UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
-v-	:	14-cr-68 (KBF)
ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road,"	:	OPINION & ORDER
Defendant.	:	

KATHERINE B. FORREST, District Judge:

On February 4, 2014, Ross Ulbricht ("defendant" or "Ulbricht") was indicted on four counts. (ECF No. 12.) On September 5, 2014, he was arraigned on superseding indictment S1 14 Cr. 68 (KBF) (the "Indictment"). The Indictment charges Ulbricht with the following crimes: Narcotics Trafficking (Count One), Distribution of Narcotics by Means of the Internet (Count Two), Narcotics Trafficking Conspiracy (Count Three), Continuing Criminal Enterprise ("CCE") (Count Four), Conspiracy to Commit and Aid and Abet Computer Hacking (Count Five), Conspiracy to Traffic in Fraudulent Identification Documents (Count Six), and Money Laundering Conspiracy (Count Seven). (ECF No. 52 ("Ind.").) Ulbricht's trial is scheduled to commence on November 10, 2014.

Before this Court is defendant's motion to suppress virtually all evidence in the case, for a bill of particulars, and to strike surplusage. (ECF No. 46.) For the reasons set forth below, the motion is DENIED.

I. BACKGROUND

A. Allegations against Ulbricht

Ulbricht is charged with seven separate crimes—all involving the creation, design, administration and operations of an online marketplace known as "Silk Road." The Government alleges that Ulbricht created Silk Road (Ind. ¶ 1) and that he has been in control of all aspects of its administration and operations (Ind. ¶ 3). The Government's charges against Ulbricht are premised upon a claim that through Silk Road, defendant enabled and facilitated anonymous transactions in a variety of illicit goods and services including, inter alia, narcotics, fake identification documents, and materials used to hack computers, and that he conspired, participated directly in, or aided and abetted others in substantive crimes.

Silk Road is alleged to have operated on the Tor network ("Tor"). (Declaration of Christopher Tarbell ¶¶ 4-5, ECF No. 57 ("Tarbell Decl.").) The Tor network is designed to conceal the Internet Protocol ("IP") addresses of the computers operating on it, "including servers hosting websites on Tor, such as Silk Road." (Tarbell Decl. ¶ 4.) The Government alleges that Silk Road also supported anonymity through its reliance on "Bitcoin" as a method of payment.[1] (Ind. ¶ 28.) The use of Bitcoins concealed the identities and locations of users transmitting and receiving funds. (Ind. ¶ 28.) The Government alleges that over the period of time it was up and running, Silk Road was used by several thousand drug dealers and well over one hundred thousand buyers worldwide to purchase illegal narcotics and

[1] Bitcoin is the name of an encrypted online currency. It is managed through a private network and not through any Government, central bank or formal financial institution. The Government does not allege that the use of Bitcoin itself is illegal.

illicit goods, and that it was also used to launder hundreds of millions of dollars derived from these transactions. (Ind. ¶ 2.) Ulbricht himself is alleged to have made commissions worth tens of millions of dollars from these sales. (Ind. ¶ 3.)

B. The Investigation of Ulbricht

The instant motion is primarily concerned with whether the Government's methods for investigating Ulbricht violated his Fourth Amendment right to be free from unreasonable searches and seizures. Importantly, while the Government alleges that Ulbricht and Silk Road are one and the same, Ulbricht has not conceded that he created Silk Road, or that he administered or oversaw its operations, or even that he used or accessed it at all. Ulbricht has not submitted a declaration or affidavit attesting to any personal privacy interest that he may have in any of the items searched and/or seized and as to which his motion is directed. Ulbricht's lawyer has, however, argued that his "expectation of privacy in his laptop, Google or Facebook accounts" is "manifest" (ECF No. 83 at 2 n.2), and the Government has stipulated to his "expectation of privacy" in those (ECF No. 85).[2]

The Government's investigation involved, inter alia, the imaging and subsequent search of a server located in Iceland (the "Icelandic server") in July 2013. Based in large part on the results of information learned from the Icelandic server, the Government then obtained various court orders for pen-registers and trap and trace devices (the "Pen-Trap Orders"), and warrants to seize and then

[2] On October 7, 2014, the Court issued an order in which it provided the defendant a "final opportunity" to submit a declaration or affidavit establishing some privacy interest in the items searched and/or seized. (ECF Nos. 76-77.) By letter dated October 7, 2014, his lawyer responded that "Mr. Ulbricht rests on his papers already submitted." (ECF No. 83.)

search a number of other servers located within the United States, as well as a laptop associated with Ulbricht and his Facebook and Gmail accounts. In total, the Government obtained 14 warrants and court orders over the course of its investigation. (Declaration of Joshau L. Dratel ¶ 3(a)-(n), ECF No. 47 ("Dratel Decl.").) Those warrants and orders are as follows:

Warrant No. 1: Windstream "JTan" server #1 (Pennsylvania) (9/9/13);

Warrant No. 2: Windstream "JTan" server #2 (Pennsylvania) (9/9/13);

Warrant No. 3: Voxility server (California) (9/19/13);

Warrant No. 4: Windstream servers assigned host numbers 418, 420 and 421 (Pennsylvania) (10/1/13);

Warrant No. 5: Voxility server with IP addresses 109.163.234.40 and 109.163.234.37 (California) (10/1/13);

Warrant No. 6: Samsung laptop with MAC address 88-53-2E-9C-81-96 (California) (10/1/13);

Warrant No. 7: Premises at 235 Monterey Boulevard (California) (10/1/13);

Warrant No. 8: The Facebook account associated with username "rossulbricht" (California) (10/8/13);

Warrant No. 9: The Gmail account rossulbricht@gmail.com (10/8/13);

Pen-Trap Order No. 1: To Comcast re IP address 67.170.232.207 (9/16/13);

Pen-Trap Order No. 2: To Comcast re IP address 67.169.90.28 (9/19/2013);

Pen-Trap Order No. 3: Re the wireless router with IP address 67.169.90.28 located at 235 Monterey Boulevard (California) (9/20/13);

Pen-Trap Order No. 4: Re certain computer devices associated with MAC addresses including 88-53-2E-9C-81-96, (9/20/13); and

Pen-Trap Order No. 5: Re the wireless router with IP address 67.169.90.28 located at 235 Monterey Boulevard (California) (9/19/13).

