UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

| | | |
|---|---|---|
| UNITED STATES OF AMERICA | : | |
| - v. - | : | S1 14 Cr. 68 (KBF) |
| ROSS ULBRICHT,<br>a/k/a "Dread Pirate Roberts,"<br>a/k/a "DPR,"<br>a/k/a "Silk Road," | : | |
| Defendant. | : | |

**MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS EVIDENCE, OBTAIN DISCOVERY AND A BILL OF PARTICULARS, AND STRIKE SURPLUSAGE**

PREET BHARARA
United States Attorney
Southern District of New York
One St. Andrew's Plaza
New York, New York 10007

SERRIN TURNER
TIMOTHY T. HOWARD
Assistant United States Attorneys
*Of Counsel*

**TABLE OF CONTENTS**

# TABLE OF AUTHORITIES

**Federal Cases**

**Federal Statutes**

**Federal Rules**

## PRELIMINARY STATEMENT

Having failed in his prior motion to dismiss all of the Government's charges, Ulbricht now moves this Court to suppress virtually all of the Government's evidence, on the ground that it was supposedly obtained in violation of the Fourth Amendment. Ulbricht offers no evidence of any governmental misconduct to support this sweeping claim. Instead, Ulbricht conjures up a bogeyman – the National Security Agency ("NSA") – which Ulbricht suspects, without any proof whatsoever, was responsible for locating the Silk Road server, in a manner that he simply assumes somehow violated the Fourth Amendment. "If," Ulbricht contends, all of the Government's evidence was the "fruit of this poisonous tree," it must all be suppressed.

The law, however, turns on facts, not speculation. And the facts are not at all what Ulbricht imagines them to be. As explained below, the Silk Road server was located not by the NSA but by the Federal Bureau of Investigation ("FBI"), using perfectly lawful means: FBI agents noticed the server's Internet protocol ("IP") address leaking in traffic sent from the Silk Road website when FBI agents interacted with it. After taking additional steps to corroborate that the server was indeed hosting Silk Road, the FBI asked law enforcement authorities in the foreign country where the server was located to image the server's contents, which those authorities agreed to do, pursuant to their own laws and investigative authority. The FBI's actions were utterly proper and did not violate the Fourth Amendment in any way.

Beyond making speculative claims of fact, Ulbricht offers only specious theories of law in advancing the rest of his suppression arguments. First, Ulbricht contends that the Government was required to get a warrant to authorize the search of the Silk Road server; but it is well established that warrants are not required for searches by foreign authorities of property overseas. Second, Ulbricht complains that the Government should have disclosed how it located

the Silk Road server in applying for search warrants later in the investigation; but the law requires a warrant application to include only those facts necessary to establish probable cause, and it was not necessary to explain how the Government located the Silk Road server in order to do so. Third, Ulbricht challenges the Government's use of pen registers during the investigation without a warrant; but pen registers merely collect routing data, and both statute and case law make clear that they do not require a warrant. Fourth, Ulbricht challenges certain language in search warrants the Government obtained for his laptop and email and Facebook accounts; but the language was specifically approved by two magistrate judges based on a corresponding showing of probable cause in the accompanying agent affidavits. In short, notwithstanding the lengthy exposition of Fourth Amendment jurisprudence in Ulbricht's brief – most of which has nothing to do with this case – his various claims are bereft of any support in the law.

Ulbricht's requests in his motion for relief other than suppression of evidence – for discovery, a bill of particulars, and the striking of "surplusage" from the Indictment – are likewise meritless. Ulbricht's discovery requests are not based on any showing that they will yield material evidence; instead, they amount to a pointless fishing expedition aimed at vindicating his misguided conjecture about the NSA being the shadowy hand behind the Government's investigation. Ulbricht's request for a bill of particulars is also unjustified, given the extensive disclosures the Government has made to Ulbricht about the case already, through its detailed Complaint and voluminous, well-organized discovery production. Finally, the language that Ulbricht seeks to strike from the Indictment is not "surplusage" but instead is language relevant to the crimes charged; most significantly, the language concerning the murders-for-hire that Ulbricht is alleged to have solicited is relevant to Ulbricht's criminal intent in his operation of Silk Road.

In short, not a single one of the numerous arguments in Ulbricht's scattershot motion hits its mark. The motion should be denied in its entirety.

## FACTUAL BACKGROUND

### A. Searches of Silk Road Servers

Contrary to Ulbricht's conjecture that the server hosting the Silk Road website (the "SR Server") was located by the NSA, the server was in fact located by the FBI New York Field Office in or about June 2013. (Decl. of Christopher Tarbell ("Tarbell Decl.") ¶ 5). The Internet protocol ("IP") address of the SR Server (the "Subject IP Address") was "leaking" from the site due to an apparent misconfiguration of the user login interface by the site administrator – *i.e.*, Ulbricht. (*Id.* ¶ 4-8). FBI agents noticed the leak upon reviewing the data sent back by the Silk Road website when they logged on or attempted to log on as users of the site. (*Id.* ¶¶ 7-8). A close examination of the headers in this data revealed a certain IP address not associated with the Tor network (the "Subject IP Address") as the source of some of the data. (*Id.* ¶ 8). FBI personnel entered the Subject IP Address directly into an ordinary (non-Tor) web browser, and it brought up a screen associated with the Silk Road login interface, confirming that the IP address belonged to the SR Server. (*Id.*).

Based on publicly available information, the Subject IP Address was associated with a server housed at a data center operated by a foreign server-hosting company in Iceland. (*Id.* ¶ 9). Accordingly, on June 12, 2013, the United States issued a request[1] to Iceland for Icelandic authorities to take certain investigative measures with respect to the server, including collecting

[1] Although the Complaint and search warrants in this case refer to the request as a "Mutual Legal Assistance Treaty request," this description is not technically correct, as the United States does not have an MLAT with Iceland. The request was instead an official request to Iceland issued pursuant to the 2001 Council of Europe Convention on Cybercrime and other relevant law of Iceland, and as a matter of comity.

routing information for communications sent to and from the server, and covertly imaging the contents of the server. (*Id.* ¶ 9 & Ex. A).[2] The Reykjavik Metropolitan Police ("RMP") provided routing information for the server soon thereafter, which showed a high volume of Tor traffic flowing to the server – further confirming that it was hosting a large website on Tor. (*Id.* ¶¶ 10-11). Subsequently, after obtaining the legal process required under Icelandic law to search the server, and after consulting with U.S. authorities concerning the timing of the search, the RMP covertly imaged the server and shared the results with the FBI on or about July 29, 2013. (*Id.* ¶ 12). Forensic examination of the image by the FBI immediately and fully confirmed that the server was in fact hosting the Silk Road website, *i.e.*, that it was in fact the SR Server. (*Id.* ¶ 13). The server contained what were clearly the contents of the Silk Road website – including databases of vendor postings, transaction records, private messages between users, and other data reflecting user activity – as well as the computer code used to operate the website. (*Id.*).

From examining the computer code on the SR Server, the FBI learned of IP addresses of additional servers used in connection with administering the Silk Road website. (*Id.* ¶ 15). In particular, the FBI found the IP address of a server used to back up the contents of the SR Server, housed at a data center in Pennsylvania. (*Id.* ¶ 16). The FBI obtained a warrant to search this backup server on September 9, 2013, and again on October 1, 2013 – the day before the seizure of the Silk Road website – to ensure collection of any data added or modified since the initial search. (*Id.* ¶¶ 16-17 & Exs. E-G). The October 1 search warrant also authorized the search of a secondary backup server at the same Pennsylvania data center.[3] (*Id.* ¶ 17 & Ex. G).

[2] The exhibits to the Tarbell Declaration are being filed under seal with the Court.

[3] The FBI's analysis of the SR Server yielded IP addresses of other servers associated with the Silk Road site as well, some of which were hosted by U.S.-based providers and some of which were hosted by foreign providers. (*Id.* ¶ 15). The Government obtained the contents of the

**B. Pen Registers and Search Warrants Relating to Ulbricht**

By mid-September 2013, Ulbricht was the Government's lead suspect as the owner and operator of Silk Road, known on the site as "Dread Pirate Roberts," or "DPR." (*Id.* ¶ 18). Accordingly, around that time, the Government obtained several judicially authorized pen registers for the purpose of confirming the identity of Ulbricht as "DPR." (*Id.* ¶ 19 & Exs. H-K). These pen registers authorized the FBI to collect routing data from the Internet service provider ("ISP") account associated with Ulbricht's residence (the "ISP Account"), the wireless router associated with that account (the "Router"), and certain hardware devices that were determined to be regularly connecting to the router (the "Devices"). (*Id.* ¶ 19). The data collected through these pen registers (the "Pen Registers") did not include the contents of any communications. (*Id.*). Instead, the data consisted of the IP addresses in contact with the ISP Account, Router, and Devices, along with the dates, times, durations, and other routing information associated with these connections – similar to the connection data associated with incoming and outgoing phone calls that the Government can obtain with a pen register on a phone line. (*Id.*).

Contrary to Ulbricht's claims, (Br. 39), the Government did not use the Pen Registers to track his physical location. Instead, the Government used the Pen Registers to ascertain when he was connected to the Internet and what IP addresses he was connecting to – just as a pen register on a telephone is used to monitor when a person is using a phone line and what phone numbers they are calling during the communications. (*Id.* ¶ 20). By monitoring when Ulbricht appeared to be logged in to Silk Road (as reflected by his activity on the Silk Road discussion forum), the

---

former through search warrants and obtained the contents of the latter through requests for law enforcement assistance directed to the corresponding foreign countries. (*Id.* ¶ 15). Ulbricht does not make any specific challenge to the searches of these additional servers in his motion.

FBI was able to collect additional evidence corroborating that Ulbricht and "DPR" were one and the same. (*Id.*).

On October 1, 2013, in the morning before Ulbricht's arrest later that day, the FBI obtained two search warrants from the United States District Court for the Northern District of California – one authorizing a search of Ulbricht's residence, and the other authorizing a search of his computer. (*Id.* ¶ 22 & Exs. L & M). The warrants were issued by a magistrate judge based upon sworn agent affidavits, which the magistrate judge found to establish probable cause to believe that Ulbricht was the administrator of the Silk Road website and that evidence of his criminal activity was likely to be found in the premises and computer to be searched. (*Id.* Exs. L & M).

A week after Ulbricht's arrest, on October 8, 2013, the FBI obtained two warrants from the United States District Court for the Southern District of New York, pursuant to the Stored Communications Act, 18 U.S.C. § 2703, authorizing the FBI to obtain the contents of Ulbricht's email and Facebook account from Google and Facebook. (*Id.* ¶ 23 & Exs. N & O). The warrants were issued by a magistrate judge based upon sworn agent affidavits, which, again, the magistrate judge found to establish probable cause to believe that evidence of Ulbricht's criminal activity would be found in the accounts. (*Id.* Exs. N & O). In particular, the affidavits explained that Ulbricht had been identified as "DPR" based in substantial part on information gleaned about Ulbricht from his public online footprint, and that it was believed that his Facebook and Gmail accounts would reveal similar evidence that would further corroborate the identification. (*Id.* Ex. N at ¶¶ 6-8, Ex. O at ¶¶ 6-8).

