UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

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

DECLARATION OF CHRISTOPHER TARBELL

Pursuant to 28 U.S.C. § 1746, I, Christopher Tarbell, declare the following under penalty of perjury:

Employment, Education, and Training

1. I am currently employed as a Managing Director at FTI Consulting, Inc., in New York, New York, where I conduct cybersecurity investigations.

2. Prior to joining FTI Consulting, I was employed with the Federal Bureau of Investigation ("FBI") from 2005 to 2014. Specifically, from 2005 to 2009, I served as a computer forensic examiner with the FBI's global forensic team, where I engaged in computer forensic investigations and data collections all over the world on matters that included international terrorism, botnets, and crimes against children. In 2009, I joined a cybercrime squad in the FBI's New York Field Office known as "CY-2" as a Special Agent. During my tenure at CY-2, I served as the lead case agent in numerous cybercrime investigations, including the investigation of the Silk Road website.

3. I hold a master's degree in computer science with a concentration in information security from James Madison University. I obtained extensive technical training during my service with the FBI, including being certified by both the FBI and the International Association of Computer Investigative Specialists as a Forensic Computer Examiner. I have also been qualified and have testified as an expert computer forensic witness at two federal criminal trials. I have been regularly called upon to advise and teach cyber investigative techniques to foreign and domestic law enforcement officers.

Location of the Silk Road Server

4. As explained in the complaint filed against defendant Ross Ulbricht (the "Complaint"), the server that hosted the Silk Road website (the "SR Server") operated on the Tor network. The Tor network is a special network of computers on the Internet, known as Tor "nodes," designed to conceal the IP addresses[1] of the computers operating on it – including servers hosting websites on Tor, such as Silk Road, known as "hidden services."

5. In order for the IP address of a computer to be fully hidden on Tor, however, the applications running on the computer must be properly configured for that purpose. Otherwise, the computer's IP address may "leak" through the traffic sent from the computer. *See, e.g.*, Tor Project, Guide on How to Tor-ify Various Applications, https://trac.torproject.org/projects/tor/wiki/doc/TorifyHOWTO ("Tor does not protect all of your computer's Internet traffic when you run it. Tor only protects your applications that are properly configured to send their Internet traffic through Tor."). During the course of the FBI's investigation of the Silk Road website, the

[1] An Internet protocol or "IP" address is a unique numerical identifier assigned to every computer connected to the Internet. Through the use of legal process, a computer's IP address can be used to determine the physical location of the computer.

SR Server was located by myself and another member of the CY-2 squad of the FBI New York Field Office as a result of such a leak.

6. The IP address leak we discovered came from the Silk Road user login interface. As noted in the Complaint, any Internet user could access the Silk Road website using free, publicly available "Tor browser" software. Upon typing in the address of the site (known as a ".onion" address) into the browser, the user would be directed to Silk Road's user login interface, which consisted of a black screen containing a prompt for a username and password, as well as a "CAPTCHA" prompt, requiring the user to type in certain letters and numbers displayed in a distorted manner on the screen, in order to prove that the user was a human and not an automated computer script.[2]

7. In or about early June 2013, another member of CY-2 and I closely examined the traffic data being sent from the Silk Road website when we entered responses to the prompts contained in the Silk Road login interface. This did not involve accessing any administrative area or "back door" of the site. We simply were interacting with the website's user login interface, which was fully accessible to the public, by typing in miscellaneous entries into the username, password, and CAPTCHA fields contained in the interface. When we did so, the website sent back data to the computer we were using – specifically, the Silk Road homepage, when we used valid login credentials for undercover accounts we had on the site, or an error message, when we used any username, password, or CAPTCHA entry that was invalid.

[2] If the user did not have a username and password, the user could create one. The user did not have to be "vouched" in by other members or otherwise meet any restrictions to entry. The site was open to all members of the public.

8. Upon examining the individual packets of data being sent back from the website,[3] we noticed that the headers of some of the packets reflected a certain IP address not associated with any known Tor node[4] as the source of the packets. This IP address (the "Subject IP Address") was the only non-Tor source IP address reflected in the traffic we examined. The Subject IP Address caught our attention because, if a hidden service is properly configured to work on Tor, the source IP address of traffic sent from the hidden service should appear as the IP address of a Tor node, as opposed to the true IP address of the hidden service, which Tor is designed to conceal. When I typed the Subject IP Address into an ordinary (non-Tor) web browser, a part of the Silk Road login screen (the CAPTCHA prompt) appeared. Based on my training and experience, this indicated that the Subject IP Address was the IP address of the SR Server, and that it was "leaking" from the SR Server because the computer code underlying the login interface was not properly configured at the time to work on Tor. [5]

---

[3] All communications on the Internet are broken up into "packets" when they are transmitted from one computer to another; the packets are reassembled when they reach the destination computer. Each packet contains, among other things, "header" information, analogous to the outside of a mailing envelope, which includes the IP addresses of the source and destination computers used to route the packet over the Internet.

