UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

| | | |
|---|---|---|
| UNITED STATES OF AMERICA | : | 14 Cr. 68 (KBF) |
| - against - | : | (Electronically Filed) |
| ROSS ULBRICHT, | : | |
| Defendant. | : | |

**DECLARATION OF JOSHUA J. HOROWITZ**

Joshua J. Horowitz, Esq., pursuant to 28 U.S.C. §1746, hereby declares the following under penalty of perjury:

1. I am an attorney licensed to practice law in New York State, and admitted to practice in the United States District Courts for the Southern and Eastern Districts of New York. My practice is concentrated on criminal defense matters that require expertise in technology and computer software.

2. Along with Joshua L. Dratel, P.C., I represent Ross Ulbricht in the above-captioned matter, and make this statement with regard to technical assertions made in the Government's response to Defendant's omnibus motion.

3. As detailed below, my review of the discovery has led to the following conclusions:

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

(2) the account by former Special Agent Tarbell in his Declaration differs in important respects from the government's June 12, 2013, letter to Icelandic

authorities. For example, that letter (which is Exhibit A to the government's opposition papers) suggests the possibility of an alternative method for the government's identifying and locating the Silk Road Server;

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

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

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

## I. *Qualifications*

4. For the past ten years, I have used a variety of GNU/Linux operating systems and have become extensively familiar with their configuration and operation. My technical knowledge has been acquired through building a variety of computer systems over the course of a lifetime.

5. I have previously been retained for my expertise as a technology lawyer in matters involving organized crime, public corruption, and violations of HIPAA. I have

also been successful in tracing the origins of an anonymous threatening e-mail through the use of pre-action discovery.

6. While in law school, I received training at the Software Freedom Law Center, a non-profit organization providing *pro bono* counsel to Free and Open Source Software developers (FOSS).

7. I have lectured to the New York Criminal Bar Association on issues involving technology in criminal defense practice. I have also lectured at several conferences for software developers on legal issues in software development.

8. I am an active member of the New York State Association of Criminal Defense Lawyers and have co-authored an article on forensic laboratory accreditation for the organization's publication, *Atticus*.

## II. *Description of Materials Reviewed*

9. In preparing this Affidavit, I have reviewed the materials provided to the defense in discovery and the documents filed in connection with this proceeding. The discovery materials included forensic images of the Silk Road web server.[1] According to the government, the earliest image was captured June 6, 2013, and the latest in November 2013. The server images contained web server configuration files, records of traffic on the Silk Road site, MySQL databases, and a number of other file types.

10. The discovery materials provided to defense counsel include three two-terabyte hard drives and several USB thumb drives. Each hard drive contains numbered folders corresponding to item numbers contained in the Government's March 21, 2014,

[1] Each web server forensic image is a snapshot of the entire contents of the server at the exact moment the image was captured.

letter, a copy of which is attached hereto as Exhibit 1. The total volume of discovery is several terabytes of data comprised of several hundred thousand digital files.

## III. *Silk Road Server Configuration*

11. The server images provided in discovery establish that the Silk Road was run on the Ubuntu Server operating system, version 12.04.2. Ubuntu is a widely distributed and freely available Linux-based open-source operating system. The server utilized Nginx to serve its web content, a popular, high-performance web server capable of handling high volumes of traffic. The role of the web server is to deliver web content to the client, *i.e.*, the individual visiting the site.[2]

12. Nginx has the capability to serve more than one website from the same physical hardware server. In order to do so, the server must affirmatively be configured for that purpose. This type of configuration is called virtual hosting. There are two file folders containing virtual host configuration files, "sites-available" and "sites-enabled."

13. The "sites-available" folder contains the configuration files for any of the virtual hosts available on the server. To be activated, the "sites-enabled" folder must contain a link to a configuration file in the "sites-available" folder. Without the existence of that link, the site configuration in the virtual host file is not active.[3]

14. In July 2013, the Silk Road site was split between two different servers, a front-end and back-end server. The front-end is what the user sees and interacts with,

[2] According to the nginx wiki, a number of popular web services such as Netflix, Airbnb, and Zappos utilize Nginx. *See* wiki.nginx.org.

[3] For example, if there are ten virtual host configurations in the "sites-available" folder, but no links to any of them in the "sites-enabled" folder, then there are no live virtual host configurations.

while the back-end is where the "under the hood" operations take place, such as fetching data and entering new data in a database.

15. By default, the Nginx web server maintains two separate logs of activity on the server, an access log and an error log. The access log stores information about requests for information processed by the web server, while the error logs store information about any problems encountered by the web server.

