary rule when they attempt to introduce as evidence the fruits of searches undertaken on the basis of warrants containing only a

catch-all description of the property to be seized."

Consequently, the inapplicability of the good faith exception to the warrants at issue here is manifest. *See e.g. Roberts v. United States*, 656 F. Supp. 929, 934-35 (S.D.N.Y. 1987) (warrant invalid because "[b]y listing every type of record that could conceivably be found in an office . . . the warrant violated the cardinal rule of Fourth Amendment law"), *rev'd on other grounds by United States v. Roberts*, 852 F.2d 671 (2d Cir. 1988); *see also In re Grand Jury Proceedings*, 716 F.2d 493, 498 (8th Cir. 1983) (deeming a warrant "general" because it authorized seizure of a "laundry list of various type of records," without "designations or references to particular transactions or to specific individuals or specific files, or to a reasonably specific time [period]").

In addition, here, since the government in effect concedes that the unrestricted nature of the warrants was *by design*, and not inadvertent, the concept of "good faith" does not apply. The absence of any particularity in these warrants simply defies any claim of good faith. Nor can the government, as it apparently argues in its Memo of Law, at 32, present a patently general warrant and then blame the Magistrate Judge for signing it. Also, the cases it cites, at 32, *United States v. Falso*, 544 F.3d 110, 129 (2d Cir. 2008), and *United States v. Cancelmo*, 64 F.3d 804, 807 (2d Cir. 1995), are distinguishable because those cases involved a challenge to the probable cause determination, and not the scope of the warrant.

4. *The Warrants Are Not Severable*

In its Memo of Law, at 32-33, the government maintains the warrants, if invalid, are severable. However, again, that misapprehends the evil of general warrants. Indeed, any purportedly valid portion of the warrants are inseparable from those that violate the Fourth

Amendment because *there are no boundaries between them* – the *entire* warrant is indistinguishable.

Any other conclusion would simply encourage the government to present for approval *only* general warrants, and then, if subsequently (successfully) challenged by a defendant, simply retain for use what would have been permissible to search or seize if the warrant had been properly drawn. That is a perversion of the exclusionary rule, deterrence, and the Fourth Amendment.

As Judge Gleeson recognized in *United States v. Simels*, not reported in F. Supp.2d, 2009 WL 1924746 (E.D.N.Y. July 2, 2009), in the context of the failure to minimize interception of legitimate attorney-client conversations recorded pursuant to a defective Title III electronic eavesdropping warrant, the wholesale failure to minimize required wholesale suppression. *Id*., at 13-15.

Similarly, conceptually, a general warrant defies severability, and the warrants here are not severable because they are infected in their entirety and, indeed, deliberately in their conception.

POINT II

THE COURT SHOULD COMPEL THE GOVERNMENT TO PRODUCE THE REQUESTED DISCOVERY

The government contends that Mr. Ulbricht has "lard[ed] his motion with over twenty sweeping discovery requests, which he claims are 'necessary to assist defense counsel in determining whether any information gathered during the course of the government's investigation was obtained in violation of [his] rights pursuant to the Fourth Amendment" and

that these requests should be denied on the basis that Mr. "Ulbricht failed to make any specific showing of materiality that would justify these requests." Government's Memo of Law, at 34. In support of its position the government cites Second Circuit case law for the proposition that "a defendant bears the burden of making a *prima facie* showing that any documents he seeks under Rule 16(a)(1)(E) are material to preparing a defense." *Id., quoting United States v. Maniktala*, 934 F.2d 25, 28 (2d. Cir. 1991).

Mr. Ulbricht has more than met his burden. Indeed, the Horowitz Declaration, submitted in conjunction with this Reply, provides not only a *prima facie* showing, but unimpeachable proof that the government has failed to provide adequate discovery and explanation as to how it obtained the Silk Road server, which is necessary and material to Mr. Ulbricht's preparation of his defense.

Moreover, the discovery demands contained in Mr. Ulbricht's initial motion, as well as in a subsequent September 17, 2014, letter from Joshua L. Dratel, Esq., to AUSAs Serrin Turner and Timothy Howard, attached to the Horowitz Declaration as Exhibit 3, are not sweeping, but rather targeted to fill the holes in the government's discovery and in its explanation as to how the FBI was able to locate the Silk Road server.

For instance, former SA Tarbell's Declaration, submitted in response to only a small portion of Mr. Ulbricht's discovery demands, has introduced whole categories of material discovery, such as pen register data and traffic and communication logs for the Icelandic server assigned IP address 193.107.84.4, that the defense was not previously aware even existed, and which the defense has since requested from the government (as part of the September 17, 2014, set of demands), and is now in the process of reviewing and evaluating.