# ARGUMENT

## POINT I:
## ALL OF ULBRICHT'S SUPPRESSION ARGUMENTS ARE MERITLESS AND SHOULD BE DENIED

### A. The FBI Lawfully Located the Silk Road Server

Ulbricht begins his argument by hypothesizing that "if" the Government located the SR Server "unlawfully," then "all subsequent searches and seizures" conducted in the Government's investigation were unlawful as well, to the extent that they derived from information recovered from the SR Server. (Br. 29). In light of the actual facts, set forth above, this hypothetical can be quickly dispatched. The FBI located the SR Server through means that were entirely lawful, by identifying its true IP address through publicly accessible information that Ulbricht apparently did not realize was visible to anyone who visited the Silk Road website.

Again, the SR Server was located as a result of a "leak" of its IP address in data sent back from the Silk Road website when agents logged in or attempted to log in to the site. (Tarbell Decl. ¶¶ 4-15). There was nothing unconstitutional or otherwise unlawful in the FBI's detection of that leak. The Silk Road website, including its user login interface, was fully accessible to the public, and the FBI was entitled to access it as well. *See United States v. Meregildo*, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012) (noting that web content accessible to the public is not protected by the Fourth Amendment and can be viewed by law enforcement agents without a warrant).

The FBI was equally entitled to review the headers of the communications the Silk Road website sent back when the FBI interacted with the user login interface, which is how the Subject IP Address was found. Particularly given that the FBI itself was a party to the communications, Ulbricht cannot claim that the FBI violated any legitimate privacy expectation of his by examining them. *See United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) (holding that

sender of electronic communication loses any legitimate expectation of privacy in the communication once it has reached its recipient); *see generally United States v. White*, 401 U.S. 745, 748-49 (1971) (holding that Fourth Amendment does not protect communications made to undercover government agent). Moreover, an IP address is not part of the contents of a communication and no legitimate expectation of privacy attaches to it in the first instance. *See United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010) (no expectation of privacy in IP address conveyed to third-party).

It 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. *See United States v. Borowy*, 595 F.3d 1045, 1048 (9th Cir. 2010) (finding that defendant had no legitimate privacy interest in child pornography files posted on peer-sharing website, notwithstanding that defendant had made "ineffectual effort" to use site feature that would have prevented his files from being shared); *United States v. Post*, __ F. Supp. 2d __, 2014 WL 345992, at *2-*3 (S.D. Tex. Jan. 30, 2014) (finding that defendant had no legitimate privacy interest in metadata used to identify him that was embedded in file he had posted on Tor website, notwithstanding that "he did not realize he was releasing that information and he intended to remain anonymous").

In short, the FBI's location of the SR Server was lawful, and nothing about the way it was accomplished taints any evidence subsequently recovered in the Government's investigation.

**B. A Warrant Was Not Required for the Search of the Silk Road Server**

Beyond speculating that the SR Server was located through illegitimate means, Ulbricht also seeks suppression of the SR Server's contents on the ground that the server was searched without a warrant. (Br. 29). As explained below, the argument is meritless. The SR Server was searched by

Icelandic authorities, to whom the Fourth Amendment and its exclusionary rule do not apply in the first instance. While Icelandic authorities conducted the search at the request of U.S. law enforcement authorities, that is not enough to render the search subject to Fourth Amendment requirements. And even if it were, a warrant still would not have been required for the search, since the Fourth Amendment's warrant requirement does not apply extraterritorially. Instead, an extraterritorial search by U.S. law enforcement need only be reasonable, which the search of the SR Server clearly was, given that there was probable cause to believe it was hosting an enormous black market for illegal drugs and other illicit goods and services.

*1. The Silk Road Server Was Searched by Foreign Law Enforcement Authorities to Whom the Fourth Amendment Does Not Apply*

It has long been the law that "the Fourth Amendment and its exclusionary rule do not apply to the law enforcement activities of foreign authorities acting in their own country." *United States v. Busic*, 592 F.2d 13, 23 (2d Cir.1978); *see also United States v. Getto*, 729 F.3d 221, 227 n.7 (2d Cir. 2013) ("It is . . . well established that the Fourth Amendment's exclusionary rule generally does not apply to evidence obtained by searches abroad conducted by foreign officials."); *United States v. Lee*, 723 F.3d 134, 140 (2d Cir. 2013) (same). Thus, "'information furnished [to] American officials by foreign police need not be excluded simply because the procedures followed in securing it did not fully comply with our nation's constitutional requirements.'" *Getto*, 729 F.3d at 227 n.7 (quoting *United States v. Cotroni*, 527 F.2d 708, 711 (2d Cir. 1975)). "This is so even when 'the persons arrested and from whom the evidence is seized are American citizens.'" *Id.* (quoting *Stowe v. Devoy*, 588 F.2d 336, 341 (2d Cir. 1978)).

Searches by foreign law enforcement authorities implicate constitutional restrictions only in two narrowly limited circumstances: "(1) where the conduct of foreign law enforcement officials rendered them agents, or virtual agents, of United States law enforcement officials; or (2) where the cooperation between the United States and foreign law enforcement agents is designed to evade

constitutional requirements applicable to American officials." *Id.* at 230. As to the "virtual agency" exception, the Second Circuit has made clear that it applies only where U.S. authorities "have authority to control or direct an investigation abroad." *Id.* at 231. "It is not enough that the foreign government undertook its investigation pursuant to an American MLAT request." *Id.* at 230. Nor does it matter that the foreign government "would not have investigated . . . but for the MLAT request." *Id.* at 232. Even if the foreign authorities cooperated so closely with their U.S. counterparts as to make their efforts a "joint venture," the Fourth Amendment is not implicated. *Id.* at 233. Again, only where U.S. authorities "direct or otherwise control" the actions of foreign authorities do Fourth Amendment restrictions attach. *Id.* at 233.

In this case, the SR Server was imaged by Icelandic authorities, specifically, the RMP, after the RMP decided that the imaging was feasible and appropriate under Icelandic law. (Tarbell Decl. ¶ 12). RMP personnel obtained all legal process needed under Icelandic law to search the SR Server and executed the imaging of the server themselves. (*Id.*). The mere fact that the RMP did so in response to a request for assistance by the United States did not render them "virtual agents" of U.S. law enforcement. *See id.* at 231 & n.9 (finding no "virtual agency" where "American agents were not involved in the preparation, submission, and execution of search warrants" obtained by foreign authorities). While the RMP consulted with U.S. authorities concerning the timing of the imaging and shared the results of the operation promptly, such "robust information-sharing and cooperation" does not amount to U.S. direction and control. *Id.* at 232 (finding no "virtual agency" even where American and foreign agents were "in contact frequently" and foreign agents provided a live video feed of their surveillance activity to U.S. agents). Indeed, any contrary rule would only serve to discourage "successful coordinated law enforcement activity" between U.S. authorities and foreign governments. *Id.* at 233; *see also id.* at 232 (citing *United States v. Morrow*, 537 F.2d 120, 140 (5th

Cir. 1976) ("Normal lines of communication between the law enforcement agencies of different countries are beneficial without question and are to be encouraged.")).

Further, the cooperation between U.S. and Icelandic authorities was not designed to evade constitutional requirements. U.S. authorities approached Iceland for assistance because the FBI's investigation indicated that the SR Server was located in Iceland, and the FBI needed the help of Icelandic authorities in order to image its contents. *See Getto*, 729 F.3d at 232-33 (finding no intent to evade constitutional requirements where "the decision to request [foreign] assistance was motivated by the inability of American law enforcement agents to further investigate criminal activity occurring substantially within the territory of a foreign sovereign"). Ulbricht's conjecture that the FBI knew of the Silk Road backup servers inside the United States before approaching Iceland, and opted to ask Iceland to search the SR Server merely to avoid having to apply for a warrant for such U.S.-based servers, (Br. 35 n.17), is baseless. The reality is that the FBI did not learn of the Silk Road backup servers in the United States until after reviewing the image of the SR Server provided by Icelandic authorities, which was found to contain references to the IP addresses of such other servers. (Tarbell Decl. ¶ 15).

In short, the SR Server was imaged by foreign authorities acting under their own direction and control, based on a request by U.S. law enforcement driven by entirely proper investigative needs. Accordingly, the imaging was not subject to the restrictions of the Fourth Amendment.

*2. Even Assuming the Search of the Silk Road Server Was Subject to the Fourth Amendment, the Search Was Reasonable and Did Not Require a Warrant*

Even if Icelandic authorities had acted under the direction and control of U.S. authorities in searching the SR Server, a warrant would still not have been required for the search. It is well established that the Fourth Amendment's warrant requirement does not apply overseas – even to searches conducted directly by U.S. law enforcement agents of property belonging to a U.S. citizen. *See United States v. Vilar*, 729 F.3d 62 (2d Cir. 2013); *In re Terrorist Bombings of U.S. Embassies in*

*East Africa*, 552 F.3d 157, 167 (2d Cir. 2008). Instead, such searches "need only satisfy the Fourth Amendment's requirement of reasonableness." *In re Terrorist Bombings*, 552 F.3d at 167.

To determine whether a search is "reasonable" under the Fourth Amendment, a court must "examine the totality of the circumstances to balance, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Id*. at 172 (internal quotation marks omitted). Although probable cause to believe that a search will uncover evidence of crime is not necessarily required to establish that a search is reasonable, it is sufficient. *In re Terrorist Bombings of U.S. Embassies in East Africa*, 553 F.3d 150, 152 (2d Cir. 2009); *see also Whren v. United States*, 517 U.S. 806, 818 (1996) (holding that reasonableness determination is not usually necessary where probable cause exists). Here, the search of the SR Server was plainly reasonable: to the extent that Ulbricht had any legitimate privacy interest in the SR Server, which is doubtful, it was vastly outweighed by the fact that law enforcement had probable cause to believe the server was hosting the Silk Road website.

Whether Ulbricht had a legitimate expectation of privacy with respect to the SR Server is questionable at best. This 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. *See New York v. Burger*, 482 U.S. 691, 700 (1987) ("An expectation of privacy in commercial premises . . . is different from, and indeed less than, a similar expectation in an individual's home."); *cf. In re Terrorist Bombings*, 552 F.3d at 173 (finding that defendant had expectation of property with respect to his overseas home). Indeed, the SR Server was not even owned by Ulbricht. He leased it, anonymously, from a third-party webhosting service, which leased it in turn from the data center that owned it. (Tarbell Decl. ¶ 10). Moreover, the webhosting service had terms of service that prohibited the illegal use of its systems and that warned that its "systems may be monitored for all lawful purposes, including to ensure that use is authorized." (*Id.* & Ex. C). Accordingly, Ulbricht had little reason to assume that the illegal drug-trafficking enterprise he was

running on the SR Server would remain private. *See United States v. Warshak*, 631 F.3d 266, 287 (6th Cir. 2010) (en banc) (noting that subscriber may lack reasonable expectation of privacy where provider's terms of service express an intention to "monitor" contents of subscriber accounts); *United States v. Bode*, 12 Cr. 158 (ELH), 2013 WL 4501303, at *18 (D. Md. Aug. 21, 2013) (holding that chat service user had no reasonable expectation of privacy where terms of service warned that communications over service would be "logged and supervised" and potentially reported to authorities); *see generally United States v. Gray*, 491 F.3d 138, 146 (4th Cir. 2007) ("[T]hose who venture forth to conduct illegal business often do not hold a legitimate expectation of privacy in locations that are not their own.").