16. A single logged request in the access log looks as follows:

"62.75.246.20 - - [14/Jul/2013:06:55:33 +0000] "GET /orders/cart HTTP/1.0" 200 49072 "http://silkroadvb5piz3r.onion/silkroad/item/0f81d52be7" "Mozilla/5.0 (Windows NT 6.1; rv:17.0) Gecko/20100101 Firefox/17.0"[4]

This snippet provides information about the IP address of the web client accessing the server, what files were accessed, how the web server responded to the user request, and the dates and times of access. From this log and the server configuration files, it is apparent that the server assigned IP address 193.107.86.49 (hereinafter the ".49 server") was configured as the back-end to the Silk Road. The access logs show that the server assigned IP address 65.75.246.20 was constantly requesting data from the .49 server.[5] This is because the server with IP address 65.75.246.20 (hereinafter "the front end server") acted as the front-end to the Silk Road site.

[4] This excerpt of the Nginx access log is located in the first item discovery in the directory/orange21/var/log/nginx. According to law enforcement, this server was assigned IP address 193.107.86.49.

[5] The server assigned IP address 65.75.246.20 was provided as Item 15 in discovery and was imaged in October 2013. *See* Exhibit 1.

## IV. *Former Special Agent Tarbell's Explanation Of Receiving Part of the Silk Road Login Page from a Non-Tor Browser is Implausible*

### A. *The Server Configuration Files Refute Tarbell's Claims*

17. Based on the server configuration files provided by the government, access to market data from a non-Tor IP address would have been precluded.[6]

18. The Government's response to Mr. Ulbricht's omnibus motion filed September 5, 2014, contains a Declaration from former FBI Special Agent Christopher Tarbell, attached hereto as Exhibit 2 (Dkt #57). The Declaration contains a vague explanation of how the IP address of the Silk Road server was initially discovered. For instance, former SA Tarbell asserts that, "[w]hen 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." Tarbell Decl. at ¶ 8. As explained below, based upon the Nginx server configuration files provided in discovery, that was not possible.

#### 1. *Live-ssl Configuration*

19. The "sites-available" directory from Item 1 contains four files: live-ssl, default, phpmyadmin, and test-domain. The "sites-enabled" folder contains two links to the live-ssl and phpmyadmin files. As discussed **ante**, at ¶ 13, this means that at the time this image was captured only the live-ssl and phpmyadmin virtual host site configuration files were active.

---

[6] The guide on "Torifying" various applications cited to in ¶ 5 of the Tarbell Declaration is applicable to client-side configurations, not server-side. The client-side vulnerabilities discussed in the guide apply to end-users attempting to configure various applications on their local machines to connect to the Tor network. For discussion on properly configuring Tor hidden services, *see* https://www.torproject.org/docs/tor-hidden-service.html.en (last accessed September 21, 2014).

20. Based on my experience, I know that Linux-based operating systems (such as Ubuntu, which was used to power the Silk Road Server) record modification times for each file. This is known as a file's "mtime," which shows the age of the data contained in the file. When information is added or deleted from a file, its mtime will be updated by the operating system.[7] The mtime for the live-ssl configuration file provided in Item 1 of discovery is June 7, 2013, and the phpmyadmin configuration is July 6, 2013.[8] *See* mtime for site configuration files from Item 1 of discovery and the contents of the 'sites-enabled' directory, attached hereto as Exhibit 2.

21. In response to defense counsel's September 17, 2014 letter, demanding additional discovery, attached hereto as Exhibit 3, the government provided additional information and discovery by letter dated September 23, 2014, attached hereto as Exhibit 4. The government's September 23, 2014, letter included an excerpt of 19 lines from Nginx access logs, attached hereto as Exhibit 5, supposedly showing law enforcement access to the .49 server from a non-Tor IP address June 11, 2013, between 16:58:36 and 17:00:40. According to the Government, this is the only contemporaneous record of the actions described by the Tarbell Declaration at ¶¶ 7-8.[9]

22. Spanning from May 26, 2013 to October 2, 2013, there were a total of 168,361,443 lines of Nginx access logs provided to defense counsel. Of those, roughly 25,988,136 fit within the early June 2013 timeframe provided in the Tarbell Declaration,

---

[7] *See*, mtime, ctime, and atime, available at http://www.unix.com/tips-and-tutorials/20526-mtime-ctime-atime.html (accessed September 21, 2014).
[8] Since Item 1 is the oldest image provided in discovery the defense does not have site configuration data prior to June 7, 2013.
[9] *See* government September 23, 2014, letter (Ex.4), at 4, which states: "[o]ther than Attachment 1, the Government is not aware of any contemporaneous records of the actions described in paragraphs 7 and 8 of the Tarbell declaration."