According to defendant, virtually all of the Government's evidence stems from the initial search of the Icelandic server in July 2013, which occurred before any of the above warrants issued.[3] The vast bulk of defendant's submission is concerned with raising questions regarding how the Government obtained the information that led it to the Icelandic server. One of defendant's lawyers, Joshua Horowitz, has some technical training, and he asserts that the Government's explanation of the methods it used is implausible. (See Declaration of Joshua J. Horowitz ¶¶ 4-8, 17-51, ECF No. 70 ("Horowitz Decl.").) Defendant insists that this Court must therefore hold an evidentiary hearing to determine whether the methods the Government asserted it used and that led it to the Icelandic server were in fact its actual methods or not. (See 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 at 28-34, ECF No. 48 ("Def.'s Br."); 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 at 4-8, ECF No. 69 ("Def.'s Reply Br.").) Defendant argues that if that search of the Icelandic server was only possible

[3] U.S. law enforcement began working with law enforcement in Iceland on this investigation as early as February 2013. A server—later determined to no longer be in primary use—was imaged in the spring or early summer of 2013 ("Icelandic Server #1"). Ulbricht asserts that the process leading to the imaging of the server may also have been constitutionally infirm. But Icelandic Server #1 is in all events irrelevant, as the Government has represented that it does not intend to use any evidence obtained from that server.

because of a preceding constitutionally infirm investigation, then all subsequent warrants and court orders based on that search constitute fruits of the poisonous tree and must be suppressed.

In addition, defendant also asserts that the warrants relating specifically to the servers located in Pennsylvania (nos. 1, 2 and 4) as well as the warrants relating to Ulbricht's laptop, Facebook and Gmail accounts (nos. 6, 8 and 9) are unconstitutional general warrants; and finally that the Pen-Trap Orders were unlawful because a warrant was required and they failed to include appropriate minimization procedures. Defendant has retained experienced counsel who certainly understand Fourth Amendment jurisprudence. It has long been established—indeed, it is a point as to which there can be no dispute—that (1) the Fourth Amendment protects the constitutional right of an individual to be free from unreasonable searches and seizures; (2) the rights conferred by the Fourth Amendment may not be vicariously asserted; and (3) the Fourth Amendment does not confer any general right available to anyone impacted by an investigation to pursue potentially or actually unlawful law enforcement techniques. The only exception to that is extremely narrow: when law enforcement techniques are so egregious (defined as actions such as torture, not simply unlawful conduct) as to violate the Fifth Amendment, a court may suppress the evidence.

Defendant has not asserted a violation of the Fifth Amendment—nor could he. Defendant has, however, brought what he must certainly understand is a fatally deficient motion to suppress. He has failed to take the one step he needed to

take to allow the Court to consider his substantive claims regarding the investigation: he has failed to submit anything establishing that he has a personal privacy interest in the Icelandic server or any of the other items imaged and/or searched and/or seized. Without this, he is in no different position than any third party would be vis-à-vis those items, and vis-à-vis the investigation that led U.S. law enforcement officers to Iceland in the first place.

There is no doubt that since defendant was indicted and charged with seven serious crimes resulting from that initial investigation and the searches that followed it, he has a "personal interest" in the Icelandic server in a colloquial sense. But longstanding Supreme Court precedent draws a stark difference between that sort of interest and what the law recognizes as necessary to establish a personal Fourth Amendment right in an object or place. To establish the latter, defendant must show that he has a personal privacy interest in the object (e.g., a server) or premises searched, not just that the search of the specific object or premises led to his arrest. Were this or any other court to ignore this requirement in the course of suppressing evidence, the court would undoubtedly have committed clear error.

Further, defendant could have established such a personal privacy interest by submitting a sworn statement that could not be offered against him at trial as evidence of his guilt (though it could be used to impeach him should he take the witness stand). Yet he has chosen not to do so.

In short, despite defendant's assertions and the potential issues he and his counsel raise regarding the investigation that led to the Icelandic server, he has not

provided the Court with the minimal legal basis necessary to pursue these assertions. Thus, the declaration submitted by Joshua J. Horowitz, Esq. (ECF No. 70) along with all the arguments regarding the investigation and the warrants based on it are not properly before this Court. The only arguments that this Court must consider as a substantive matter are those concerning property and accounts as to which defendant has an arguable and cognizable (though itself not legally established) personal privacy interest: the laptop, the Gmail account, and the Facebook account.[4]

II. SEARCHES AND SEIZURES

A. The Fourth Amendment

Ulbricht's motion to suppress evidence is premised upon an assertion that the Government has, or may have, engaged in one or more unreasonable searches and seizures in violation of the Fourth Amendment of the U.S. Constitution. The Fourth Amendment protects the people against unreasonable searches and seizures. U.S. Const. amend. IV. "Ever since its inception, the rule excluding evidence seized in violation of the Fourth Amendment has been recognized as a principal mode of discouraging lawless police conduct." Terry v. Ohio, 392 U.S. 1, 12 (1968). In the absence of a warrant or the applicability of an exception, law enforcement does not have a general right to enter one's home, rifle through drawers, and take what might be found therein. See, e.g., United States v. Jenkins, 876 F.2d 1085, 1088 (2d Cir. 1989).

[4] For reasons the Court does not understand, Ulbricht chose not to submit a declaration claiming any personal privacy interest and expectation of privacy in the search of 235 Monterey Boulevard or the wireless router located at those premises.

Evidence seized in violation of the Fourth Amendment is subject to exclusion at trial—hence, references to "the exclusionary rule" in Fourth Amendment jurisprudence. See, e.g., Terry, 392 U.S. at 13. Exclusion ensures judicial integrity and protects courts from being made a party to "lawless invasions of the constitutional rights of citizens by permitting unhindered governmental use of the fruits of such invasion." Id. Direct and indirect evidence may be subject to preclusion: all evidence that flows directly or indirectly from unlawfully seized evidence is considered "fruit of the poisonous tree." Wong Sun v. United States, 371 U.S. 471, 484-85 (1963) (the exclusionary rule of the Fourth Amendment extends to indirect evidence as well as direct evidence).

"[T]he Fourth Amendment protects people, not places." Katz v. United States, 389 U.S. 347, 351 (1967). In Katz, petitioner sought to suppress evidence of his end of a telephone call, obtained by the FBI after it placed a listening device on a public telephone booth. Id. at 348-50. The Supreme Court defined the issue not as one regarding whether a particular physical space was a constitutionally protected area, or whether physical penetration of a protected area was required for a Fourth Amendment violation. Id. at 350-51. This is important for this Court's consideration here of Ulbricht's claims. The Supreme Court in Katz then stated that the Fourth Amendment cannot be translated into a general constitutional "right to privacy," nor does it cover some nebulous group of "constitutionally protected area[s]." Id. A person's general right to privacy—his right to be let alone by other people—is, like the protection of his property and his very life, left largely

to the law of the individual states. Id. Thus, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." Id.

1. Foreign searches and seizures.

The law has long been clear that the protections of the Fourth Amendment do not extend to searches conducted outside the United States by foreign law enforcement authorities. See, e.g., United States v. Lee, 723 F.3d 134, 139 (2d Cir. 2013) ("[T]he 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."); United States v. Busic, 592 F.2d 13, 23 (2d Cir. 1978) ("[T]he Fourth Amendment and its exclusionary rule do not apply to the law enforcement activities of foreign authorities acting in their own country."); accord United States v. Peterson, 812 F.2d 486, 490 (9th Cir. 1987).