In any event, whatever expectation of privacy Ulbricht did have in the SR Server, it was plainly outweighed by the Government's legitimate need to search its contents. The Government had ample evidence, easily enough to establish probable cause, that the SR Server was hosting the Silk Road website. The FBI had detected the IP address of the SR Server leaking in web traffic sent back from the Silk Road website. (Tarbell Decl. ¶ 7). When the FBI input the IP address into an ordinary web browser, a part of the Silk Road login interface appeared. (*Id.* ¶ 8). Further, traffic data for the SR Server provided by Icelandic authorities showed large volumes of Tor traffic flowing to the server, consistent with a Tor hidden service such as the Silk Road website. (*Id.* ¶ 11). Accordingly, the Government had probable cause to believe that the SR Server was hosting the Silk Road website, and that it was therefore likely to contain extensive evidence, fruits, and instrumentalities of crime, given that the website was known to host a vast criminal enterprise.

Under the circumstances, searching the server was more than reasonable. It was a law enforcement imperative that would have been a gross dereliction of duty for the Government not to pursue.

*3. Obtaining a Warrant under the Stored Communications Act to Search the Silk Road Server Was Neither Feasible Nor Required*

Notwithstanding the above, Ulbricht argues, with little in the way of explanation, that the Government was required to obtain a warrant to search the SR Server pursuant to the Stored Communications Act, *codified in relevant part at* 18 U.S.C. § 2703 ("SCA"). (Br. 36). However, obtaining an SCA warrant was not even an option, let alone required, given that the SR Server was controlled by a foreign data center.

The SCA provides for several forms of process through which the Government may compel electronic communication service providers and remote computing service providers to produce customer records to the Government, including the contents of communications. In particular, the SCA enables the Government to compel such production without notice to the customer by obtaining a search warrant. *See* 18 U.S.C. § 2703(a)&(b)(1)(A). Thus, using a warrant issued pursuant to the SCA, the Government may compel a data center that leases servers to the public to produce the contents of a particular server, without notifying the customer involved.

However, the SCA applies only to providers that are subject to service of U.S. legal process and to the personal jurisdiction of U.S. courts. By contrast, the SR Server was maintained at an overseas data center operated by an Icelandic company with no apparent presence in the United States. Thus, Ulbricht's reliance on *In the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corporation*, __ F. Supp. 2d __, 2014 WL 1661004 (S.D.N.Y. 2014), is misplaced. That ruling concerned enforcement of an SCA warrant against Microsoft, with respect to data stored abroad at a Microsoft overseas data center. The warrant was held to be enforceable because, even though the data was stored abroad, Microsoft still controlled it and, as a U.S.-based company, was subject to the issuing court's jurisdiction. *See id.* at *10 ("[A]n entity subject to jurisdiction in the United States, like Microsoft, may be required to obtain evidence from abroad in connection with a criminal investigation."). In this case, the SR Server was

maintained by a foreign company outside U.S. jurisdiction, rendering the SCA of no avail, as an SCA warrant could neither be served on the company nor enforced against it.

Even if the SCA had been somehow applicable here, nothing would have *required* the Government to use it to obtain the contents of the SR Server. The SCA merely provides one mechanism for the Government to obtain the contents of data stored by a third-party provider; it does not purport to provide the exclusive mechanism. *See* 18 U.S.C. §§ 2703(a)&(b)(1)(A) (providing that the Government "may" require a provider to disclose records with a warrant issued under the statute). The Government is free to use any other available means to obtain such data – such as a traditional physical search warrant under Rule 41 where the data is stored within the United States, or a request for foreign law enforcement assistance where the data is stored overseas – if the Government deems preferable.

### C. There Was No Material Omission Concerning the Discovery of the Silk Road Server in Any Search Warrant Applications for Other Electronically Stored Information

Beyond arguing that a warrant was required to search the SR Server itself, Ulbricht also faults the Government for failing to disclose how it located the server in its subsequent applications for various search warrants in the investigation. (Br. 36-37). Ulbricht even faults the magistrate judges who approved these applications, whom Ulbricht accuses of failing to inquire into the "lawfulness and/or reliability" of the means used by the Government. (*Id.*) These contentions are meritless.

A search warrant affidavit need not contain "every piece of information gathered in the course of an investigation." *United States v. Awadallah*, 349 F.3d 42, 67–68 (2d Cir. 2003) (internal quotation marks omitted); *see also United States v. Rajaratnam*, 719 F.3d 139, 153-54 (2d Cir. 2013) (same). Rather, an affidavit need only include those facts "'*necessary* to the finding of probable cause'" – as opposed to including any fact that "might have been relevant to that finding" or that may have been "of interest to a magistrate judge." *United States v. Vilar*, 05 Cr. 0621 (KMK), 2007 WL

1075041, at *27 (S.D.N.Y. Apr. 4, 2007) (emphasis in original) (quoting *Franks v. Delaware*, 438 U.S. 154, 156 (1978)).

Accordingly, where an affidavit is challenged for omitting certain information, courts apply an "exacting standard": "To require suppression, a movant must demonstrate, by a preponderance of the evidence, both the affiant's *intent* to mislead the issuing judge and the *materiality* of the affiant's . . . omissions." *United States v. Lahey*, 967 F. Supp. 2d 698 (S.D.N.Y. 2013) (emphasis in original). As to intent, it must be shown that the omissions in question were "the result of the affiant's deliberate falsehood or reckless disregard for the truth." *United States v. Canfield*, 212 F.3d 713, 717-18 (2d Cir. 2000). As to materiality, it must be shown that the omission was "necessary to the [issuing] judge's probable cause finding," such that, if the omitted information had been included, the warrant would not have been issued. *Id.* at 718.

There was no such omission of material information – intentional or unintentional – from any search warrant affidavit submitted in the Government's investigation here. All the affidavits explained that the FBI had located the server hosting the Silk Road website in a foreign country, obtained an image of the server's contents through an official request to that country, and subsequently confirmed, through forensic examination of that image, that the server was in fact hosting the Silk Road website. (Tarbell Decl. Exs. E-G & L-O). Nothing further needed to be said in the affidavits to establish that the Government had obtained a reliable copy of the SR Server. In particular, there was no need to delve into the details of the means by which the FBI had located the SR Server in the first place. All that mattered was that the FBI had in fact located it, as its forensic examination of the server had confirmed. *How* the FBI had done so was not necessary to establish probable cause for subsequent searches of other property. *See Wilson v. Russo*, 212 F.3d 781, 787 (3d Cir.2000) ("All storytelling involves an element of selectivity. We cannot demand that police

officers relate the entire history of events leading up to a warrant application with every potentially evocative detail that would interest a novelist or gossip.").[4]

Nor was the Government required to detail how it located the SR Server in order to establish the "lawfulness" of the evidence found therein. Again, the affidavits explained the legal mechanism through which the Government obtained a copy of the SR Server: it was obtained from a foreign nation through an official request for legal assistance. There was no need to explain further in order to dispel any baseless suspicions, like those of Ulbricht here, that the Government had used nefarious methods to locate the server in the first instance. The actions of law enforcement officials are presumed to be lawful, not the other way around. *See Franks*, 438 U.S. at 171 ("There is . . . a presumption of validity with respect to the affidavit supporting [a] search warrant."); *see generally United States v. Chemical Foundation*, 272 U.S. 1, 14–15 (1926) (holding that government officials enjoy a "presumption of regularity" and are presumed to have "properly discharged their official duties"). Moreover, the Government in fact had nothing to hide, as the FBI had located the SR Server using entirely lawful means. Had those means been detailed in the search warrant affidavits, it would have made no difference to the probable cause analysis. If anything, the Government's probable cause showing would have only been strengthened, insofar as the explanation of how the SR Server was located would have simply corroborated the authenticity of the server image received from Icelandic authorities. *See Rajaratnam*, 719 F.3d at 155 (finding no material or intentional omission from wiretap application where "it [was] clear that fully disclosing [the omitted information] would only have *strengthened* the . . . application[ ]" (emphasis in original)).

There is likewise no merit in Ulbricht's contention that the magistrate judges who approved the Government's search warrant affidavits somehow abdicated their responsibility by not pressing

[4] Indeed, each of the search warrant affidavits prepared in the investigation expressly stated that it was being submitted for the limited purpose of establishing probable cause for a particular search and therefore did not include all the facts learned during the investigation.

the Government for details as to how it located the SR Server. A magistrate's determination of probable cause is owed "great deference" by reviewing courts, *Illinois v. Gates*, 462 U.S. 213, 236 (1983), and, for the above reasons, there is certainly no reason to disturb that deference here. Indeed, three different magistrate judges in three different judicial districts all approved the affidavits at issue, including the nearly identical language they all contained concerning the discovery of the SR Server. Deference to their determinations is thus especially warranted. *See United States v. Carpenter*, 341 F.3d 666, 670 (8th Cir. 2003) (fact that multiple judges found application to establish probable cause underscores deference owed by reviewing court).

### D. The Pen Registers Used to Monitor Ulbricht's Internet Activity Collected Purely Non-Content Data and Did Not Require a Warrant

Ulbricht devotes a considerable number of pages in his motion to arguing that the Pen Registers, which were used to log his Internet activity, were unlawful because they were obtained without a warrant. (Br. 37-48). The argument has no support in statute or case law, and should be rejected.

The Pen Registers did not collect the contents of Ulbricht's Internet communications, or anything that might arguably be characterized as contents. In particular, contrary to Ulbricht's speculation, the Pen Registers did not collect things like the website addresses of the "New York Times . . . articles" Ulbricht viewed or the "search phrases" Ulbricht entered into Google. (Br. 41). Instead, the Pen Registers collected only routing data associated with Ulbricht's Internet traffic – mainly, the IP addresses to which Ulbricht was connecting, and the dates, times, and durations of those connections. This 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.

All of the Pen Registers were validly obtained pursuant to the pen register statute, 18 U.S.C. § 3121 *et* seq. That statute defines a "pen register" to mean a process for recording "dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted," 18 U.S.C. § 3127(3) – which is precisely what was collected through the Pen Registers.[5] As the statute requires, to obtain the Pen Registers, the Government certified to a judge that the information likely to be collected through the Pen Registers was relevant to an ongoing criminal investigation. 18 U.S.C. § 3122. The statute requires no more; in particular, it does not require that the Government obtain a warrant based on a showing of probable cause.

