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. | : | |

**GOVERNMENT RESPONSE TO**
**THE DECLARATION OF JOSHUA HOROWITZ**

At the Court's invitation, the Government submits this response to the Declaration of Joshua Horowitz (the "Horowitz Declaration"), which takes issue with the Declaration of Christopher Tarbell ("Tarbell Declaration") concerning how the FBI located the server hosting the Silk Road website (the "SR Server"). While the Government believes the Horowitz Declaration is factually and analytically flawed in a number of respects, the Court need not resolve these disputes in order to rule on Ulbricht's suppression motion. The declaration does not come close to alleging facts that, if proven, would establish a violation of Ulbricht's Fourth Amendment rights. Accordingly, Ulbricht has failed to meet his *prima facie* burden and his motion should therefore be denied without a hearing.

DISCUSSION

"A party seeking to raise a factual issue to be determined at an evidentiary hearing must submit admissible evidence which, if credited, would make out a *prima facie* case on the issue." *United States v. Ahmad*, 992 F. Supp. 682, 685 (S.D.N.Y. 1998) (citing *United States v. Gillette*,

383 F.2d 843, 848 (2d Cir. 1967)). Accordingly, "[a] defendant seeking the suppression of evidence is not automatically entitled to an evidentiary hearing on his claim; rather, the defendant must first 'state sufficient facts which, if proven, would [require] the granting of the relief requested.'" *United States v. Seijo*, No. 02 Cr. 1415, 2003 WL 21035245, at *4 (S.D.N.Y. May 7, 2003) (quoting *United States v. Kornblau*, 586 F. Supp. 614, 621 (S.D.N.Y. 1984) (quoting *United States v. Culotta*, 413 F.2d 1343, 1345 (2d Cir. 1969))); *see also United States v. Navas*, 640 F. Supp. 2d 256, 264 (S.D.N.Y. 2009), *rev'd in part on other grounds*, 597 F.3d 492 (2010) (noting that a defendant seeking to suppress evidence "must present a *prima facie* case showing a Fourth Amendment violation" (internal quotation marks omitted)); *United States v. Aparo*, 221 F. Supp. 2d 359, 369 (E.D.N.Y.2002) (denying motion to suppress given that defendant had "not submitted an affidavit alleging facts which would require . . . suppression . . . if those facts were proved at a hearing"). "It is well-settled that such showing must be made by an affidavit of someone with personal knowledge of the underlying facts." *United States v. Shaw*, 260 F. Supp. 2d 567, 570 (E.D.N.Y. 2003); *see also United States v. Dewar*, 489 F. Supp. 2d 351, 359 (S.D.N.Y. 2007) (same).

Hence, the burden is on Ulbricht to allege facts that, if proven, would establish a violation of his Fourth Amendment rights. The Horowitz Declaration manifestly fails to satisfy that burden. As a threshold matter, the declaration does not establish that Ulbricht had a reasonable expectation of privacy in the SR Server, as required for him to have standing to move for its suppression in the first place. Indeed, a declaration from a member of Ulbricht's legal team such as Mr. Horowitz would be insufficient for this purpose anyway. To establish standing, a defendant must submit an "'affidavit from someone with *personal knowledge* demonstrating sufficient facts to show that he had a legally cognizable privacy interest in the searched premises

at the time of the search.'" *United States v. Serrano*, No. 13 Cr. 58 (KBF), 2014 WL 2696569, at *4 (Jun. 10, 2014) (quoting *United States v. Ruggiero*, 824 F. Supp. 379, 391 (S.D.N.Y. 1993)) (emphasis added). Ulbricht's counsel would not have any personal knowledge of Ulbricht's privacy interest in the SR Server; presumably, only Ulbricht would. *See, e.g.*, *Ahmad*, 992 F. Supp. at 685 (affidavit of defense counsel insufficient to warrant hearing).

Ulbricht's assertion that he is not required to submit such an affidavit and that the issue of standing "must . . . be resolved through an evidentiary hearing," (Reply Br. 18), is flatly wrong. Again, to merit a hearing, a defendant must first allege facts that, *if proven at a hearing*, would establish a violation of his personal Fourth Amendment rights – including facts sufficient to show the defendant had a protected privacy interest in the property searched. Without competently asserting such an interest, a defendant has no standing to bring a suppression motion at all, let alone demand a hearing on the motion. *See Serrano*, 2014 WL 2696569, at *4 ("[T]o bring a motion to suppress evidence as violative of the Fourth Amendment, a defendant must establish that he has the requisite personal interest in the thing or place searched; put another way, he must establish that he has standing to bring the motion."); *United States v. Polanco*, 37 F. Supp. 2d 262, 264 (S.D.N.Y. 1999) ("In seeking to vindicate rights under the Fourth or Fifth Amendments, a defendant is required to submit a sworn affidavit in order to obtain a suppression hearing.").[1]

Because Ulbricht has not submitted any affidavit alleging that he had any possessory interest in the SR Server – let alone one that would give him a reasonable expectation of privacy

[1] *United States v. Pena*, 961. F.2d 333 (2d Cir. 1992), cited by Ulbricht (Reply Br. 18-19), is not to the contrary. The opinion makes clear that a "defendant seeking suppression bears the burden" of establishing, through a personal affidavit, a "Fourth Amendment privacy interest" in the property searched – whether this issue is framed as one of "standing" or otherwise. *Id.* at 336-37.