An exception to this rule is when foreign law enforcement authorities become agents of U.S. law enforcement officials. See Lee, 723 F.3d at 140 (constitutional requirements may attach "where the conduct of foreign law enforcement officials rendered them agents, or virtual agents, of United States law enforcement officials" (quoting United States v. Maturo, 982 F.2d 57, 61 (2d Cir. 1992))). If, for instance, U.S. law enforcement was able to and did command and control the efforts of foreign law enforcement, an agency relationship might be found. United States v. Getto, 729 F.3d 221, 224 (2d Cir. 2013) (holding that "ongoing collaboration between an American law enforcement agency and its foreign counterpart in the course of

parallel investigations does not—without American control, direction, or an intent to evade the Constitution—give rise to a relationship sufficient to apply the exclusionary rule to evidence obtained abroad by foreign law enforcement"). The foreign searches must, however, be "reasonable." In re Terrorist Bombings of U.S. Embassies in E. Africa, 552 F.3d 157, 167 (2d Cir. 2008) (holding that "foreign searches of U.S. citizens conducted by U.S. agents are subject only to the Fourth Amendment's requirement of reasonableness").[5] As the Supreme Court has explained:

> The test of reasonableness under the Fourth Amendment is not capable of precise definition or mechanical application. In each case it requires a balancing of the need for the particular search against the invasion of personal rights that the search entails. Courts must consider the scope of the particular intrusion, the manner in which it is conducted, the justification for initiating it, and the place in which it is conducted.

Bell v. Wolfish, 441 U.S. 520, 559 (1979).

2. Personal privacy interest.

Supreme Court precedent, binding on this and all courts in this land, establishes that the "capacity to claim the protection of the Fourth Amendment depends . . . upon whether the person who claims the protection of the [Fourth] Amendment has a legitimate expectation of privacy in the invaded place." Rakas v. Illinois, 439 U.S. 128, 143 (1978); see also United States v. Watson, 404 F.3d 163, 166 (2d Cir. 2005) (affirming denial of a suppression motion on the basis that the

[5] It is unclear whether foreign searches of objects or premises in which only non-citizens have a privacy interest are subject to the Fourth Amendment's reasonableness requirement. See United States v. Bin Laden, 126 F. Supp. 2d 264, 276 (S.D.N.Y. 2000) (collecting cases).

defendant had failed to show an expectation of privacy). This principle derives from the Supreme Court's holding in Katz v. United States, in which the Court found that while common law trespass had long governed Fourth Amendment analysis, the capacity to claim the protection of the Fourth Amendment depended first and foremost on a personal expectation of privacy in the invaded place. 389 U.S. at 352-53. The Court found that even though petitioner was located in a public telephone booth when the search occurred, "the Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied . . . and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment." Id. at 353.

The law therefore leaves no doubt that Fourth Amendment rights are based on a personal, subjective expectation of privacy; they are rights of a person, not rights of a "thing"—whether that thing be a server, a car, or a building. If a person—a human—cannot establish a cognizable personal expectation of privacy in the place or thing searched, there is no Fourth Amendment issue and no reason to undertake a Fourth Amendment analysis.

How, then, is one's interest in a place or thing established? It must be established by a declaration or other affirmative statement of the person seeking to vindicate his or her personal Fourth Amendment interest in the thing or place searched. See, e.g., United States v. Smith, 621 F.2d 483, 487 (2d Cir. 1980) (defendants had no legitimate expectation of privacy in trunk of car where they did not assert ownership of car, knowledge of trunk's contents, or access to trunk);

United States v. Montoya-Echevarria, 892 F. Supp. 104, 106 (1995) ("The law is clear that the burden on the defendant to establish [Fourth Amendment] standing is met only by sworn evidence, in the form of affidavit or testimony, from the defendant or someone with personal knowledge."); United States v. Ruggiero, 824 F. Supp. 379 (S.D.N.Y. 1993) ("It is well established that in order to challenge a search, a defendant must submit an affidavit from someone with personal knowledge demonstrating sufficient facts to show that he had a legally cognizable privacy interest in the searched premises at the time of the search."). The Supreme Court has also established that the defendant—not the Government—bears the burden of proving that he has a legitimate expectation of privacy. Rawlings v. Kentucky, 448 U.S. 98, 104 (1980); see also Watson, 404 F.3d at 166.

The requirement that one must have a personal expectation of privacy at the time of the search in the thing or place searched is not novel and has been repeatedly litigated. One can easily see why: even if one did not have an expectation of privacy at the time of the search, the search might lead to inculpatory evidence. At that point, the now-defendant might certainly desire that the thing or place searched had been left alone.

In Rakas, the Supreme Court reviewed the question of whether passengers in a vehicle that was searched could move to suppress the evidence obtained thereby. 439 U.S. at 130-32. In that case, the police received a report of a robbery and the description of a getaway car. Id. at 130. Shortly thereafter, an officer stopped and searched a vehicle matching that description. Id. The search revealed ammunition

and a firearm. Id. Petitioners had been passengers in the vehicle and were arrested following the search. Id. Neither the car nor the evidence seized belonged to them. Id. at 131. They moved to suppress the evidence on the basis that the search violated their rights under the Fourth Amendment. Id. at 130-31.

The question before the Court was presented as whether petitioners had "standing" to bring the suppression motion. Id. at 131-32. Petitioners urged the Court to relax or broaden the rule of standing so that any criminal defendant at whom a search was "directed" would have standing to challenge the legality of the search. Id. at 132. The Court recognized that prior case law (including Jones v. United States, 362 U.S. 257 (1960)) had discussed the concept of standing as whether the individual challenging the search had been the "victim" of the search. Petitioners in Rakas urged the Court to broaden the "victim" concept to a "target theory" of standing for Fourth Amendment purposes. Id. at 132-33. The Supreme Court declined to do so, reiterating that the law has long been clear that Fourth Amendment rights were personal rights which may not be vicariously asserted. Id. at 133-34. The Court recited numerous instances over time in which courts had rejected defendants' assertions that they were aggrieved by unconstitutional searches of third parties' premises or objects. Id. at 134 (collecting cases). "A person who has been aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by a search of a third person's premises or property has not had any of his Fourth Amendment rights infringed." Id. "[I]t is proper to permit only defendants whose Fourth Amendment rights have been

violated to benefit from the rule's protections." Id. The Court stated, "[c]onferring standing to raise vicarious Fourth Amendment claims would necessarily mean a more widespread invocation of the exclusionary rule during criminal trials." Id. at 137. The Court further reasoned that "[e]ach time the exclusionary rule is applied it exacts a substantial social cost for the vindication of Fourth Amendment rights," in that "[r]elevant and reliable evidence is kept from the trier of fact and the search for truth at trial is deflected." Id.

The Court also concluded that whether a defendant has the right to challenge a search and seizure is best analyzed under "substantive Fourth Amendment doctrine," and not standing, though the inquiry ought to be the same under either. Id. at 139.