[4] The IP addresses of most Tor nodes are publicly listed and updated on a regular basis. *See, e.g.*, http://torstatus.blutmagie.de.

[5] After Ulbricht's arrest, evidence was discovered on his computer reflecting that IP address leaks were a recurring problem for him. In a file containing a log Ulbricht kept of his actions in administering the Silk Road website, there are multiple entries discussing various leaks of IP addresses of servers involved in running the Silk Road website and the steps he took to remedy them. For example, a March 25, 2013 entry states that the server had been "ddosd" – *i.e.*, subjected to a distributed denial of service attack, involving flooding the server with traffic – which, Ulbricht concluded, meant "someone knew the real IP." The entry further notes that it appeared someone had "discovered the IP via a leak" and that Ulbricht "migrated to a new server" as a result. A May 3, 2013 entry similarly states: "Leaked IP of webserver to public and had to redeploy/shred [the server]." Another entry, from May 26, 2013, states that, as a result of changes he made to the Silk Road discussion forum, he "leaked [the] ip [address of the forum server] twice" and had to change servers.

9. Based on publicly available information, I subsequently learned that the Subject IP Address was assigned to a server (the "Subject Server") housed at an overseas data center operated by a foreign company in Iceland (the "Data Center").[6] Accordingly, on June 12, 2013, an official request (the "June 12 Request") was made to Icelandic authorities to: (1) obtain subscriber information associated with the Subject Server; (2) collect routing information for communications sent to and from the Subject Server, including historical routing data from the prior 90 days; and (3) covertly image the contents of the Subject Server. *See* Ex. A (Letter from Assistant U.S. Attorney Serrin Turner to Reykjavik Metropolitan Police dated June 12, 2013).[7]

10. The June 12 Request was subsequently executed by the Reykjavik Metropolitan Police (the "RMP"). The RMP obtained subscriber information for the Subject Server first, which reflected that the server was leased by the Data Center to a non-U.S.-based webhosting

---

[6] Registration information for IP addresses (reflecting contact information for the company or person who controls any given IP address) is publicly available through such sources as the WHOIS database. *See, e.g.*, http://www.whois.net.

[7] Several months earlier, the FBI had developed a lead on a different server at the same Data Center in Iceland ("Server-1"), which resulted in an official request for similar assistance with respect to that server on February 28, 2013. *See* Ex. B. Due to delays in processing the request, Icelandic authorities did not produce traffic data for Server-1 to the FBI until May 2013. *See* Ex. A. By the time the FBI received the Server-1 traffic data, there was little activity on Server-1, indicating that it was no longer hosting a website. (As a result, the FBI did not request that Icelandic authorities proceed with imaging Server-1.) There was still some outbound Tor traffic flowing from Server-1, though, consistent with it being used as a Tor node; yet Server-1 was not included in the public list of Tor nodes, *see supra* n.4. Based on this fact, I believed, by the time of the June 12 Request, that the administrator of Silk Road was using Server-1 as a Tor "bridge" when connecting to the SR Server, as indicated in the June 12 Request. *See* Ex. A, at 1. (A Tor "bridge" is a private Tor node that can be used to access the Tor network, as opposed to using a public Tor node that could be detected on one's Internet traffic. *See* Tor: Bridges, *available at* http://torproject.org/docs/bridges.) To be clear, however, the traffic data obtained for Server-1 did not reflect any connection to, or otherwise lead to the identification of, the Subject IP Address. The Subject IP Address was independently identified solely by the means described above – *i.e.*, by examining the traffic data sent back from the Silk Road website when we interacted with its user login interface.

provider (the "Webhosting Provider"). Based on my training and experience, I believed at the time that the Webhosting Provider, in turn, leased the Subject Server to the administrator of Silk Road. After Ulbricht's arrest, data was subsequently recovered from his computer reflecting that he in fact had leased several servers, including the Subject Server, from the Web Hosting Provider. Notably, the operation of Silk Road on the Subject Server was in violation of the Webhosting Provider's terms of service, which prohibited the illegal use of its systems and warned that its "systems may be monitored for all lawful purposes, including to ensure that use is authorized." *See* Ex.C (archived Terms of Service webpage from July 27, 2013).

11. After obtaining subscriber information for the Subject Server, the RMP next obtained traffic data (not including content) for the Subject Server, which showed a very large volume of Tor traffic flowing to the server. Based on my training and experience, this traffic strongly evidenced that the Subject Server was being used as a Tor hidden service and corroborated the information we already had indicating that the Subject Server was being used to host Silk Road.

12. Given this corroboration, we asked the RMP, which coordinated with the FBI on the timing of the search of the Subject Server, to proceed with covertly imaging the server. After obtaining the necessary court order under Icelandic law, the RMP imaged the Subject Server on July 23, 2013. The FBI was not involved in obtaining that court order or ever given a copy of it. Nor was the FBI present for or otherwise involved in the imaging of the server, other than consulting with the RMP as to when the imaging should be done. At no time did the FBI possess any authority to direct or control the RMP's actions. The RMP decided independently that imaging the Subject Server was feasible and appropriate under Icelandic law and they ultimately decided precisely when and how to do it.