The Supreme Court long ago affirmed that a warrant is not constitutionally required for pen register information. Specifically, the Court held in *Smith v. Maryland*, 442 U.S. 735 (1979), that the use of a pen register on a phone line does not constitute a search for Fourth Amendment purposes. *Id*. at 745–46. As the Court explained, every phone user "must convey [incoming and outgoing] phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." *Id*. at 742 (internal quotation marks omitted). Because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," a warrant is not needed for the Government to collect such information through a pen register. *Id*. at 743–44. The Court distinguished pen registers from more intrusive surveillance techniques requiring a showing of probable cause, such as

[5] A "pen register" records such information for outgoing signals, while a "trap and trace device" is defined under the statute to mean a process for recording such information for incoming signals. The pen register orders in this case authorized the use of both a pen register and trap and trace device with respect to the facilities at issue. The orders are referred to herein as "pen registers" simply for brevity.

wiretaps, on the ground that "pen registers do not acquire the contents of communications" but rather obtain only the routing information associated with phone calls. *Id*. at 741.

The use of a pen register to collect routing data with respect to a user's Internet activity is "constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*." *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). Like telephone users, Internet users "rely on third-party equipment in order to engage in communication" and "have no expectation of privacy in . . . the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information." *Id.* Moreover, "IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers." *Id.* "At best, the government may make educated guesses about what was viewed on the websites [visited by the user] based on its knowledge of the . . . IP addresses – but this 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." *Id.* Accordingly, IP address and similar routing information is not protected by the Fourth Amendment and can be collected through a pen register as opposed to a warrant. *Id.*; *accord In re Nickelodeon Consumer Privacy Litigation*, MDL No. 2443 (SRC), 2014 WL 3012873 (D.N.J. Jul. 2, 2014); *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, 48 (D. Mass. 2005).

Much of Ulbricht's argument challenging the Pen Registers appears to be based on the erroneous premise that the data collected from the Pen Registers was used to track Ulbricht's geolocation. (Br. 45-48). That is simply not what the Pen Registers were used for. They were used to detect when Ulbricht was logged onto the Internet and to record what IP addresses he

was visiting. The Pen Registers did not collect any geolocation data and thus could not have been used to track Ulbricht's location in any event. (Tarbell Decl. ¶ 21.) At most, one might be able to infer from Internet activity on Ulbricht's residential ISP account when he was likely inside the residence, but this is no different from being able to infer that a subject is at home when a pen register on his landline phone shows it to be in use. The Supreme Court's holding in *Smith* precludes the imposition of a warrant requirement on that basis alone.

Ulbricht lastly makes the perfunctory claim that the Pen Registers amounted to "general warrants" because they did not include "minimization procedures." (Br. 49). However, "minimization procedures" are only applicable to interceptions of the contents of communications under Title III. They are not applicable to mere pen registers. *See United States v. Rizzo*, 491 F.2d 215, 216 n.3 (2d Cir. 1974) ("[N]either state nor federal minimization laws are applicable to mere interception of what telephone numbers are called, as opposed to the interception of the contents of the conversations.").

### E. The Search Warrants for Electronically Stored Information Satisfied the Particularity Clause and Were Not Overbroad

Ulbricht's final suppression argument is directed at several search warrants the Government obtained during the investigation for electronically stored information – specifically, the two warrants for the Backup Servers located in Pennsylvania (the "Backup Server Warrants"), the warrant for Ulbricht's laptop (the "Laptop Warrant"), and the warrant for Ulbricht's email and Facebook accounts (the "Email/Facebook Warrants"). Ulbricht contends that all of these warrants were "general warrants" that failed to place appropriate limits on the discretion of the agents conducting the search. This argument is meritless. As detailed below, none of the warrants at issue were "general warrants." The warrants all satisfied the Fourth Amendment's particularity requirement, by specifying the categories of evidence agents were

authorized to search for, and they were not overbroad, as the categories listed were each supported by probable cause.

*1. The Backup Server Warrants Were Not "General Warrants"*

Ulbricht contends – in an argument consisting of a mere two sentences – that the Backup Server Warrants were "general warrants" because they authorized a "search of the *entire* server(s)" on which the backups of Silk Road were stored. (Br. 49 (emphasis in original)). Ulbricht argues that this was improper because "the commerce on Silk Road included legitimate transactions" along with illegitimate ones. (*Id.*). The 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 the law.

As an initial matter, it was wholly proper, and consistent with routine practice, for the Backup Server Warrants to authorize a search of the backup servers in their entirety for the categories of evidence specified in the warrants. *See In the Matter of a Warrant for All Content and Other Information Associated with the Email Account xxxxxxx@gmail.com*, __ F. Supp. 2d ___, 2014 WL 3583529, at *5 (S.D.N.Y. Jul. 18, 2014) (Gorenstein, M.J.) (surveying case law reflecting that courts "routinely" uphold searches of entire computers in executing search warrants for electronically stored information). [6] Indeed, this procedure is not merely proper but

[6] Ulbricht acknowledges Judge Gorenstein's opinion at one point of his brief, yet points to two contrary opinions by magistrate judges in other districts. (Br. 57 (citing *In the Matter of the Search of Information Associated with [Redacted] @mac.com that is Stored at Premises Controlled by Apple, Inc.*, 2014 WL 1377793 (D.D.C. Apr. 7, 2014) and *In the Matter of Applications for Search Warrants for Information Associated With Target Email Accounts/Skype Accounts*, 2013 WL 4647554 (D. Kan. Aug. 27, 2013)). The first opinion, however, was recently reversed, *see In the Matter of the Search of Information Associated with [Redacted] @mac.comthat is Stored at Premises Controlled by Apple, Inc.*, __ F. Supp. 2d __, 2014 WL 4094565, at *4-*6 (D.D.C. Aug. 7, 2014), while the reasoning of the second was rejected by the authoring magistrate judge's district court, *see United States v. Deppish*, __ F. Supp. 2d __, 2014 WL 349735, at *6-*7 (D. Kan. Jan. 31, 2014).

necessary, as there is typically no way for law enforcement agents to know in advance what precise data will be found in the device, or where the data will be stored. The principle is the same with respect to searches of physical documents: "In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized." *Andresen v. Maryland*, 427 U.S. 463, 482 n. 11 (1976). As the Second Circuit has noted, "allowing some latitude in this regard simply recognizes the reality that few people keep documents of their criminal transactions in a folder marked 'drug records.'" *United States v. Riley*, 906 F.2d 841, 845 (2d Cir. 1990).

As for the scope of the evidence the Backup Server Warrants authorized agents to "seize," *i.e.*, locate, on the servers, the warrants used language properly tailored to the criminal investigation, including, in the warrants' most expansive clause, "any evidence concerning . . . an underground website operating a marketplace for illegal drugs and other illegal goods and services." (Tarbell Decl., Exs. E-G (warrant riders)). To the extent that such language authorized a broad search for any evidence relating to the operation of Silk Road, the language was appropriately broad. "When . . . criminal activity pervades [an] entire business, seizure of all records of the business is appropriate, and broad language used in warrants will not offend the particularity requirements." *U.S. Postal Service v. C.E.C. Servs.*, 869 F.2d 184, 187 (2d Cir. 1989); *see also United States v. Bowen*, 689 F. Supp. 2d 675, 683 (S.D.N.Y. 2010) (noting the propriety of seizing "all of an enterprise's records when the enterprise is primarily engaged in unlawful activity and sufficient evidence is presented of the pervasiveness of that unlawful activity within the enterprise").

If there was ever a business enterprise that was "pervaded" by criminal activity, it is Silk Road. Notwithstanding Ulbricht's attempts to portray Silk Road as some kind of content-neutral

website that happened to be used occasionally by criminals, in fact Silk Road was, as the application for the Backup Server Warrants explained, "dedicated to the sale of illegal narcotics and other black-market goods and services." (Tarbell Decl., Ex. E-G, ¶ 6). The application elaborated:

> The illegal nature of the wares on sale through the website is readily apparent to any user visiting the site. Illegal drugs, such as heroin and cocaine, are openly advertised and sold on the site and are immediately and prominently visible on the site's home page. Moreover, there is a discussion forum linked to the site in which the site's users frequently and openly discuss, among other things, how to conduct transactions on the site without being caught by law enforcement.

(*Id.*) The application further explained that the illegal commerce on Silk Road was no accident. It detailed how the website was "specifically designed to facilitate the illegal commerce hosted on the site by ensuring absolute anonymity on the part of both buyers and sellers," through the use of the Tor network and the site's Bitcoin-based payment system. (*Id.* ¶ 7). All of these assertions were accurate. As the evidence at trial will show, the amount of commerce on Silk Road that had no obvious criminal component was trivial compared with the blatantly illegal commerce the site hosted, which consisted overwhelmingly of drug trafficking.

Accordingly, it is unremarkable that the Backup Server Warrants used broad language in authorizing a search of the servers. As is typically the case with an illegal business, it was not possible to segregate "legitimate" transactions from "illegitimate" transactions in searching the servers. All of the transactions conducted on the site were recorded in a single website database. Excising "legitimate" transactions from that database would not even have been feasible without impairing the integrity of the data. *See C.E.C. Servs.*, 869 F.2d at 187 (upholding broad search of business engaged in fraudulent scheme given that it would have been "virtually impossible to segregate" records unrelated to scheme); *United States v. Johnson*, 886 F. Supp. 1057, 1072 (W.D.N.Y. 1995) (explaining that search of all of a business's records is justified where its

criminal operations are "inseparable from the other business operations" (internal quotation marks omitted)).

Moreover, *all* of the transactions reflected in the database *are* relevant to the case. Just as a business's entire bookkeeping records are typically relevant where the business is suspected of engaging in fraud – even though the books may reflect some lawful transactions – Silk Road's transactional database was similarly subject to seizure in its entirety. To the extent there may be certain transactions reflected in the server data that were not illegal by themselves, such transactions nonetheless provide relevant context and allow for a full understanding of the nature and scope of the illegal activity hosted on the site. Indeed, the fact that there were so few such transactions conducted on Silk Road underscores the site's pervasive criminality. *See Cohan*, 628 F. Supp. 2d at 364 ("[C]ourts have often found probable cause for the seizure of the records of 'innocent' transactions when those records made the [criminality] of other transactions clear."); *United States v. Blumberg*, 97 Cr. 119 (EBB), 1998 WL 136174, at *7 (D. Conn. Mar. 11, 1998) ("To force the government to limit the search to documents containing evidence of a crime, as the defendants assert should have been done, was impractical since legitimate business records are also material to a reconstruction of the methodology and extent of . . . a complex scheme."); *United States v. Regan*, 706 F. Supp. 1102, 1113 (S.D.N.Y. 1989) ("[M]aterial evidence of criminal activity is not necessarily limited just to evidence describing the criminal activity . . . . In order to reconstruct defendants' true financial . . . picture, evidence regarding legal as well as illegal transactions may be necessary.").

Accordingly, there was nothing improper about the breadth of the Backup Server Warrants.