Rakas and the case law on which it is based and which has followed it thus require this Court to ask whether a defendant who is challenging a search or seizure has established a sufficient personal privacy interest in the premises or property at issue. A defendant may make such a showing by asserting that he owned or leased the premises (for example, the leasing of a server would count) or had dominion or control over them. Watson, 404 F.3d at 166; United States v. Villegas, 899 F.2d 1324, 1333 (2d Cir. 1990). Indeed, to a limited extent, yet to be defined by the courts, an authorized user of a premises might have a sufficient expectation of privacy. See Rakas, 439 U.S. at 142-43 ("[A] person can have a legally sufficient interest in a place other than his own home so that the Fourth Amendment protects him from unreasonable governmental intrusion into that

place."). Factual claims made in an affirmation by defendant's counsel may be an insufficient basis upon which to challenge a search if they are made without personal knowledge or are otherwise insufficiently probative. See Watson, 404 F.3d at 166-67.

There are limited situations—"extreme case[s]," United States v. Rahman, 189 F.3d 88, 131 (2d Cir. 1999) (per curiam)—in which a government practice might be "so outrageous that due process principles would absolutely bar the [G]overnment from invoking judicial processes to obtain a conviction . . . ." United States v. Russell, 411 U.S. 423, 431-32 (1973); see also United States v. Christie, 624 F.3d 558 (3d Cir. 2010) ("The pertinent question is whether the government's conduct was so outrageous or shocking that it amounted to a due process violation."); Czernicki v. United States, 270 F. Supp. 2d 391, 394-95 (S.D.N.Y. 2003). However, only conduct that "shocks the conscience" amounts to a due process violation in this context. Rahman, 189 F.3d at 131 (quoting Rochin v. California, 342 U.S. 165, 172 (1952)).

Defendant cites U.S. v. Gelbard, 408 U.S. 41 (1972), and United States v. Ghailani, 743 F. Supp. 2d 261 (S.D.N.Y. 2010), for the proposition that "a defendant is entitled to know whether a Government's investigation was predicated on illegal government conduct, and [obtain] relief therefrom." (Def.'s Reply Br. at 7.) That is only so to the extent that the issues concern a defendant's personal Fourth Amendment rights, or if "extreme conduct" is involved. Unlawful conduct alone is not enough. See, e.g., United States v. Payner, 447 U.S. 727, 729-31 (1980). In

Ghailani, the issue concerned whether the court would allow testimony from a cooperating witness who had been tortured. 743 F. Supp. 2d at 267. The court ruled that it would not, id. at 287-88, but importantly, Ghailani was "not a Fourth Amendment search and seizure case," id. at 285.

A defendant seeking both to establish an interest in items seized, and to put the Government to its proof of establishing a connection, is protected to the extent that any declaration or affidavit he submits may not be offered against him at trial. Simmons v. United States, 390 U.S. 377, 393-94 (1968) ("[W]hen a defendant testifies in support of a motion to suppress evidence on Fourth Amendment grounds, his testimony may not thereafter be admitted against him at trial on the issue of guilt unless he makes no objection."). This does not insulate the defendant from all risk, however. His statement may nonetheless be used to impeach him should he take the witness stand in his own defense and, at that time, open the door to the statement. United States v. Jaswal, 47 F.3d 539, 543 (2d Cir. 1995); United States v. Beltran-Gutierrez, 19 F.3d 1287, 1291 (9th Cir. 1994). (Of course, perjury in a declaration or on the stand is never permitted; so there are reasons to expect consistency.) It is certainly true, therefore, that the requirement of a statement of a personal privacy interest in an item seized requires a defendant to make choices.[6]

[6] The order of proof at trial is known in advance: the Government bears the burden of proof, which means the Government goes first. If, after the Government rests, it has failed to present sufficient evidence, the defendant can move pursuant to Rule 29 of the Federal Rules of Criminal Procedure for a judgment of acquittal. Ulbricht would not take the witness stand (if at all) until those prior steps had occurred, and so the impeachment, if any, of Ulbricht with a statement setting forth a privacy interest in the Icelandic server would not occur until that point. (The Court recognizes that trial strategy is often cemented during open statements.)

Simply asserting a personal privacy interest in a premises or an object does not—even when a warrantless search has occurred—require a finding of a Fourth Amendment violation. A court asks a second question: whether society is willing to recognize that this expectation is, in turn, reasonable. California v. Ciraolo, 476 U.S. 207, 211 (1986); Katz, 389 U.S. at 360. For instance, that an individual has taken measures to restrict third-party viewing of his activities in a space that he owns or leases does not necessarily mean that that privacy interest is one society is prepared to recognize as reasonable. See Ciraolo, 476 U.S. at 209-10, 215 (finding no Fourth Amendment violation when aerial photographs had been taken above a property whose owner had taken fairly extensive measures to shield from view); see also Oliver v. United States, 466 U.S. 170, 182-84 (1984) (placement of "No Trespassing" signs on secluded property does not create legitimate privacy interest in marijuana fields).

Assuming a cognizable privacy interest, the court can then turn to whether the search was lawful.[7]

3. Warrants.

Searches not incident to arrest or exigent circumstances are generally based on a warrant. Kentucky v. King, 131 S. Ct. 1849, 1856 (2011). The Warrant Clause of the Fourth Amendment provides that "no Warrants shall issue, but upon

[7] In the absence of a cognizable privacy interest, the Court has no basis to proceed with a suppression motion, and therefore no basis on which to hold an evidentiary hearing. Evidentiary hearings are only necessary when a defendant makes a sufficient offer of proof with respect to his allegation that a false statement was made knowingly and intentionally, or with reckless disregard for the truth, by an affiant in a warrant affidavit, and if, when material that is the subject of the alleged falsity or reckless disregard is set to one side, there remains sufficient content in the warrant affidavit to support a finding of probable cause, no evidentiary hearing is required. Franks v. Delaware, 438 U.S. 154, 171 (1978).

probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. An application for a warrant must state under penalty of perjury facts supporting probable cause. See U.S. Const. amend. IV (warrant may not issue unless supported by probable cause, supported by "oath or affirmation"). A magistrate judge then reviews the warrant, determines whether the showing of probable cause and particularity is sufficient, and if so, signs it. See United States v. George, 975 F.2d 72, 76 (2d Cir. 1992) ("The particularity requirement prevents this sort of privacy invasion and reduces the breadth of the search to that which a detached and neutral magistrate has determined is supported by probable cause."). A magistrate judge's review is based on the totality of the circumstances. Illinois v. Gates, 462 U.S. 213, 238-39 (1983). In later reviewing such determination on a motion to suppress, the reviewing court is to give the magistrate judge's review a high degree of deference. See id. at 236 ("A magistrate's 'determination of probable cause should be paid great deference by reviewing courts.'" (quoting Spinelli v. United States, 393 U.S. 410, 419 (1969), abrogated on other grounds by Gates, 462 U.S. 213))).