– his motion should be denied. *See United States v. Watson*, 404 F.3d 163, 167 (2d Cir. 2005) (upholding denial of suppression motion without a hearing where defendant failed to proffer affidavit alleging possessory interest in premises searched); *Serrano*, 2014 WL 2696569, at *7 (denying motion to suppress phone data without a hearing where defendant had "not proffered an affidavit that he has a privacy interest in that phone"); *United States v. Parilla*, No. 13 Cr. 360 (AJN), 2014 WL 1621487, at *5 (S.D.N.Y. Apr. 22, 2014) (denying motion to suppress fruits of vehicle search without a hearing where defendant had failed to show that he possessed "any property rights in the vehicle").[2]

Even if Ulbricht were to demonstrate that he has standing, which he plainly has failed to do, the Horowitz Declaration still would not warrant a hearing because it fails to allege facts that, if proven, would establish a violation of Ulbricht's Fourth Amendment rights. The Horowitz Declaration nowhere alleges that the SR Server was either located or searched in a manner that violated the Fourth Amendment. It merely critiques certain aspects of the Tarbell Declaration concerning how the SR Server was located. The Horowitz Declaration fails to allege *any* alternative explanation of how the SR Server was located that, if proven, would establish that Ulbricht's Fourth Amendment rights were somehow violated.[3] Thus, whatever quarrel Mr.

[2] Ulbricht has also failed to address the fact that the terms of service of the webhosting provider from which the SR Server was leased prohibited the use of its systems for illegal purposes and warned that its systems were subject to monitoring for unauthorized use. Thus, even if Ulbricht were to establish that he had a possessory interest in the server, he still would not have had a legitimate expectation of privacy in it, given the patently illegal enterprise he was hosting on the server in clear violation of the provider's terms. (Gov't Mem. 12-13). For this reason as well, Ulbricht has failed to meet his burden of establishing a protected privacy interest in the searched property.

[3] The only alternative version of events offered by the Horowitz Declaration is the assertion that when former Agent Tarbell typed the IP address of the SR Server into an ordinary web browser – *after* he had already observed the IP address leaking from the Silk Road website – he would have seen a login page for the "phpmyadmin" interface on the server – a "back-end" part of the

Horowitz has with the Tarbell Declaration is irrelevant in the absence of any competent, affirmative allegations of fact that could supply a basis for suppression if proven at a hearing. *See Parilla*, 2014 WL 1621487, at *5 (denying suppression motion where defendant merely argued that agent affidavit failed to adequately explain the circumstances leading to the seizure of the evidence at issue: "[W]ithout evidence showing that the search violated [defendant's] rights, there is no basis for suppression . . . [and] likewise no basis for [an] evidentiary hearing."); *United States v. Getto*, No. 09 CR 667 (HB), 2010 WL 3467860, at *3 (S.D.N.Y. Aug. 25, 2010) (holding that, where defendant "does not have any significant evidence . . . that would necessitate suppression," he is not entitled to an evidentiary hearing to "explore" whether such evidence in fact exists).

Even Ulbricht's briefs fail to set forth any specific account of how his Fourth Amendment rights were violated by the Government's location and search of the SR Server; instead, Ulbricht offers only speculation. Ulbricht has repeatedly suggested the possibility that the National Security Agency ("NSA") assisted in some way in locating the server and has sought discovery into that possibility. (Def. Br. 30-31; Reply Br. 14 n.9). However, the NSA

---

website – rather than part of the login page for the "front-end" of the Silk Road marketplace. Horowitz Decl. ¶¶ 28-29. Even assuming that were true, however, that would not impact the lawfulness of the initial identification of the IP address. Moreover, the Government would still have had ample reason to ask Icelandic authorities to search the SR Server and, thus, to the extent the Fourth Amendment even applies to that search, it was plainly reasonable. Among other things, the IP address of the server had leaked from the Silk Road website, and pen register data for the server collected by Icelandic authorities reflected a high volume of Tor traffic flowing to the server, consistent with it hosting a Tor hidden service. Indeed, the fact that the SR Server was running "phpmyadmin" would have further corroborated that it was hosting Silk Road, since "phpmyadmin" is used to administer PHP databases – which are commonly used to run online businesses – and Silk Road's reliance on PHP databases was readily observable from the website itself during the time of its operation. *See Watson*, 404 F.3d at 167 (upholding denial of suppression motion without hearing where "defendant failed to show that he could challenge the search under the Fourth Amendment, even assuming we credited the facts asserted in his counsel's affirmation").

did not provide technical support to the FBI of any kind in identifying the IP address of the SR Server, or any other server located in the FBI's investigation – let alone in a manner that somehow violated Ulbricht's Fourth Amendment rights. Not surprisingly, the Government has no evidence of such involvement to produce in discovery, and Ulbricht's conjecture that there was such involvement is not a sufficient basis for a hearing. *See, e.g., United States v. Castellano*, 610 F. Supp. 1359, 1439 (S.D.N.Y. 1985) (evidentiary hearing not required "where a defendant's allegations are general and conclusory or are based upon suspicion or conjecture").