*2. The Laptop and Email/Facebook Warrants Were Not "General Warrants"*

As to the Laptop Warrant and Email/Facebook Warrants, Ulbricht argues they amounted to "general warrants" because they "expressly included materials and information for which probable cause did not exist." (Br. 49-50). Ulbricht points to two clauses in the warrants in particular – authorizing agents to seize "any communications or writings by Ulbricht" and "any evidence concerning Ulbricht's travel or patterns of movement" – which Ulbricht characterizes as a license for agents to engage in "unrestrained rummaging" through his private papers in violation of the Fourth Amendment. Notwithstanding this inflammatory rhetoric, the inclusion of these categories of evidence in the warrants was specifically justified by probable cause set forth in the underlying warrant applications, and did not give rise to "general warrants."

At the outset, Ulbricht consistently misuses the term "general warrant." The term does not refer to warrants that merely provide agents with broad search authority, or even search authority extending beyond the probable cause showing made in the warrant application. A "general warrant" is a warrant that fails to specify the scope of an authorized search *at all*. Historically, the term was used to describe the "indiscriminate searches and seizures" conducted by the British in colonial times, pursuant to warrants that "specified only an offense – typically seditious libel – and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Steagald v. United States*, 451 U.S. 204, 220 (1981). The particularity requirement of the Fourth Amendment was intended to prevent such searches, by requiring that a warrant specify: (1) the offenses for which probable cause has been established; (2) the places to be searched; and (3) the items to be seized relating to the specified offenses. *See United States v. Galpin*, 720 F.3d 436, 445-46 (2d Cir. 2013).

The Laptop Warrant and Email/Facebook Warrants do not remotely resemble "general warrants." The warrants specify the offenses for which the accompanying agent affidavits

established probable cause; they specify the places to be searched – Ulbricht's laptop and his email and Facebook accounts; and they list numerous categories of evidence the agents were authorized to "seize," *i.e.*, locate, in the searched data.

The warrants are in no way comparable to warrants that the Second Circuit has found to be so lacking in particularity as to constitute "general warrants." Ulbricht points to *United States v. Galpin*, 720 F.3d 436 (2d Cir. 2013), but in that case the warrant violated the particularity requirement because it "generally authorized officers to search [a defendant's] physical property and electronic equipment for evidence of violations of 'NYS Penal Law and or Federal Statutes'" – thus failing to limit the search to specified offenses. *Id.* at 447. Here, by contrast, the warrants specified the crimes at issue – narcotics trafficking, money laundering, computer hacking, and murder for hire. (Tarbell Decl., Ex. M-O (warrant riders)). The Second Circuit has also found warrants to be "general warrants" where they specify the offense but fail to provide *any* specific guidance on the items relating to the offense that are subject to seizure. *See United States v. Buck*, 813 F.2d 588, 590 (2d Cir. 1987) (holding insufficiently particular a search warrant authorizing the seizure of "any papers, things or property of any kind relating to [the] previously described crime"). But again, here, the warrants did provide such guidance, as they contained extensive lists of the categories of evidence that were the object of the search.[7]

[7] The Laptop Warrant, for example, authorized seizure of:

1. Any evidence relating in any way to the Silk Road website, including but not limited to:
    a. any copies, backups, drafts, fragments, or other forms of data associated with the Silk Road website, such as web content, server code, or database records associated with the site;
    b. any evidence concerning any servers or other computer equipment or services associated with Silk Road, including but not limited to: encryption keys, login credentials, or other access devices used to access or control such equipment or services; records of logins to such equipment or services; communications with or records of payments made to any providers of such equipment or services; and

Ulbricht objects to the categories in the warrants covering "any communications or writings by Ulbricht" and "any evidence concerning Ulbricht's travel or patterns of movement"; but these categories do not run afoul of the particularity requirement. They are phrased in clear language and "identify with reasonable certainty those items that the magistrate has authorized [the agents] to seize," as opposed to simply leaving it to the agents' discretion what may be seized. *United States v. George*, 975 F.2d 72, 75 (2d Cir. 1992). Ulbricht's true objection instead seems to be that these categories are overbroad, *i.e.*, that they extend beyond the scope of

---

records concerning the IP addresses or locations of any such equipment or services;

c. any records of e-mails, private messages, forum postings, chats, or other communications concerning Silk Road in any way, including but not limited to communications with Silk Road administrators or users;
d. any evidence concerning funds used to facilitate or proceeds derived from Silk Road, including but not limited to: Bitcoin "wallet" files; records of any Bitcoin transactions, including transactions with any Bitcoin exchangers; information concerning any computer devices, file locations, or Bitcoin addresses where any Bitcoins may be stored; information concerning any financial accounts or safe deposit boxes where Silk Road funds may be stored; and any spreadsheets, ledgers, or other documents concerning Silk Road funds;
e. any evidence concerning any illegal activity associated with Silk Road, including but not limited to narcotics trafficking, money laundering, computer hacking, and identity document fraud; and
f. any evidence of the use of the Tor network or any other methods used to anonmyize or conceal activity on the Internet and to evade law enforcement.

2. Any evidence concerning ROSS WILLIAM ULBRICHT relevant to the investigation of the SUBJECT OFFENSES, including but not limited to:
   a. any communications or writings by ULBRICHT;
   b. any evidence concerning any computer equipment, software, or usernames used by ULBRICHT;
   c. any evidence concerning ULBRICHT'S travel or patterns of movement;
   d. any evidence concerning ULBRICHT's technical expertise concerning Tor, Bitcoins, computer programming, website administration, encryption, or any other area of technical expertise relevant to administering the Silk Road website;
   e. any evidence concerning any efforts by ULBRICHT to obtain fake identification documents;
   f. any evidence concerning any aliases used by ULBRICHT; and
   g. any evidence concerning any effort to evade law enforcement.

(Tarbell Decl., Ex M (warrant rider)).

the probable cause established in the warrant applications. However, the warrant applications specifically explained why these categories of evidence were included in the warrants: they were "relevant to corroborating the identification of Ulbricht as the Silk Road user 'Dread Pirate Roberts.'" (Tarbell Decl., Ex. M ¶ 44; *see also id.* Ex. N ¶ 8, Ex. O ¶ 9).

That identification was the fundamental objective of the Government's investigation. The criminality of the conduct of the Silk Road user "Dread Pirate Roberts" was manifest throughout the operation of Silk Road. The mystery was his true identity. And the Government sought to analyze Ulbricht's writings and his travel patterns in order to confirm that "Dread Pirate Roberts" was indeed Ulbricht. As the warrant applications explained, the Government had initially identified Ulbricht as "Dread Pirate Roberts" based on parallels between the online persona of "Dread Pirate Roberts" on Silk Road and postings by Ulbricht on the Internet – including parallels in the tone, style, and viewpoints reflected in the writings of each. (Tarbell Decl., Ex. M ¶¶ 20-27, Ex. N ¶¶ 6-8, Ex. O ¶¶ 7-9). Even similarities in spelling tendencies – such as the spelling of "yeah" as "yea" – had been identified as a link between "Dread Pirate Roberts" and Ulbricht, as noted in the warrant applications. (*Id.*). Accordingly, the warrant applications requested authorization to retrieve Ulbricht's "writings and communications" from the Laptop and Gmail/Facebook Accounts to allow for further comparison of Ulbricht's writings and communications with those of "Dread Pirate Roberts," and thereby corroborate the identity between the two. (*Id.*)

The Government had also linked Ulbricht to "Dread Pirate Roberts" based on comparisons of the times when "Dread Pirate Roberts" was active on Silk Road with the times when Ulbricht was logged into the Internet, as reflected in pen register records. (Tarbell Decl., Ex. M ¶¶ 33-41). Thus, the applications also requested authorization to search for evidence of

Ulbricht's travel or patterns of movement, "to allow comparison with patterns of online activity of 'Dread Pirate Roberts' and any information known about his location at particular times." (Tarbell Decl., Ex. M ¶ 44.c, Ex. N ¶ 8.c, Ex. O ¶ 9.c). Again, such evidence was relevant to further corroborating the identity between Ulbricht and "Dread Pirate Roberts."

A reviewing court should pay "great deference" to a magistrate judge's probable cause determination. *United States v. Smith*, 9 F.3d 1007, 1012 (2d Cir. 1993). Here, the warrant language protested by Ulbricht was approved by two different magistrate judges in two different districts, again underscoring the appropriateness of such deference. *See Carpenter*, 341 F.3d at 670. While the language at issue was broad, the magistrate judges were entitled to authorize it based on their conclusion that it was supported by probable cause. *United States v. Hickey*, 16 F. Supp. 2d 223, 240 (E.D.N.Y. 1998) ("[A] warrant—no matter how broad—is, nonetheless, legitimate if its scope does not exceed the probable cause upon which it is based."). Here, the affidavits submitted to the magistrate judges specifically explained why evidence of Ulbricht's writings and patterns of movement was needed: to help corroborate the identification of Ulbricht as "Dread Pirate Roberts."[8] Particularly given that Ulbricht had gone to extraordinary lengths to operate anonymously on Silk Road and to conceal his identity as "Dread Pirate Roberts," the Government was entitled to seek as many sources of evidence as possible to confirm that identity. *See Cohan*, 628 F. Supp. at 362 (broad warrant language permissible where needed to

[8] *See United States v. Cohan*, 628 F. Supp. 2d 355, 364 n.4 (E.D.N.Y. 2009) ("[T]he affidavit must . . . be considered for purposes of an overbreadth (i.e., probable-cause) analysis because . . . the probable-cause analysis must be performed from the perspective of the magistrate who issued the warrant." (citations omitted)).

investigate a "complex . . . scheme whose existence could be proved only by piecing together many bits of evidence" (internal quotation marks omitted)).[9]

Even if the magistrate judges who issued the warrants were deemed to have erred by approving the clauses Ulbricht finds objectionable, application of the exclusionary rule would not be appropriate, as the agents were entitled to rely in good faith upon the magistrate judges' probable cause determination in executing the searches at issue. *See United States v. Leon*, 468 U.S. 897, 921 (1984) ("It is the magistrate's responsibility to determine whether the officer's allegations establish probable cause and, if so, to issue a warrant comporting in form with the requirements of the Fourth Amendment."). This is not a case where the warrant applications were "so lacking in indicia of probable cause" or where the warrant was so "facially deficient" that reliance upon the warrant was "entirely unreasonable," so as to render the good-faith exception inapplicable. *Leon*, 468 U.S. at 923. To the contrary, the agents who executed the warrant affidavits specifically explained the probable cause supporting the two warrant clauses in question. And the magistrate judges clearly accepted the agents' explanation, as they signed the warrants with these clauses included, as part of a larger list of categories of "evidence concerning ROSS WILLIAM ULBRICHT relevant to the investigation of the SUBJECT OFFENSES." (Tarbell Decl., Exs. M-O (warrant riders)). A law enforcement agent is not "required to disbelieve a judge who has just advised him, by word and by action, that the warrant he

[9] The identification evidence sought did not itself need to directly reflect criminal activity in order to be a proper object of the search. The Fourth Amendment requires "only probable cause . . . to believe the evidence sought will aid in a particular apprehension or conviction." *Messerschmidt v. Millender*, 132 S. Ct. 1235, 1248 (2012) (internal quotation marks omitted) (upholding search warrant authorizing search for evidence of gang membership in connection with investigation of assault, even though gang membership was not an element of the crime charged, on basis that "membership in a gang might prove helpful in impeaching [defendant] or rebutting various defenses he could raise at trial").

possesses authorizes him to conduct the search he has requested." *Buck*, 813 F.2d at 592 (quoting *Massachusetts v. Sheppard*, 468 U.S. 981, 989–90 (1984)); *see also United States v. Falso*, 544 F.3d 110, 129 (2d Cir. 2008) (declining to hold that agents acted unreasonably in relying on judge's probable cause determination because "the error . . . was committed by the district court in issuing the warrant, not by the officers who executed it"); *United States v. Cancelmo*, 64 F.3d 804, 807 (2d Cir.1995) (holding that any error in issuance of warrant was "attributable to the magistrate who determined that the facts as alleged by the agents established probable cause").