In addition to its probable cause requirement, the Warrant Clause contains a prohibition against "general warrants." Andresen v. Maryland, 427 U.S. 463, 480 (1976). "'The problem (posed by a general warrant) is not that of intrusion Per se, but of a general, exploratory rummaging in a person's belongings . . . (the Fourth Amendment addresses the problem) by requiring a 'particular description' of the

things to be seized.'" Id. at 480 (quoting Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971)). General warrants are therefore prohibited; the particularity requirement is to ensure that nothing is left to the discretion of the officer when a warrant is being executed—if the item is described as among those to be seized, it may be seized. See Andresen, at 480; see also Stanford v. Texas, 379 U.S. 476, 485 (1965).

B. The Riley, Jones, and Kyllo Cases

Defendant refers to the decisions in Riley v. California, 134 S. Ct. 2473 (2014), United States v. Jones, 132 S. Ct. 945 (2012), and Kyllo v. United States, 533 U.S. 27 (2001), as supportive of his motions to suppress and as responding to the "essential privacy imperatives of the digital age." (Def.'s Reply Br. at 1, 13, 19, 21-28; see also Def.'s Br. at 3, 13-15, 17-19, 22-28, 42, 45-49, 59.) These cases do not help defendant on this motion. They are consistent, not inconsistent, with the above longstanding Fourth Amendment principles.

Riley concerned the search of data on a seized cell phone. The lawfulness of the seizure of the object itself —the cell phone—was not contested. The subsequent search of the data on the cell phone was. In Riley, the defendant was stopped for a traffic violation which resulted in his arrest on weapons charges. 134 S. Ct. at 2480. A cell phone was seized as a result of a lawful search of Riley's person incident to his arrest. Id. The arresting officer reviewed the contents of the cell phone without a warrant, and another officer conducted a subsequent and further review of those contents. Id. at 2480-81. The Supreme Court articulated the issue before it as how the requirement of "the reasonableness of a warrantless search

incident to a lawful arrest" applies to "modern cell phones." Id. at 2482, 2484. The Court acknowledged that the rationale of prior cases dealing with searches incident to arrest involving physical objects (such as those typically found on an arrestee's person) did not have as much force in the digital context. A "search of the information on a cell phone bears little resemblance to the type of brief, physical search considered in [United States v. Robinson, 414 U.S. 218 (1973)]." Id. at 2485. Because the data on a cell phone are generally far more extensive than the contents of physical objects and do not present the same type of safety issues, the Court determined that warrants are generally required to search the contents of cell phones. Id. at 2485-86. The Court based its decision both on the potential breadth of the information a cell phone might contain, as well as on the fact that digital data generally cannot be used as a weapon or to cause immediate physical danger. Id. Nothing in the Court's opinion in Riley suggests any departure from any of the principles regarding the need to establish a personal privacy interest, as discussed above, and as is obvious, the opinion says nothing concerning searches by foreign law enforcement officers outside the United States.

Jones concerned the warrantless attachment of a Global-Positioning-System ("GPS") tracking device to a Jeep vehicle and the subsequent monitoring of the movements of that vehicle. 132 S. Ct. at 948. The Supreme Court examined the question of whether the physical placement of the GPS device constituted a search within the meaning of the Fourth Amendment and found that it did. There, the Supreme Court returned to age-old concepts of physical trespass and the Fourth

Amendment. See id. at 949-54. In this context, the physical attachment of the device was found to unreasonably intrude on the defendant's reasonable expectation of privacy and, "[b]y attaching to the device to the Jeep, officers encroached on a protected area." Id. at 952. The Court acknowledged that more nuanced cases—such as situations involving the transmission of electronic signals without trespass—were different from the case then at hand and would be subject to analysis under the factors set forth in Katz. Id. at 953. Jones neither alters nor extends Fourth Amendment law in light of the digital era. Indeed, the majority opinion looks more to the past than it does to the future.

In Kyllo, the Supreme Court did find that relatively new technology—thermal imaging used on the exterior of a private residence, and which provided information as to what was occurring in that private residence—constituted a search for purposes of the Fourth Amendment. Kyllo, 533 U.S. at 40. The thermal imaging was performed from the exterior of the house and occurred over a span of just a few minutes. Id. at 29-30. Based upon the information obtained, the investigating agent drew the conclusion that the residence functioned in part as a grow-house for marijuana. Id. at 30. There, too, the Court applied longstanding principles of law to find that the defendant had a reasonable expectation of privacy in his residence—the sanctity of which has long been the concern of Fourth Amendment jurisprudence. Id. at 34-40. The Court held that "[w]here, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the

surveillance is a 'search' and is presumptively unreasonable without a warrant." Id. at 40.

C. Discussion

Here, the Government obtained nine warrants and five pen-trap orders. Ulbricht argues that all of the warrants and orders suffer from one overarching infirmity: they are based on the cursory recitation of an "investigation" that was only possible as the result of the search that led to the authorities to Iceland. Ulbricht argues that how that search was conducted is unknown, and that if it was conducted in an unlawful manner, then all of the warrants are constitutionally defective.[8]

Ulbricht's motion is largely, therefore, directed at an investigation and search of objects (servers) and premises in which he has carefully avoided establishing a personal privacy interest. As the above principles make clear, just because the investigation eventually led to his arrest on criminal charges does not ipso facto give him a privacy interest in any Silk Road servers. Katz, 389 U.S. at 351 ("[T]he Fourth Amendment protects people, not places.").

As the Court has set forth above, Ulbricht was provided ample opportunity to establish such an interest—including an additional and specific request by this

[8] Ulbricht also argues that the magistrate judges who received the warrant applications failed appropriately to inquire into how the preliminary investigation was conducted. (Def.'s Br. at 36-37.) For all of the reasons discussed throughout this opinion, he has not established a personal privacy interest that would allow him to pursue this argument. Nevertheless, even if this Court were to perform a substantive review of the merits it would find that there is no deficiency. This Court is to give a receiving magistrate's determination of probable cause a high degree of deference. See Gates, 462 U.S. at 236. It is apparent from the face of the affidavit in support of Warrant No. 1—which contains a handwritten addition by the affiant and the initials of the reviewing magistrate—that the application was carefully reviewed and probable cause established.

Court on October 7, 2014. (ECF Nos. 76-77.) He elected to "rest[] on his papers." (ECF No. 83.) This is either because he in fact has no personal privacy interest in the Icelandic server, or because he has made a tactical decision not to reveal that he does.

The requirement to establish a personal privacy interest might appear to place Ulbricht in a catch-22: if the Government must prove any connection between himself and Silk Road, requiring him to concede such a connection to establish his standing the searches and seizures at issue could be perceived as unfair. But as Ulbricht surely knows, this is not the first court, nor is he the first defendant, to raise such an issue. See, e.g., Payner, 447 U.S. 727. In Payner, the Government obtained evidence against a defendant based on a "flagrantly illegal search of a [third party's] briefcase." Id. at 729. The Supreme Court referenced having decided Rakas the prior term, reaffirming the "established rule that a court may not exclude evidence under the Fourth Amendment unless it finds that an unlawful seizure violated the defendant's own constitutional rights." Id. at 731 (collecting cases). "And the defendant's Fourth Amendment rights are violated only when the challenged conduct invaded his legitimate expectation of privacy rather than that of a third party." Id. (emphasis in original) (citing, inter alia, Rakas, 439 U.S. at 143.)