¶ 7. Without identification by the Government, it was impossible to pinpoint the 19 lines in the access logs showing the date and time of law enforcement access to the .49 server.

23. The "live-ssl" configuration controls access to the market data contained on the .49 server. This is evident from the configuration line: [10]

```
root /var/www/market/public
```

which tells the Nginx web server that the folder "public" contains the website content to load when visitors access the site.

24. The critical configuration lines from the live-ssl file are:

```
allow 127.0.0.1;
allow 62.75.246.20;
deny all;
```

These lines tell the web server to allow access from IP addresses 127.0.0.1 and 65.75.246.20, and to *deny* all other IP addresses from connecting to the web server. IP address 127.0.0.1 is commonly referred to in computer networking as "localhost" *i.e.*, the machine itself, which would allow the server to connect to itself. 65.75.246.20, as discussed **ante**, is the IP address for the front-end server, which must be permitted to access the back-end server. The "deny all" line tells the web server to deny connections from any IP address for which there is no specific exception provided.

25. Based on this configuration, it would have been impossible for Special Agent Tarbell to access the portion of the .49 server containing the Silk Road market data, including a portion of the login page, simply by entering the IP address of the server in his browser. As discussed in ¶ 24, the server was configured to refuse connections from all outside IP addresses with only one exception, the front-end server IP. Certainly, the IP address of the machine that Tarbell attempted to connect with did not have this IP

[10] The full text of the live-ssl configuration file is attached as Exhibit 6.

address, and the server would therefore have refused his connection attempt.

**2. *Phpmyadmin Configuration***

26. As discussed ante at ¶ 19, the .49 server contained two live virtual host configuration files, live-ssl and phpmyadmin. Phpmyadmin is an extremely popular open-source tool used to administrate MySQL databases from a web browser such as Google Chrome, Mozilla Firefox, or Internet Explorer. According to Sourceforge.net, phpmyadmin has been downloaded 2,375,431 times just this year and is available in numerous languages.[11] It is implemented on a large number of web servers around the world.

27. The active phpmyadmin configuration file contained in Item 1 of discovery contains the following lines[12]:

```
listen 80;
root /usr/share/phpmyadmin;
allow 127.0.0.1;
```

These lines direct the phpmyadmin virtual host to listen on port 80, which is the standard port for web traffic, and also tells Nginx to serve files from the phpmyadmin folder. The absence of "deny all" means that it would be possible for an IP address outside the Tor network to connect to the .49 server.

28. However, an IP address outside the tor network would have been able to access

[11] *See* http://sourceforge.net/projects/phpmyadmin/files/stats/timeline?dates=2014-01-01+to+2014-09-27, (last accessed September 27, 2014). Sourceforge.net is a popular site used by open-source software developers to host projects.
[12] The full text of the phpmyadmin configuration file is attached as Exhibit 7.

*only* the login page for phpmyadmin[13] and the files contained in the phpmyadmin folder, *not* any part of the Silk Road market or even the login screen, as claimed in the Tarbell Declaration, at ¶ 8. The 19-line excerpt from the Nginx access logs provided by the government confirms that fact. According to that excerpt, the server files accessed by law enforcement were all contained within the phpmyadmin folder and there was never any direct access to the actual Silk Road market data or even a login page for the market.

29. Rather, based on the server configuration files provided, the Silk Road login page referred to in ¶ 8 of the Tarbell Declaration must have been merely the login page for phpmyadmin and its underlying files. As discussed **ante**, phpmyadmin is an extremely popular tool for database administration, and its mere existence on the .49 server does not in any way demonstrate that illegal activity was conducted on the server.

30. Of the total 168,361,443 lines of Nginx access logs provided in discovery, only 3,348 show access to the .49 server from an outside IP address. All of these attempts show access to either the phpmyadmin files contained on the server or hacking attempts conducted on port 80. This data demonstrates that an outside IP address was never able to access the Silk Road market login page or files, and the law enforcement IP was no exception.

### B. *The Tarbell Declaration Raises More Questions Than it Answers*

#### 1. *Lack of Supporting Evidence*

31. Agent Tarbell explains that in early June 2013, he and another FBI Agent, "closely examined the traffic data being sent from the Silk Road website" and that they

[13] A screenshot of the phpmyadmin login page is attached hereto as Exhibit 8. For comparison, a screenshot of the Silk Road market login page is attached hereto as Exhibit 9, available at http://www.businessinsider.com/silk-road-walkthrough-2013-3?op=1 (last accessed September 30, 2014).

had, "examin[ed] the individual packets of data being sent back from the website . . . notic[ing] that the headers of some of the packets reflected a certain IP address not associated with any known Tor node." *See* Tarbell Decl. ¶¶ 7-8. Based on my experience, I know this to describe an activity commonly referred to as packet sniffing.