Finally, even if the magistrate judges were deemed to have erred in finding probable cause for the requests to review Ulbricht's writings and patterns of movement, *and* the agents were deemed to have acted unreasonably in relying on the magistrate judges' findings, suppression of the warrants in their entirety – which is what Ulbricht seeks – would still not be appropriate. "[A] search conducted pursuant to a warrant held unconstitutional in part does not invalidate the entire search." *George*, 975 F.2d at 79. Rather, the Fourth Amendment requires "suppressing only those items whose seizure is justified *solely* on the basis of the constitutionally infirm portion of the warrant." *Id.* (emphasis added); *see also Galpin*, 720 F.3d at 448 ("[I]t would be unduly 'harsh medicine' to suppress evidence whose seizure was authorized by a particularized portion of a warrant simply because other portions of the warrant failed that requirement."). As long as the invalid parts of a warrant are "distinguishable from the nonvalid parts," and the valid parts do not "make up 'only an insignificant or tangential part of the warrant,'" severance is appropriate. *Galpin*, 720 F.3d at 448-49 (quoting *George*, 975 F.2d at 80).

Here, the clauses at issue were only two clauses in an extensive list of clauses in the Laptop Warrant and Email/Facebook Warrants detailing the categories of evidence to be seized. Ulbricht does not raise any specific objection to these other clauses; nor could he, for they describe evidence that was undeniably relevant to the investigation of Ulbricht and his role in administering Silk Road. For example, the warrant for the Laptop authorizes agents to seize, among other things: copies or drafts of content from the Silk Road website; evidence concerning any computer servers used to operate the website; communications with Silk Road users and administrators; Bitcoin wallets where Silk Road proceeds may be stored; evidence concerning any narcotics trafficking activity on Silk Road; evidence concerning Ulbricht's technical expertise concerning Tor, Bitcoins, and computer programming; and evidence of aliases used by Ulbricht and any efforts by Ulbricht to evade law enforcement. The warrants for Ulbricht's email and Facebook account contained many similarly detailed and unobjectionable categories of evidence that agents were authorized to search for. These portions of the warrant are readily distinguishable from the clauses of the warrant to which Ulbricht objects, and by no means constitute an "insubstantial" or "tangential" part of the warrant. Accordingly, even if Ulbricht's objections had merit – which they do not – the remedy would be to excise the two particular clauses to which his objections attach, leaving the remaining clauses intact. *See Vilar*, 2007 WL 1075041, at *31 (finding severance appropriate where the warrant contained "[m]any . . . paragraphs . . . both sufficiently particularized and firmly rooted in probable cause").

**F. None of Ulbricht's Arguments Merit a Suppression Hearing**

Because Ulbricht's motion is built on a hollow foundation of factual conjecture and specious legal claims, there is no need to conduct a suppression hearing in order to resolve the motion. A suppression hearing is required only where "the moving papers are sufficiently definite, specific, detailed, and nonconjectural to enable the court to conclude that contested issues of fact going to the

validity of the search are in question." *United States v. Pena*, 961 F.2d 333, 339 (2d Cir. 1992). Because a suppression motion must be supported by an affidavit of someone alleging personal knowledge of the relevant facts, *United States v. Gillette*, 383 F.2d 843, 848 (2d Cir. 1967), an evidentiary hearing should be denied where the motion is supported by mere conjecture and speculation. *United States v. Ferguson*, 758 F.2d 843, 849 (2d Cir. 1985). Statements submitted by an attorney in motion papers before a district court "cannot by themselves create a factual issue" that would justify a hearing. *United States v. Mottley*, 130 F. App'x 508, 509-10 (2d Cir.2005).

Because Ulbricht's motion has failed to raise any factual issue supported by competent evidence, Ulbricht's motion should be denied without a hearing.

**POINT II:**
**ULBRICHT'S DISCOVERY REQUESTS SHOULD BE DENIED**

Lacking any evidence to support his hypothesis that it was the "NSA" that located the SR Server through some unspecified unlawful means, and that the FBI engaged in "parallel reconstruction" after the fact to build the case against him, Ulbricht lards his motion with over twenty sweeping requests for discovery, 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." (Br. 60-61). Ulbricht has failed to make any specific showing of materiality that would justify these requests, and they should therefore be denied.

Ulbricht's discovery requests are based on nothing more than a figment of Ulbricht's imagination – that his Fourth Amendment rights were somehow violated by the "NSA" – as opposed to a competent showing of materiality. 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 the defense. *United States v. Maniktala*, 934 F.2d 25, 28 (2d Cir. 1991); *United States v.*

*McGuinness*, 764 F.Supp. 888, 894 (S.D.N.Y.1991). To satisfy this burden, the defendant "must offer more than the conclusory allegation that the requested evidence is 'material.'" *United States v. Ashley*, 905 F.Supp. 1146, 1168 (E.D.N.Y.1995) (citing *McGuinness*, 764 F.Supp. at 895). Similarly, "basing discovery requests on nothing more than mere conjecture" is a "non-starter." *United States v. Persico*, 447 F. Supp. 2d 213, 217 (E.D.N.Y. 2006) (rejecting discovery request for "long list of items," where "[t]he theme underlying these requests is that only Defendants, upon review of the requested material, will be able to discern whether or not impeachment or exculpatory information is embedded therein," adding: "[T]he criminal pretrial discovery process does not work that way.").

The Government has explained herein and in the accompanying Tarbell Declaration how the FBI was able to locate the SR Server; and it has already explained at length in the Complaint filed in this matter how Ulbricht was identified as "DPR." There is therefore no basis – especially at this late juncture, six months after discovery was originally produced – for Ulbricht to go on a "blind and broad fishing expedition" for proof of some darker, alternative storyline, somehow involving violations of his Fourth Amendment rights, when there isn't a shred of evidence that any such violations actually happened. *United States v. Larranga Lopez*, 05 Cr. 655 (SLT), 2006 WL 1307963, at *7-*8 (E.D.N.Y. May 11, 2006) (Rule 16 "does not entitle a criminal defendant to a 'broad and blind fishing expedition among [items] possessed by the Government on the chance that something impeaching might turn up'" (quoting *Jencks v. United States*, 353 U.S. 657, 667 (1957) (quoting *Gordon v. United States*, 344 U.S. 414, 419 (1953))); *see also United States v. Wilson*, 571 F. Supp. 1422, 1424 (S.D.N.Y. 1983) (rejecting discovery motion where its "wide-ranging scope suggests that the defendant is not seeking information to which he is entitled under the discovery rules to enable him to defend against the current charge,

but that he is engaged upon a fishing expedition which, if permitted, would in effect require the government to disgorge material contained in its internal investigatory files").[10]

The Government has already made extensive disclosures to Ulbricht of materials properly subject to disclosure under Rule 16. In doing so, the Government has made clear that it is aware of its continuing obligations to produce any exculpatory evidence in its possession, or any further material evidence within the parameters of Rule 16. There is no reason to doubt that the Government has acted in good faith. Accordingly, Ulbricht's discovery requests should be denied. *See United States v. Savarese*, 01 Cr. 1121 (AGS), 2002 WL 265153, at *2 (S.D.N.Y. Feb. 22, 2002) ("To the extent [defendant] seeks more specific types of documents, the materiality of which he can articulate in more than a conclusory fashion, he may make a further

[10] Ulbricht's discovery requests are improper for other reasons as well. For one thing, they are posed in the form of interrogatories, which are out of place in the criminal context. *See United States v. Conder*, 423 F.2d 904, 910 (6th Cir. 1970) ("By its very terms Rule 16[] is limited to inspection and copying of tangible objects. Clearly therefore, the interrogatories filed by the defendants here were not an appropriate mode of discovery . . . ."); *United States v. Cameron*, 672 F.Supp.2d 133, 137 (D. Me. 2009) (rejecting criminal discovery demands that "sound more like civil interrogatories under civil Rule 33 than document requests under Rule 16(a)(1)(E)"); *United States v. Schluter*, 19 F.R.D. 415, 416 (S.D.N.Y. 1956) ("There is no counterpart in the Rules of Criminal Procedure providing for . . . interrogatories such as are permitted under . . . the Rules of Civil Procedure."). Moreover, even to the extent Ulbricht's discovery requests could be construed as seeking documents, the documents that would be at issue – to the extent they existed – would consist largely or entirely of internal reports or other documents generated by agents or attorneys during the investigation, which are not subject to discovery under Rule 16. *See* Fed. R. Crim. P. 16(a)(2) (Rule 16 "does not authorize the discovery or inspection of reports, memoranda, or other internal government documents made by an attorney for the government or other government agent in connection with investigating or prosecuting the case"); *see also, e.g.*, *United States v. Batista*, 06 Cr. 265, 2009 WL 910357, at *10 (E.D.N.Y. Mar. 31, 2009) (denying defendant's request for "a variety of government and reports and records" sought in effort to collect evidence for suppression motion, holding that Rule 16(a)(2) "expressly prohibits such disclosures"); *see generally United States v. Armstrong*, 517 U.S. 456, 463 (1996) ("[U]nder Rule 16(a)(2), [a defendant] may not examine Government work product in connection with his case."); *United States v. Rufolo*, 89 Cr. 938 (KMW), 1990 WL 29425, at *1 (S.D.N.Y. Mar. 13, 1990) (holding Rule 16(a)(2) to bar disclosure of investigative, agent, and surveillance reports prepared by federal agents).

request. Otherwise, the Court must, as always, depend upon the Government's good faith in complying with its obligations under Rule 16.").

**POINT III:**
**ULBRICHT'S REQUEST FOR A BILL OF PARTICULARS SHOULD BE DENIED**

Beyond seeking wide-ranging discovery, Ulbricht also requests an extensive bill of particulars, arguing that unless he is provided with "particularization and enumeration of the specific transactions in the Indictment" and "the manner of, contents of, and parties involved in, the communications alleged. . . his ability to prepare a defense will be irreparably impaired. (Br. 66). The request is meritless and should be denied. Ulbricht has been provided with ample information through the Indictment and the highly detailed Complaint filed against him, as well as through the Government's extensive production of discovery, the most relevant portions of which the Government has already segregated and highlighted for the defense. These materials go well beyond what is necessary to give Ulbricht meaningful notice of the charges against him, obviating any need for a bill of particulars.