While the district court and the circuit court in Payner recognized this rule, they directly stated that a federal court should use its supervisory power to suppress evidence tainted by gross illegalities that did not infringe the defendant's constitutional rights. Id. at 733. The Supreme Court disagreed—and found that

the extension of the supervisory power would "enable federal courts to exercise a standardless discretion in their application of the exclusionary rule to enforce the Fourth Amendment." Id. at 733. The Supreme Court reiterated that it did not condone lawless behavior—but nor did lawless behavior command "the exclusion of evidence in every case of illegality." Id. at 734. "Our cases have consistently recognized that unbending application of the exclusionary sanction to enforce ideals of government rectitude would impede unacceptably the truth-finding functions of the judge and jury." Id. The Court concluded that "the supervisory power does not authorize a federal court to suppress otherwise admissible evidence on the ground that it was seized unlawfully from a third party not before the court." Id. at 735.

Ulbricht and other defendants seeking to both establish an interest in items seized, and put the Government to its proof of establishing a connection, are protected to the extent that any declaration or affidavit may not be offered against the defendant at trial. See Simmons, 390 U.S. at 393-94 (a defendant's sworn statements offered in support of a motion to suppress may not thereafter be admitted against him at trial on the issue of guilt unless defendant does not object). This does not insulate the defendant from all risk, however. His statement may nonetheless be used to impeach the defendant should he take the witness stand in his own defense and, at that time, open the door to the statement on direct. United States v. Jaswal, 47 F.3d 539, 543 (2d Cir. 1995); United States v. Beltran-Gutierrez, 19 F.3d 1287, 1291 (9th Cir. 1994). It is certainly true, therefore, that the requirement of a statement of a personal privacy interest in an item seized

requires a defendant to make hard choices. One choice is to establish an interest if such exists to enable a court to take up important issues. That could not or was not done here.

Here, the Court does not know whether Ulbricht made a tactical choice because he is—as they say—between a rock and a hard place, or because he truly has no personal privacy interest in the servers at issue.

It is clear, however, that this Court may not proceed with a Fourth Amendment analysis in the absence of the requisite interest. If a third party leased a server on which the Government unlawfully intruded in the investigation that led to the Icelandic server, under Katz, Rakas, Payner, and a host of other case law, that is no basis for an assertion by Ulbricht that his Fourth Amendment rights were violated. Thus, whatever methods used—lawful or unlawful—are beyond this Court's purview. Payner, 447 U.S. at 735. Ulbricht therefore has no basis to challenge as violations of his Fourth Amendment rights: (1) the investigation that preceded and led to the Icelandic server, (2) the imaging and search of the Icelandic server, and (3) Warrant Nos. 1, 2, 3, 4, 5, and 7.[9]

Ulbricht has not proffered a statement that he had a personal expectation of privacy in the laptop (Warrant No. 6), Facebook (Warrant No. 8) or Gmail accounts (Warrant No. 9). While his lawyer stated that his privacy interest in the accounts and his laptop is "manifest" (ECF No. 83 at 2 n.2), the law has long held that

[9] Ulbricht has also argued that Warrant Nos. 1, 2, 3, 4, 5, and 7 are unlawful "general warrants." (See Def.'s Reply Br. at 3.) For the same reasons that he lacks a sufficient Fourth Amendment interest to challenge the investigatory technique that underlies the probable cause recited in the warrants, so too he lacks a sufficient interest as to this argument.

statements submitted by attorneys that are merely conclusory or that do not allege personal knowledge on the part of the attorney are insufficient to create an issue of fact. See United States v. Motley, 130 Fed. App'x 508, 510 (2d Cir. 2005) (summary order) (citing Lipton v. Nature Co., 71 F.3d 464, 469 (2d Cir. 1995); United States v. Gillette, 383 F.2d 843, 848-49 (2d Cir. 1967). While the Court may assume based on his attorney's statement and the Government's stated intention not to contest that position that these accounts and the laptop belong to Ulbricht, that does not necessarily mean that he has a reasonable expectation of privacy as to their respective contents. There are, of course, many ways in which users may set up the privacy settings or password protection for their Facebook and Gmail accounts, as well as access to their laptops—and these settings and protections are relevant to a Katz analysis. See United States v. Meregildo, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012) ("When a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment. However, postings using more secure privacy settings reflect the user's intent to preserve information as private and may be constitutionally protected." (citations omitted)). It is also possible for more than one individual to have access to a single shared Facebook or Gmail account. It also seems likely that many of Ulbricht's emails were to individuals other than himself, which could defeat an expectation of privacy in them. See United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) (explaining that emailers generally lose a legitimate expectation of privacy in an email that has already reached its recipient (citing Guest v. Leis, 255 F.3d 325, 333 (6th Cir.

2001))).[10] The Court has no idea whether Ulbricht had a reasonable subjective expectation that all aspects of his Facebook and Gmail accounts would be private, or none. The Court has no idea whether his laptop was password protected or not. And that makes a difference. The Court cannot just assume a subjective expectation of privacy.[11]

In any event, the warrants relating to these three items were lawful. As the Court has set forth above, Ulbricht cannot challenge the initial investigation that led to the Icelandic server. Information obtained from the search of that server led law enforcement to other servers within the United States (as to which Ulbricht similarly has no demonstrated privacy interest), and the information gathered as a result of those searches undoubtedly found its way into the probable cause analysis for Warrant Nos. 6, 8 and 9. That probable cause supported Warrants 6, 8 and 9 was well and solidly established—even without the deference this Court must give to the reviewing magistrate judge. See Gates, 462 U.S. at 236; United States v. Martin, 426 F.3d 68, 73 (2d Cir. 2005) (courts must afford a presumption of validity to the affidavits supporting a search warrant); United States v. Carpenter, 341 F.3d

---

[10] The Court does not here decide that Ulbricht could never have an expectation of privacy in an email he sent to a third party.

[11] It is particularly inappropriate to do so in light of published user terms for both Gmail accounts and Facebook which indicate that under certain circumstances the accounts may be turned over, without notice, to law enforcement. See Privacy Policy, Google, http://www.google.com/policies/privacy/ (last modified Mar. 31, 2014) ("Your domain administrator may be able to . . . receive your account information in order to satisfy applicable law, regulation, legal process or enforceable government request. . . . We will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that . . . the information is reasonably necessary to: meet any applicable law, regulation, legal process, or enforceable governmental request."); Information for Law Enforcement Authorities, Facebook, https://www.facebook.com/safety/groups/law/guidelines/ (last visited October 9, 2014) (explaining that under certain circumstances Facebook may provide a user's information to law enforcement authorities without notice to the user).