Still other categories of material discovery flow logically from the government's claims as to how it obtained access to the server, but which have not yet been turned over to defense counsel (for reasons set forth in the government's September 23, 2014, response to the September 17, 2014, demands), not to mention potentially untold quantities of discovery that could be revealed if the government were to respond to the many other discovery demands set forth in Mr. Ulbricht's initial motions.

Accordingly, the fruit borne by the few requests to which the government has been responsive justifies Mr. Ulbricht's tailored requests for additional discovery pursuant to Rule 16, Fed.R.Crim.P., *Brady v. Maryland*, 373 U.S. 83 (1963) and/or *Giglio v. United States*, 405 U.S. 150 (1972). The government's failure to adequately respond to Mr. Ulbricht's discovery demands also buttresses Mr. Ulbricht's request for an evidentiary hearing.

POINT III

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

In opposing Mr. Ulbricht's demand for a Bill of Particulars, the government has attempted the classic "bait and switch." In opposing Mr. Ulbricht's pretrial motions challenging the Indictment, the government insisted that merely tracking the language of the specific statutes sufficed. *See* Government's Memo of Law in Response to Defendant's Pre-Trial Motions Challenging the Face of the Indictment (Dkt #26), at 6-7. Yet now, according to the government, that bare bones indictment somehow provides Mr. Ulbricht sufficient notice of the precise nature of the charges therein.

The government cannot have it both ways. Having defended the Indictment

(successfully) on the ground that its spare language was sufficient, it cannot now claim that a Bill of Particulars is unwarranted because the Indictment provides the necessary detail. For example, Count Four, which charges a violation of 21 U.S.C. §848(a), remains a moving target, as the government refuses to enumerate the three offenses it will use – and ostensibly presented to the grand jury – to establish that particular element of the offense.

Thus, the government's claim, in its Memo of Law, at 43, that "[t]here is simply no mystery here concerning the nature of the charges Ulbricht is facing or the nature of the evidence supporting those charges[,]" (citations omitted) is astonishing in light of the lack of specific information about an essential element for Count Four.

The government's attempted sleight of hand extends as well to its legal arguments. For instance, in its Memo of Law, at 39, it cites *United States v. bin Laden*, 92 F.Supp.2d 225, 242 (S.D.N.Y. 2000), in which the District Court *granted* a Bill of Particulars, noting that case law on the subject is of limited value because of the fact-specific context of individual cases, and ordering the Bill of Particulars because, in part, of the defense's difficulty in finding the particular alleged criminal conduct within the vast scope of discovery. *Id.*, at 234-35.

Also, the government's contention that its production of discovery resolves the issue (of the necessity for a Bill of Particulars) is not only not an adequate answer, but it completely reverses the reality of the situation. In fact, the quantum of discovery *is*, in many respects, the *problem*: the government has provided the defense with at least six terabytes of information that, within the time frame allotted, cannot be reviewed by even an army of lawyers or staff (resources the defense does not possess).

Moreover, the government failed to provide a substantial volume of discovery that the

defense realized existed (and had not been provided) only by reading the government's response to these motions. As a result, the defense has submitted a supplemental discovery demand to the government, which has agreed to produce at least some of the designated items (but has not yet responded to the letter as a whole). *See* September 17, 2014, Letter from Joshua L. Dratel, Esq. (Exhibit 3 to the Horowitz Declaration).[17]

POINT IV

THE COURT SHOULD STRIKE IRRELEVANT AND PREJUDICIAL SURPLUSAGE FROM THE INDICTMENT

Regarding Mr. Ulbricht's motion to strike surplusage from the Indictment, that request is reinforced by the government's failure to include in the Superseding Indictment formal, statutory charges relating to the alleged murder-for-hire plots. Accordingly, it is respectfully submitted that Mr. Ulbricht's motion should be granted, and the offending language stricken from the Superseding Indictment.

[17] As noted **ante**, at n. 1, the impact of the Superseding Indictment, as well the government's supplemental and continuing discovery, on Mr. Ulbricht's motion for a Bill of Particulars will be addressed in his motions responding to the Superseding Indictment.

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, or conduct an evidentiary hearing, and for discovery, for a bill of particulars, and to strike irrelevant and prejudicial surplusage from the Indictment, in their entirety.

Dated: 30 September 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

Joshua J. Horowitz
225 Broadway, Suite 1804
New York, New York 10007
(845) 667-4451

Attorneys for Defendant Ross Ulbricht

– Of Counsel –

Joshua L. Dratel
Lindsay A. Lewis
Whitney G. Schlimbach
Joshua J. Horowitz