The only proper purpose of a bill of particulars is to provide sufficient information about the nature of the charge to enable a defendant to prepare for trial, to avoid unfair surprise, and to have protection against a second prosecution for the same offense. *See* Fed. R. Crim. P. 7(f); *United States* v. *Torres*, 901 F.2d 205, 234 (2d Cir. 1990), *abrogated on other grounds, United States* v. *Marcus*, 628 F.3d 36 (2d Cir. 2010); *United States* v. *Bortnovsky*, 820 F.2d 572, 574 (2d Cir. 1987). As this Court has recently emphasized, "[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. Mostafa*, 965 F. Supp. 2d 451, 465 (S.D.N.Y. 2013) (quoting *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))). Moreover, even where the indictment describes the charges in broad strokes, if detailed information about the offenses is provided through discovery or some other means, a bill of particulars is not necessary. *See Bortnovsky*, 820 F.2d at 574; *see also Walsh*, 194 F.3d at 47 (affirming denial of request for bill of particulars where Government adequately informed defendant of the nature of the charges through discovery); *Torres*, 901 F.2d at 234 (affirming denial of request for bill of particulars based on indictment and evidentiary detail from discovery); *United States v. Panza*, 750 F.2d 1141, 1148 (2d Cir. 1984) (affirming denial of request for bill of particulars based on indictment and pretrial discovery in a case that involved 150 separate fraud claims because counsel "was furnished with all information needed to prepare for trial[]").

A bill of particulars is not appropriate where it is sought merely to obtain evidentiary detail that may be useful to the defendant but is not necessary to apprise him of the charges. *See Torres*, 901 F.2d at 234. "A bill of particulars is not a general investigative tool, a discovery device or a means to compel the government to disclose evidence or witnesses to be offered prior to trial." *United States* v. *Gibson*, 175 F. Supp. 2d 532, 537 (S.D.N.Y. 2001) (citation omitted). The Government is not required to "particularize all of its evidence," *United States v. Cephas*, 937 F.2d 816, 823 (2d Cir. 1991), disclose the precise manner in which the crimes charged in the indictment were committed, *see Torres*, 901 F.2d at 233-34, or preview its trial evidence or legal theory, *see United States* v. *Muyet*, 945 F. Supp. 586, 599 (S.D.N.Y. 1996); *United States* v. *Taylor*, 707 F. Supp. 696, 699 (S.D.N.Y. 1989). The ultimate test is, again, whether the information sought in a bill of particulars is necessary to give notice of the charges against the defendant, not whether it would be helpful to him. *See United States* v. *Trippe*, 171 F. Supp. 2d

230, 240 (S.D.N.Y. 2001); *United States* v. *Conley*, No. 00 Cr. 816, 2002 WL 252766, at *4 (S.D.N.Y. Feb. 21, 2002).

Applying these principles, courts routinely deny motions for bills of particulars that are, at bottom, demands for additional details of the manner in which the offense was committed. *See United States* v. *Mitloff*, 165 F. Supp. 2d 558, 569 (S.D.N.Y. 2001). Courts also routinely deny demands for bills of particulars setting forth the identities of co-conspirators. *Trippe*, 171 F. Supp. 2d at 240; *see also United States* v. *Bin Laden*, 92 F. Supp. 2d 225, 242 (S.D.N.Y. 2000) ("[R]equests . . . for particulars as to when, where, how, and with whom each individual defendant joined an alleged conspiracy have 'almost uniformly been denied.'") (citation omitted); *Torres*, 901 F.2d at 233-34 (demands for "whens" and "wheres" and "by whoms" within charged conspiracy are improper attempts at general pre-trial discovery).

Here, a bill of particulars is unwarranted because Ulbricht has already been provided with a wealth of information about the nature of the charges in this case, far beyond what is included in the Indictment itself.[11] First, the 33-page Complaint provides Ulbricht with a crystal-clear picture of the basis for the charges he is facing. The Complaint details, among other things: how the Silk Road website was designed to provide anonymity to users engaging in unlawful activity; what types of illegal goods and services were sold on the website; how the site's Bitcoin-based payment system operated to conceal ownership of the criminal proceeds generated by the site; what volume of illegal transactions occurred over the Silk Road; how Ulbricht was identified as

[11] Tellingly, Ulbricht's motion dwells almost exclusively on the allegations in the Indictment and makes no reference to information disclosed in the Complaint and the Government's production of discovery. Yet both are acceptable forms through which information about the charges can be provided to the defense. *See, e.g.*, *United States v. Morgan*, 690 F. Supp. 2d 274, 284 (S.D.N.Y. 2010) (no bill of particulars required where information needed is provided "in some acceptable alternate form, such as discovery or a criminal Complaint" (internal quotation marks omitted)).

the owner and operator of the Silk Road; what Ulbricht did in that role, including controlling the underlying servers and computer code, managing the administrative staff, deciding what could be sold on the site, and collecting the commissions from Silk Road sales; and how Ulbricht was willing to use violence to protect his interests in the illegal marketplace.[12] The Complaint thus provides Ulbricht with more than adequate notice of the charges against him to prepare a defense, and on this basis alone a bill of particulars is unnecessary. *See United States* v. *Cosme*, No. 13 Cr. 43 (HB), 2014 WL 1584026, at *5 (S.D.N.Y. Apr. 21, 2014) (denying defendant's request for a bill of particulars, noting that "the Government has provided a detailed Complaint in addition to the Indictment; the Defendant is not entitled to more"); *United States* v. *Romain*, No. 13 Cr. 724 (RWS), 2014 WL 1410251, at *2 (S.D.N.Y. Apr. 11, 2014) (denying motion for bill of particulars based on detailed complaint); *United States* v. *Thompson*, No. 13 Cr. 378 (AJN), 2013 WL 6246489, at *8 (S.D.N.Y. Dec. 3, 2013) (same).

Moreover, the Government has produced extensive discovery in this case, sufficient to answer nearly every request included in Ulbricht's proposed bill of particulars. *See, e.g.*, *United States* v. *Chen*, 378 F.3d 151, 163 (2d Cir. 2004) (upholding denial of bill of particulars where "extensive discovery furnished defendants with significant insight into the government's case").[13] For example, as to Ulbricht's request for particulars concerning the transactions

[12] The Government also filed an 11-page, single-spaced opposition to Ulbricht's motion for bail during pre-indictment proceedings, which provided even more details along these lines.

[13] The only aspect of Ulbricht's requests for bill of particulars not already answered in the discovery is Ulbricht's request for the true names of Silk Road users, which are largely unknown to the Government. To the extent certain true names are known to the Government, some of those names have already been publicly released in other indicted cases, *see, e.g.*, *United States v. Andrew Michael Jones, et al.*, 13 Cr. 950 (TPG) (prosecution of three Silk Road support staff alleged to have worked under Ulbricht). Any remaining known true names belong to subjects of ongoing criminal investigations, and hence their disclosure is not required in the absence of a specific showing that they are necessary to the defense. *See United States v. Chalmers*, 410 F.

executed on Silk Road, the Government has produced a forensic copy of the Silk Road marketplace server, which contains a database detailing every single transaction that occurred on the Silk Road website of which the Government has a record. For each transaction, the database includes specific information regarding the date of the transaction, the product that was sold (for example, the type of illegal drug or other contraband), the unique Silk Road usernames of the buyer and seller, the sales price, and the commission collected by Silk Road. In addition, for the convenience of the defense, the Government has separately provided a summary spreadsheet compiling data from this database, which reflects total sales on Silk Road, broken down by drug type or other category describing the product or service sold. The Government has also provided extensive detail regarding undercover drug purchases made on Silk Road, including buy reports and lab tests, as well as specific information regarding numerous customs seizures of narcotics linked to the Silk Road website.

Similarly, as to Ulbricht's requests for particulars concerning his alleged role on Silk Road and relationships with alleged co-conspirators, the Government has made extensive discovery concerning the actions and communications of "Dread Pirate Roberts" on Silk Road, as well as evidence tying Ulbricht to this user identity. For example, the copy of the Silk Road marketplace server produced to Ulbricht contains a database of all private message communications between Silk Road users, which includes conversations using the Silk Road

---

Supp. 2d 278, 286-87 (S.D.N.Y. 2006). Particularly given that Ulbricht is charged in the District of Maryland with attempted murder of a witness, *see* Superseding Indictment, 13 Cr. 222 (D. Md. Oct.1, 2013), such disclosure would be improper. *See, e.g., United States* v. *Taylor*, 10 Cr. 268 (DLI), 2014 WL 1653194, at *13 (E.D.N.Y. Apr. 24, 2014) ("[I]dentification [of alleged co-conspirators] is generally inappropriate in cases where the defendant is charged with extreme acts of violence in order to protect the government's investigation and the safety of unindicted co-conspirators." (citations and internal quotation marks omitted); *United States* v. *Santiago*, 174 F. Supp. 2d 16, 39 (S.D.N.Y. 2001) (rejecting request to disclose identities of co-conspirators given allegations of violence pending against the defendant).

username "Dread Pirate Roberts." Again, for the convenience of the defense, the Government separately produced a set of all of "Dread Pirate Roberts'" private messages in a sortable, searchable spreadsheet. These communications specifically include communications between Ulbricht and his support staff, Silk Road vendors, and other of his co-conspirators, such as the user "redandwhite," whom Ulbricht is alleged to have solicited to murder five people. Other information about co-conspirators can be found on Ulbricht's computer, an image of which was produced to him in discovery, which includes, for example, a "to do" list containing a list of employees (identified by their Silk Road usernames) whom the list indicated needed to be paid on a weekly basis.

There is no basis for Ulbricht's protests that the Government's discovery production leaves him to search for evidence of his criminal conduct "unguided" within "mountains of documents." (Br. 69 (quoting *Bortnovsky*, *supra*, at 575). Ulbricht's reliance on *Bortnovsky* is misplaced. In that case, the defendants were charged with fabricating burglaries as part of an insurance fraud scheme. The indictment did not specify the dates of these burglaries or the documents used to falsify them; and the Second Circuit found that the Government's discovery production was insufficient to give notice of these allegations, since it included evidence of numerous actual burglaries along with fake burglaries (and did not distinguish between the two) and included among its 4,000 pages only three fraudulent documents (which were not identified as such). *Bortnovsky*, 820 F.2d at 574-75.

No comparable situation exists here. This is not a case where the defendant's criminal conduct consists of a handful of discrete acts, or where the evidence against him consists of a few needles within a haystack of discovery materials of otherwise unclear relevance. Ulbricht is charged with overseeing an entire criminal enterprise over a two-and-a-half-year period. *All* of

the discovery produced relating to Silk Road is relevant to that criminal enterprise; and he has not been left "unguided" as to what to look for in that discovery. Again, if Ulbricht wants to look for evidence of the illegal commerce on Silk Road, he knows where to look: principally, the transactional database, where illegal transactions are generally evident on their face based on the description of the product being sold. Similarly, if Ulbricht wants to look for evidence of his role on the site, he knows where to look: the communications of "Dread Pirate Roberts" and the various sources of evidence linking him to that identity, which were produced to the defense in an accessible, well-organized format. There is simply no mystery here concerning the nature of the charges Ulbricht is facing or the nature of the evidence supporting those charges. *See, e.g.*, *United States* v. *Kazarian*, No. 10 Cr. 895 (PGG), 2012 WL 1810214, at *25 (S.D.N.Y. May 18, 2012) (distinguishing *Bortnosky* where voluminous discovery production, including supplemental summary charts, provided information sought by bill of particulars); *United States* v. *Kaplan*, No. 02 Cr. 883 (DAB), 2003 WL 22880914, at *15 (S.D.N.Y. Dec. 5, 2003) (distinguishing *Bortnovsky* where the Government provided discovery "organized into case files, . . . for each of which the Government has provided a basis for its connection to the charged against the Defendant"). Accordingly, Ulbricht's request for a bill of particulars should be denied.