666, 670 (8th Cir. 2003) ("[S]uppression remains an appropriate remedy where 'the issuing magistrate wholly abandoned his judicial role.'" (quoting United States v. Leon, 468 U.S. 897, 923 (1984))). Thus, the warrants do not suffer from any probable cause deficiency.

Nor are these general warrants. A general warrant is one that lacks particularity as to the item to be seized or as to what should be searched. George, 975 F.2d at 75. Here, they were specific as to both. The warrants identified the laptop and the accounts by name. There was no lack of specificity as to the items to be seized. Thus, the entirety of the laptop and data on the hard drive of that laptop was seized, along with the entirety of the accounts.

The warrants were also specific, however, as to what type of evidence should be searched for. Each of the warrants listed specific categories of items, including evidence of aliases, evidence concerning attempts to obtain fake identification, writings which can be used as stylistic comparisons for other "anonymous" writings, evidence concerning Ulbricht's travel patterns or movement, communications with co-conspirators regarding specified offenses, evidence concerning Bitcoin in connection with the specified offenses, and other evidence relating to the specified offenses. (See Dratel Decl. exs. 11, 13, 14.)

It is certainly true that in order to search for the specified items, the Warrants sought to seize the entirety of the laptop, the Facebook account, and the Gmail account. But this does not transform the warrants into general warrants. Indeed, it is important not to confuse the separate concepts of the seizure of an

item—which were quite specifically identified but which were seized in their entirety—with the search itself. The search is plainly related to the specific evidence sought. It has long been perfectly appropriate to search the entirety of a premises or object as to which a warrant has issued based on probable cause, for specific evidence as enumerated in the warrant, which is then to be seized. For instance, warrants have long allowed searching a house high and low for narcotics—indeed, it is rare that drug dealers point out the hidden trap in the basemen—or reviewing an entire file cabinet to find files that serve as evidence of money laundering activity, which might be intermingled with files documenting lawful and irrelevant activity. This case simply involves the digital equivalent of seizing the entirety of a car to search for weapons located within it, where the probable cause for the search is based on a possible weapons offense.

In In the Matter of a Warrant for All Content and Other Information Associated with the Email Account at xxxxx@Gmail.com Maintained at the Premises Controlled by Google, Inc., No. 14 Mag. 309, 2014 WL 3583529 (S.D.N.Y. Aug. 7, 2014) ("Gmail"), Magistrate Judge Gorenstein comprehensively reviewed the current state of the law in this area. In that case, the Government sought a warrant in connection with an investigation to allow it to search the entirety of a Gmail account for specified evidence of a crime, as to which sufficient probable cause had been demonstrated. Id. at *1. The warrant did not contain a particular search protocol and did not limit the amount of time the Government could take to review the information Google would provide in response to the warrant. Id. The

warrant also did not provide for later destruction of the material. Id. The court reviewed Fourth Amendment principles with a particular focus on the requirement that courts assess the "reasonableness" of a search. Id. at *2. The court noted that courts in Washington, D.C. and Kansas had denied applications seeking warrants for entire email accounts, at least without protocols in place. Id. at *3. The court found that under long established precedent, when officers executing warrants went, for instance, to a home or office, and were authorized to seize particular types of documents, they generally were required to look into the places where any and all documents were stored; there was no practice and certainly no requirement that people universally applied to the organization of their documents to assist in quick and direct location of responsive documents should they ever be the subject of a warrant. That was not real life. Some latitude for searches had to be allowed; this was particularly true with regard to electronic evidence would could be even more voluminous and undifferentiated than paper documents. See id. at *5.

Judge Gorenstein applied these principles to the warrant before him and determined that because it specified the particular crimes as to which evidence was sought—and as to which probable cause had been established—it was not overbroad. Id. at *7. He noted that the Federal Rules of Criminal Procedure had been amended in 2009 to provide for a procedure in which a warrant could authorize the seizure of electronic storage media or the seizure or copying of electronically stored information—and that unless the warrant otherwise requires it, a later review of the media or information is allowed. Id. at *6 (citing Fed. R.

Crim. P. 41(e)(2)(B)). The decision also noted the Second Circuit's ruling in United States v. Ganias, 755 F.3d 125 (2d Cir. 2014), in which the Second Circuit held that while wholesale removal of all tangible papers from a premises was not generally acceptable, electronic media posed a different set of issues. Gmail, 2014 WL 3583529, at *6. In Ganias, the Court stated that "[i]n light of the significant burdens on-site review would place on both the individual and the Government, the creation of mirror images for offsite review is constitutionally permissible . . . ." 755 F.3d at 135.

This Court agrees entirely with Judge Gorenstein's rationale. Warrants 6, 8 and 9 are substantially similar to the warrant before Judge Gorenstein, and similarly have the necessary particularity.[12]

III. PEN-TRAP ORDERS

Defendant argues that the Pen-Trap Orders were deficient for two reasons: (1) the information obtained through the Pen-Trap Orders should have been the

---

[12] Even if this Court were to find that the magistrate judges who issued the warrants erred by approving the clauses to which Ulbricht objects as overly broad, the application of the exclusionary rule here would still be inappropriate, as the law enforcement agents who executed the searches and seizures at issue were entitled to rely in good faith upon the magistrate judges' probable cause determinations, and the warrant applications here were not so "lacking in indicia of probable cause" nor so "facially deficient" that reliance upon the warrant was "entirely unreasonable." Id. at 921-23 (quotation omitted).

The Court further notes that while it is certainly true that there circumstances under which a warrant that authorizes a seizure of "any communications or writings" in the email account of a defendant would be overbroad, it is also true that a magistrate judge's review of a warrant application must be based on the totality of the circumstances. Gates, 462 U.S. at 238-39. Here, these circumstances included many steps taken by members of the alleged conspiracy to maintain their anonymity while creating, designing, administering, operating, and using the Silk Road website, and they included the use of idiosyncratic linguistic patterns by the website's administrator. Given the high degree of deference that this Court must afford the review of the magistrate judge, see id. at 236, it is not this Court's place to second-guess their decision that the warrants were not overly broad in the context of a case where anonymity and the usage of idiosyncratic linguistic patterns are key issues.

subject of a warrant application, and (2) the orders failed to include appropriate minimization procedures. Both arguments are meritless.

The law is clear—and there is truly no room for debate—that the type of information sought in Pen-Trap orders 1, 2, 3, 4, and 5 was entirely appropriate for that type of order.[13] See 18 U.S.C. §§ 3121 et seq. In Smith v. Maryland, 442 U.S. 735 (1979), the Supreme Court found that the use of a pen-register did not constitute a search for Fourth Amendment purposes, id. at 745-46. To the extent Ulbricht wants to make novel Fourth Amendment arguments with regard to the Pen-Trap Orders,[14] he has not established the requisite privacy interest (as discussed at length above) to do so. The Court will therefore not consider those arguments.