Ulbricht also has suggested the possibility that the SR Server was located through illegally wiretapping his communications. (Def. Reply Br. 20). However, no wiretap of any kind was used in the FBI's investigation – let alone any wiretap intercepting Ulbricht's communications. (Had there been such a wiretap, the Government would have produced any intercepted communications of Ulbricht to the defense pursuant to Federal Rule of Criminal Procedure 16(a)(1)(B).) Indeed, Ulbricht did not even become a suspect in the FBI's investigation until well after the SR Server was searched. Hence, no information collected from or about Ulbricht, through a wiretap or otherwise, was ever used to locate the SR Server.

Finally, Ulbricht attempts to extrapolate from the Tarbell Declaration that the FBI located the SR Server through computer hacking. (Reply Br. 9). Citing the position of the Government in *United States v. Auernheimer*, No. 13-1816 (3d Cir.), Ulbricht argues that the conduct described in the Tarbell Declaration involved "unauthorized access" of the SR Server. The argument is meritless. As an initial matter, Ulbricht misplaces reliance on *Auernheimer*, which involved a defendant who "gained non-public information" from AT&T computers by "*impersonating* unique users who had pre-registered with AT&T, and gaining information that *the users* had provided to AT&T." Government Brief, *United States v. Auernheimer*, No. 13-

1816 (3d. Cir.), *available at* 2013 WL 5427839, at *33 (emphasis in original). The Tarbell Declaration does not describe any such impersonation of Silk Road users to gain access to their information on the SR Server. It describes former Agent Tarbell's close examination of traffic data received from the Silk Road website when he used a part of it that was fully accessible to the public at large – the login interface – and received error messages that were accessible to any user who entered erroneous login information.

In any event, even if the FBI had somehow "hacked" into the SR Server in order to identify its IP address, such an investigative measure would not have run afoul of the Fourth Amendment. Because the SR Server was located outside the United States, the Fourth Amendment would not have required a warrant to search the server, whether for its IP address or otherwise. *See United States v. Vilar*, 729 F.3d 62, 86 (2d Cir. 2013) (Fourth Amendment warrant requirement does not apply extraterritorially); *In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157, 167 (2d Cir. 2008) (same). At most, any search of the SR Server needed only to be "reasonable" – that is, justified by "legitimate governmental interests." *Vilar*, 729 F.3d at 86. Given that the SR Server was hosting a blatantly criminal website, it would have been reasonable for the FBI to "hack" into it in order to search it, as any such "hack" would simply have constituted a search of foreign property known to contain criminal evidence, for which a warrant was not necessary.[4]

[4] Ulbricht appears to argue that, even in the absence of a Fourth Amendment violation, a "hack" of the SR Server would warrant suppression under the Computer Fraud and Abuse Act ("CFAA"), *codified at* 18 U.S.C. § 1030. (Reply Br. 13-14). This argument is misguided in two respects. First, the CFAA contains an express exception for lawfully authorized law enforcement activity, *see* 18 U.S.C. § 1030(f), which would apply here, given that the FBI was pursuing a lawfully authorized criminal investigation and acting in compliance with the Fourth Amendment. Second, the remedy of suppression is not generally available for a mere statutory violation where the statute itself does not provide such a remedy. *See generally United States v.*

## CONCLUSION

In short, Ulbricht has failed to meet his *prima facie* burden of establishing a basis for suppression, and the Horowitz Declaration does nothing to cure this failure. For this reason, and all the other reasons set forth in the Government's opposition brief, his motion should be denied without a hearing.

Dated: October 6, 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

---

*Donovan*, 429 U.S. 413, 432 n. 22 (1977) ("The availability of a suppression remedy for . . . statutory, as opposed to constitutional violations . . . turns on the provisions of [the statute] rather than the judicially fashioned exclusionary rule aimed at deterring violations of Fourth Amendment rights."); *see also United States v. Amanuel*, 615 F.3d 117, 125 (2d Cir. 2010) (no suppression remedy for violations of the Electronic Communications Privacy Act given that statute does not provide for such remedy); *United States v. Deccarett*, 6 F.3d 37, 52 (2d Cir. 1993) (no suppression remedy for violations of Right to Financial Privacy Act given that statute does not provide for such remedy) (citing with approval *United States v. Thompson*, 936 F.2d 1249, 1252 (11th Cir. 1991) (courts should not imply a suppression remedy unless statute specifically refers to exclusionary rule)).