**POINT IV:**
**ULBRICHT'S REQUESTS TO STRIKE SURPLUSAGE SHOULD BE DENIED**

Finally, Ulbricht moves to strike certain language in the Indictment as "surplusage." First, Ulbricht seeks to strike allegations that Ulbricht solicited the murder-for-hire of several individuals, on the ground that the language is irrelevant and prejudicial. (Br. 83-86). Second, Ulbricht seeks to strike language in the computer hacking conspiracy charged against him, characterizing "password stealers, keyloggers, and remote access tools" as "malicious software

designed for computer hacking," on the ground, again, that the language is irrelevant and prejudicial. (Br. 86-76). Finally, Ulbricht seeks to strike such phrases in the Indictment as "others known and unknown," "among others," and "elsewhere," on the ground that this language impermissibly expands the charges against Ulbricht. (Br. 87-89). As set forth below, none of the challenged language is "surplusage," and the requests to strike should be denied.

**A. The Indictment's Murder-for-Hire Allegations Are Relevant to Ulbricht's Criminal State of Mind and Should Not Be Stricken**

"'Motions to strike surplusage from an indictment will be granted only where the challenged allegations are not relevant to the crime charged and are inflammatory and prejudicial.'" *United States* v. *Mulder*, 273 F.3d 91, 99-100 (2d Cir. 2001) (quoting *United States* v. *Scarpa*, 913 F.2d 993, 1013 (2d Cir. 1990)). Therefore, "[i]t has long been the policy of courts within the Southern District to refrain from tampering with indictments." *United States* v. *Tomero*, 496 F. Supp. 2d 253, 255 (S.D.N.Y. 2007) (quotation marks omitted) (citing *United States* v. *Bin Laden*, 91 F. Supp. 2d 600, 601 (S.D.N.Y. 2000)); *accord United States* v. *Jimenez*, 824 F. Supp. 351, 369 (S.D.N.Y.1993). "'If evidence of the allegation is admissible and relevant to the charge, then regardless of how prejudicial the language is, it may not be stricken.'" *Scarpa*, 913 F.2d at 1013 (quoting *United States* v. *DePalma*, 461 F. Supp. 778, 797 (S.D.N.Y. 1978)).

Here, as the Indictment itself indicates, the murder-for-hire allegations reflect Ulbricht's intent "to protect his criminal enterprise and the illegal proceeds it generated." (Indictment ¶ 4.) They are therefore relevant to showing that he operated Silk Road with a criminal state of mind and full knowledge that what he was doing was illegal, and they are properly included as overt act allegations in the Indictment. The use of violence and threatened violence to protect one's drug empire are relevant to proving the intentional operation of a narcotics conspiracy, and such

conduct may be alleged as overt acts in furtherance of such a charge. *See United States v. Miller*, 116 F.3d 641, 682 (2d Cir. 1997) (upholding admission of evidence in narcotics conspiracy trial of uncharged murders of "persons who were considered to be threats" to narcotics enterprise, finding that the evidence was "relevant to show the existence and nature of the enterprise and the conspiracy," and that their probative value outweighed potential for unfair prejudice); *see also United States v. Estrada*, 320 F.3d 173, 183 (2d Cir. 2003) (noting that "the use of violence to secure the organization's drug turf [and] carrying and using firearms to enforce its control over the drug market" were properly alleged as overt acts of narcotics conspiracy).

Indeed, Ulbricht has already signaled that the crux of his defense in this case is likely to be that, in operating Silk Road, he merely acted as a website administrator and cannot be considered a co-conspirator in any illegal conduct by the website's users. *See United States v. Ulbricht*, __ F. Supp. 2d __, 2014 WL 3362059, at *14 (S.D.N.Y. July 9, 2014) (discussing Ulbricht's argument in his motion to dismiss the Indictment that he was, at most, a "landlord" of the drug dealers operating on the site). As the Court recognized in ruling on Ulbricht's motion to dismiss, the murder-for-hire allegations are directly relevant to rebutting that defense and establishing that Ulbricht intentionally headed a drug trafficking enterprise in running Silk Road:

> There is no legal reason why one who designs, launches, and operates a website or any facility for the specific purpose of facilitating narcotics transactions that he knows will occur, and acts as the rule-maker of the site—determining the terms and conditions pursuant to which the sellers are allowed to sell and the buyers are allowed to buy, *taking disciplinary actions to protect that enterprise (allegedly including murder-for-hire on more than one occasion)*—could not be found to occupy [a supervisory position in a narcotics enterprise]. In this regard, the allegations amount to Ulbricht acting as a sort of "godfather"—determining the territory, the actions which may be undertaken, and the commissions he will retain; *disciplining others to stay in line*; and generally casting himself as a leader—and not a service provider.

*Ulbricht*, 2014 WL 3362059, at *17 (emphasis added). Accordingly, the murders-for-hire alleged in the Indictment are not only relevant to the crimes charged but are likely to be an important part of the Government's proof of criminal intent at trial. There is no basis for the allegations to be stricken as "surplusage."

**B. The Indictment's Reference to "Malicious Software" Is Relevant to the Computer Hacking Charge and Should Not Be Stricken**

Ulbricht moves to strike language in the computer hacking conspiracy count of the Indictment characterizing "password stealers, keyloggers, and remote access tools" as "malicious software designed for computer hacking" – a characterization which he claims to be unduly prejudicial because such tools have "numerous legitimate purposes." (Br. 86). According to Ulbricht, the inclusion of this language in the Indictment relieves the Government of its burden of proving that the users buying such software on the site intended to use it for illegitimate purposes. (Br. 87). This argument is meritless.

The "malicious" nature of the computer software sold on the Silk Road website is plainly relevant to the computer hacking conspiracy count charged in the Indictment. Indeed, it is simply part of the conduct charged: Ulbricht is alleged to have conspired to aid and abet computer hackers by conspiring to sell them software *designed* for use in computer hacking – *i.e.*, "malicious software." The use of such shorthand in an indictment is unobjectionable. *See, e.g.*, *United States v. Ruskjer*, 09 Cr. 249 (HG), 2011 WL 3841854, at *4 (D. Hi. Aug. 29, 2011) (refusing to strike the term "Ponzi scheme" from fraud indictment, finding it to be commonly used shorthand "that simply refers to a particular form of fraud, the very form that [defendant] is alleged to have engaged in"); *United States v. Giovanelli*, 747 F. Supp. 875, 889 (S.D.N.Y. 1990) (refusing to strike references to "Genovese Family," given that "such references form part of the Government's theory of the case").

Ulbricht will be free at trial, of course, to argue that the software sold on Silk Road also had legitimate uses, and that he was unaware of its actual intended use by those who bought it. These are disputes for the jury to resolve. At this stage, the language in the Indictment merely constitutes part of a factual allegation included in the computer hacking offense. Because it is relevant to that offense, it should not be stricken as "surplusage."

### C. The Indictment's Use of Catchall Language Is Unobjectionable and Does Not Impermissibly Expand the Scope of the Charges

Like many indictments, the Indictment includes at various points such catchall phrases as "the defendant, and others known and unknown," "in the Southern District of New York and elsewhere," and "among others." Ulbricht moves to strike these phrases, contending that they "impermissibly expand the charges against Mr. Ulbricht beyond the specific charges returned by the grand jury." (Br. 88). The argument is meritless.

First, with respect to allegations that Ulbricht acted with "others known and known," Ulbricht is charged with conspiring with others to commit certain of the offenses charged. The existence of other co-conspirators, even if unindicted and unnamed, is obviously relevant to those charges, and does not impermissibly expand their scope. *United States v. Kassir*, No. 04 Cr. 356 (JFK), 2009 WL 995139, at*4 (S.D.N.Y. Aug. 30, 2013) (rejecting motion to strike such language).

Second, as to the phrase "in the Southern District of New York and elsewhere," the commission of a crime "can span several districts," and in such circumstances "venue properly lies in 'any district in which such offense was begun, continued, or completed.'" *United States* v. *Rommy*, 506 F.3d 108, 119 (2d Cir. 2007). The references in the Indictment to "the Southern District of New York and elsewhere" simply make plain that the Government is charging crimes

that span multiple districts, including the Southern District of New York – as the Government is entitled to do. *See Kassir*, 2009 WL 995139, at *4.

Finally, as to the phrase "among others," the Indictment uses the phrase in alleging that the controlled substances involved in the charged narcotics offenses included – among others – certain quantities of certain controlled substances that qualify for the enhanced sentencing provisions of Title 21, United States Code, Section 841(b)(1)(A), namely, heroin, cocaine, LSD, and methamphetamine. The language is entirely proper, as it clarifies that these particular controlled substances – which must be specified in the Indictment given that they are the basis for enhanced maximum penalties[14] – were not the *only* controlled substances involved in the offense. Indeed, the Government will prove at trial that the defendant conspired to distribute a wide variety of additional controlled substances on the Silk Road website. Such additional controlled substances need not be alleged in the indictment itself, given that enhanced penalties are not sought based on these other types of controlled substances, and knowledge of the *type* of controlled substance involved in a narcotics trafficking offense is not otherwise an essential element of the offense that must be alleged in an indictment. *See United States v. Abdulle*, 564 F.3d 119, 126 (2d Cir. 2009); *United States* v. *Morales*, 577 F.2d 769, 776 (2d Cir.1978). Accordingly, the Indictment's generic reference to other types of controlled substances is relevant to the crimes charged, does not expand their scope, and is not "surplusage."[15]

[14] *United States v. Thomas*, 274 F.3d 655, 660 (2d Cir. 2001) ("[I]f the type and quantity of drugs involved in a charged crime may be used to impose a sentence above the statutory maximum for an indetermine quantity of drugs, then the type and quantity of drugs is an element of the offense that must be charged in the indictment and submitted to the jury.").

[15] The defendant has been provided with detailed evidence in discovery detailing each type of controlled substance that was distributed on the Silk Road website, including, among other things, a summary chart compiling transactional data by category of controlled substance.

## CONCLUSION

For the foregoing reasons, Ulbricht's motion should be denied in its entirety.

Dated: September 5, 2014
New York, New York

Respectfully submitted,

PREET BHARARA
United States Attorney for the
Southern District of New York

By: /s/ Serrin Turner
SERRIN TURNER
TIMOTHY HOWARD
Assistant United States Attorneys