13. The RMP provided a copy of the image of the Subject Server to the FBI on or about July 29, 2013. Forensic examination of the server by CY-2 was conducted immediately thereafter and fully confirmed that the Subject Server was in fact the server hosting the Silk Road website, *i.e.*, that it was in fact the SR Server. The server contained, among other things, databases reflecting Silk Road vendor postings, records of Silk Road sales, private messages between Silk Road users, and other forms of Silk Road user activity. The server also contained the computer code used to operate the website.

14. On September 26, 2013, in anticipation of the arrest of Ulbricht and the takedown of the Silk Road website, which occurred on October 1 and 2, 2013, respectively, a supplemental request was issued to Iceland, asking Icelandic authorities to seize the SR Server at a time to be chosen in consultation with the FBI and to re-image its contents, in order to ensure collection of any data added or modified since the initial imaging of the server in July 2013. *See* Ex. D. The RMP again obtained the necessary judicial process and executed the seizure and re-imaging.[8]

Location of Backup Servers

15. From examining the computer code and other data on the SR Server, I learned of IP addresses of additional servers that appeared to be used in connection with operating the website. (These ancillary servers were unknown to us before reviewing the data from the SR Server.) Based on their IP addresses, some of these servers were determined to be maintained by U.S.-based providers and some by foreign providers. The Government obtained the contents of

[8] This supplemental request asked Icelandic authorities to permit FBI personnel to be present during the takedown and, if necessary, access the SR Server in order to post an online seizure banner in place of the Silk Road website. However, while FBI personnel were present when the server was seized, the seizure and re-imaging of the server were executed solely by the RMP.

the former through search warrants and obtained the contents of the latter through official requests to the corresponding foreign countries.

16. One of the servers discovered in this manner was a server whose IP address was referenced in a computer script on the SR Server, which appeared to be used to back up the contents of the SR Server periodically. The FBI obtained a search warrant for this backup server (the "Primary Backup Server") on September 9, 2013. *See* Exs. E & F.[9]

17. A search of the computer code on the Primary Backup Server revealed the IP address of an additional server that appeared to be used to back up the contents of the Primary Backup Server (the "Secondary Backup Server"). The FBI obtained a search warrant for the Secondary Backup Server on October 1, 2013, which also authorized a successive search of the Primary Backup Server, in order to ensure collection of any added or modified data since the initial search. *See* Ex. G.

Pen Registers Relating to Ulbricht

18. By mid-September 2013, Ulbricht was the FBI's lead suspect as the owner and operator of Silk Road, known on the site as "Dread Pirate Roberts," or "DPR."

19. During the period from September 17 to September 20, 2013, the FBI obtained several judicially authorized pen registers for the purpose of confirming the identity of Ulbricht as "DPR" (the "Pen Registers"). *See* Exs. H through K. The Pen Registers authorized the FBI to collect routing data from the Internet service provider account associated with Ulbricht's residence, the wireless router associated with that account, and certain hardware devices that

[9] The FBI obtained both a search warrant directed to the data center where the server was physically maintained and a search warrant directed to the webhosting provider that leased the server from the data center, from whom Ulbricht subleased it (anonymously) in turn. The contents obtained from both warrants were substantively the same.

were determined to be regularly connecting to the router (based on the results of the former two pen registers). The Pen Registers did not collect the contents of any communications. They collected only routing information, such as the IP addresses being contacted using the account, router, and devices, the ports[10] being accessed, and the MAC addresses[11] of the devices involved.

20. We used the Pen Registers to track when Ulbricht was connected to the Internet and what IP addresses and ports he was connecting to. By monitoring when Ulbricht appeared to be online, and comparing it to the times when "DPR" appeared to be logged in to Silk Road (as reflected by his activity on the Silk Road discussion forum), additional evidence was collected corroborating that Ulbricht was in fact "DPR."

21. The Pen Registers did not collect any GPS data, or any comparable substitute for such data, and were not used to track Ulbricht's location.

Search Warrants Relating to Ulbricht

22. On October 1, 2013, in the morning before Ulbricht's arrest later that day, I 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 laptop computer. *See* Exs. L & M.

23. A week after Ulbricht's arrest, another law enforcement agent involved in the investigation obtained two search warrants from the United States District Court for the Southern

[10] Computers use different "ports" to handle different types of Internet traffic. For example, email traffic is handled on certain ports while website traffic is handled on others. Port information thus reveals what type of traffic is reflected on a pen register, but does not reveal the contents of that traffic.

[11] A media access control address, or "MAC address," is a unique identifier embedded in the hardware of devices with a network interface, which can be used to identify the device on any network the device connects to.

District of New York – one authorizing a search of Ulbricht's Gmail account, and the other authorizing a search of his Facebook account. *See* Exs. N & O.

Conclusion

24. I hereby declare under penalty of perjury that the foregoing is true and correct.

Dated: September 5, 2014
The Hague, Netherlands

Christopher Tarbell