Ulbricht's minimization argument is similarly off-base. Minimization refers to protocols and is used in the wiretap context to prevent investigators from listening to conversations irrelevant to their investigation. See 28 U.S.C. § 2518 (wiretaps must be conducted "in such a way as to minimize the interception of communications not otherwise subject to interception"). Minimization is directed at content. See United States v. Rizzo, 491 F.2d 215, 216 n.3 (2d Cir. 1974) (federal

---

[13] The information related to the IP addresses of individual packets of data sent to and from a particular IP address. The content of the communications was not requested. Pen-trap devices have frequently been used to obtain precisely that which was sought here. Before the Internet became widely used, pen-trap devices were used to obtain information regarding the telephone numbers associated with incoming and outgoing telephone calls. Smith v. Maryland, 442 U.S. 735 (1979).

[14] Defendant argues that 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" that what the telephone numbers associated with a telephone call would reveal. (Def.'s Reply Br. at 25.) He urges that as a result, Smith v. Maryland—which occurred in the context of landline telephones—is inapposite. This Court cannot consider that argument in light of the lack of a demonstrated privacy interest.

minimization laws do not apply "to mere interception of what telephone numbers are called, as opposed to the interception of the contents of the conversations"). The Pen-Trap Orders do not seek the content of internet communications in any directly relevant sense.

IV. BILL OF PARTICULARS

Defendant moves for an order requiring the Government to provide a bill of particulars. (Def.'s Br. at 65-79.) Defendant argues that in the absence of additional factual detail not contained in the Indictment, he will be unable to prepare his defense and will have an insufficient basis to make double jeopardy challenges to potential future charges. (Id. at 65.) Defendant argues that the volume of discovery weighs in favor of a bill of particulars. (Id. at 65-66.)

Rule 7(f) of the Federal Rules of Criminal Procedure provides that a court may direct the Government to file a bill of particulars. Fed. R. Crim. P. 7(f). However, a bill of particulars is required "only where the charges of the indictment are so general that they do not advise the defendant of the specific acts of which he is accused." United States v. Walsh, 194 F.3d 37, 47 (2d Cir. 1999) (quoting United States v. Torres, 901 F.2d 205, 234 (2d Cir. 1990)).

A bill of particulars is also unnecessary when the Government has produced materials in discovery concerning the witnesses and other evidence. See id. ("[A] bill of particulars is not necessary where the government has made sufficient disclosures concerning its evidence and witnesses by other means.") In Torres, the Second Circuit affirmed the district court's denial of a bill of particulars in part because the defendants were provided with considerable evidentiary detail outside

of the indictment. 901 F.2d at 233-34; see also United States v. Panza, 750 F.2d 1141, 1148 (2d Cir. 1984). Thus, in determining whether to order a bill of particulars, a court must examine the totality of the information available to defendant, both through the indictment and through pre-trial discovery. United States v. Bin Laden, 92 F. Supp. 2d 225, 233 (S.D.N.Y. 2000). The purpose of the bill of particulars is to avoid prejudicial surprise at trial and give defendant sufficient information to meet the charges against him. Id. (citing Torres, 901 F.2d at 234).

In Bin Laden, the court granted the defendants' motion for a bill of particulars. Id. at 227. There, however, the indictment charged 15 named defendants with 267 discrete criminal offenses, it charged certain defendants with 229 counts of murder, it covered a period of nearly ten years, and it alleged 144 overt acts in various countries. Id. at 227-28. The court noted that the "geographical scope of the conspiracies charged in the indictment is unusually vast." Id.

There is no provision in the Federal Rules of Criminal Procedure for the type of broad, sweeping discovery Ulbricht seeks here. Neither the nature of this indictment or the produced discovery calls for a departure from these general rules. That this case has a high profile does not mean that it requires special treatment. Moreover, there can be no doubt that the Indictment here is specific enough to advise Ulbricht of the acts of which he is accused, namely creating, designing, administering and operating the Silk Road website, which allegedly served as an

online one-stop-shop for narcotics, fake identification documents, and materials used to hack computers, and which was specifically designed to rely on Bitcoin, a method of payment designed to conceal the identities and locations of users transmitting and receiving funds. This case is unlike Bin Laden, which concerned hundreds of offenses associated with over one hundred alleged actions committed in far corners of the globe—it concerns a single defendant who is alleged to have run a single and clearly identified website. Further, the Court has gone to considerable lengths to ensure that Ulbricht has access to evidentiary detail outside of the Indictment, including ensuring that a laptop preloaded with certain discovery materials was provided to Ulbricht for use at the Metropolitan Detention Center ("MDC") and particular accommodations regarding the length of time he can routinely access the information. (ECF No. 40.) A bill of particulars is wholly unnecessary to avoid prejudicially surprising Ulbricht at trial.

V. SURPLUSAGE

Rule 7(d) of the Federal Rules of Criminal Procedure provides that, upon a motion by defendant, a court may strike extraneous matter or surplusage from an indictment. Fed. R. Crim. P. 7(d). However, "'[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 or prejudicial.'" United States v. Mulder, 273 F.3d 91, 99 (2d Cir. 2001) (quoting United States v. Scarpa, 913 F.2d 993, 1013 (2d Cir. 1990)).

Courts have held that statements providing background are relevant and need not be struck. Id. at 99-100 (in action charging extortion relating to labor

coalitions, upholding district court's decision not to strike background on tactics and purposes of labor coalitions).

The surplasage issues defendant has raised relating largely to the murder for hire assertions need not be fully addressed at this time. Courts in this district routinely await the presentation of the Government's evidence at trial before ruling on a motion to strike surplusage. See, e.g., Scarpa, 913 F.2d at 1012; United States v. Persico, 621 F. Supp. 842, 861 (S.D.N.Y. 1985); United States v. Ahmed, No. 10 CR. 131(PKC), 2011 WL 5041456, at *3 (S.D.N.Y. Oct. 21, 2011).

In Ahmed, the defendant's motion to strike surplusage related to background information regarding civil and sectarian violence in Somalia and the anti-American animus of Al Shabaab, which was designated by the Secretary of State as a "foreign terrorist organization." Ahmed, 2011 WL 5041456, at *1-2. The court held that it would await presentation of the Government's evidence at trial, and stated further that the Government would have some latitude to "demonstrat[e] the nexus between defendant's conduct and American interests, as well as the background of others who are members of the charged conspiracies." Id. at *3. The Court noted that denial of the motion without prejudice to renew might also allow the parties to reach a pre-trial stipulation, as had occurred in United States v. Yousef, No. S3 08 Cr. 1213(JFK), 2011 WL 2899244 (S.D.N.Y. June 30, 2011). Ahmed, 2011 WL 5041456, at *3. Here, as in Ahmed, the Court will await the Government's presentation at trial.

VI. CONCLUSION

For the reasons set forth above, defendant's motion to suppress, for a bill of particulars and to strike surplusage is DENIED.

The Clerk of Court is directed to close the motion at ECF No. 46.

SO ORDERED.

Dated: New York, New York
October 10, 2014

KATHERINE B. FORREST
United States District Judge