32. A packet sniffer is a computer program used to intercept and log traffic passing over a network interface, *i.e.*, a computer's software and/or hardware components that allow it to connect to the internet. For example, a laptop computer may have both an Ethernet port for a hard-wired internet connection and a wireless LAN card as its network interfaces.

33. One of the most popular and freely available packet sniffing tools is a computer program called Wireshark.[14] Wireshark can be easily configured to capture and record detailed information about each packet of web traffic as it is transmitted or received over a network interface. Among this information is a very precise timestamp (in seconds, to the 9th decimal place) for when the packet was logged, and information pertaining to the source and destination IP addresses of the packet.[15]

34. Using Wireshark's default configuration, the user would have had to affirmatively chosen *not* to save any logged information. Indeed, before exiting the program, the user is prompted with the question: "Do you want to save the captured packets before quitting? Your captured packets will be lost if you don't save them."[16]

---

[14] A disc of discovery materials provided to the defense by the FBI on September 18, 2014 contained a copy of Wireshark, strongly suggesting that the FBI is familiar with this tool. The disc of materials contained pen register data stored in .pcap files. Wireshark can be used to view this type of information.

[15] An example of the detailed information that can be captured about a single packet using Wireshark is attached hereto as Exhibit 10.

[16] *See* Wireshark Exit Screen screenshot, attached hereto as Exhibit 11.

35. Failure to preserve packet logs recorded while investigating the Silk Road servers would defy the most basic principles of forensic investigative techniques. Agent Tarbell is certified by the International Association of Computer Investigative Specialists as a Forensic Computer Examiner. *See* Tarbell Decl. ¶ 3. Some of the core competencies required for this certification include:

> a. Knowledge of search and seizure, legal process, and rules of evidence as applicable to computer forensics, laws, and procedures.
> b. Ability to explain on-scene actions taken for the preservation of digital evidence.
> c. Knowledge of proper computer search and seizure methodologies to include photographic and scene sketch procedures and documentation.
> d. Ability to establish, maintain and document a forensically sound examination environment.[17]

36. Despite the ease of preserving this information, The Government's September 23, 2014 letter to defense counsel explicitly provides, "[o]ther than Attachment 1, the Government is not aware of any contemporaneous records of the actions described in paragraphs 7 and 8 of the Tarbell declaration." The referenced Attachment 1 is the Nginx access log excerpt attached hereto as Exhibit 5.

37. Consequently, the government's position is that former SA Tarbell conducted his investigation of Silk Road, and penetrated the Silk Road Server, without documenting his work in *any way*.

---

[17] *See* IACIS CFCE Core Competencies, available at http://www.iacis.com/SiteAssets/Documents/CFCE_core_competencies.pdf (last accessed September 20, 2014). *See also* US DOJ: *Forensic Examination of Digital Evidence: A Guide for Law Enforcement,* Apr. 2004, available at https://www.ncjrs.gov/pdffiles1/nij/199408.pdf (Chapter 5 on Documenting and Reporting, instructing investigators to keep in-depth records of tasks performed during a forensic investigation).

### 2. *FBI Fuzzing of The Silk Road Server*

38. Former Special Agent Tarbell states, "[w]e were simply 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." Tarbell Decl., at ¶ 7 (emphasis added). I know from experience that the activity described by Special Agent Tarbell is commonly referred to as "fuzzing."

39. "Fuzzing" is the automated or semi-automated process of feeding semi-random input data into a computer program to test for vulnerabilities or security holes in the software.[18]

40. The government's September 23, 2014, letter to defense counsel (Ex. 4) makes clear that other than the 19-line excerpt from the Nginx access logs, there are no other records of the activity described in ¶¶7-8 of the Tarbell Declaration. In response to questions 6-11 (in defense counsel's September 17, 2014, letter to the government (Ex. 3)), the government has directed defense counsel to "*[s]ee* response to request #5[,]" referring to the solitary access log excerpt provided by the government. However, that excerpt explains only a very small portion of ¶8 of the Tarbell Declaration: "[w]hen I typed the Subject IP Address into an ordinary (non-Tor) browser, a part of the Silk Road login screen (the CAPTCHA prompt) appeared." None of the steps leading to the discovery of the Silk Road server IP as described in ¶¶ 7-8 are explained by the excerpt.

41. For example, request 9 in defense counsel's September 17, 2014, letter (Ex. 3) asks for, "[a]ny and all valid login credentials used to enter the Silk Road site." This request was made in light of ¶ 7 of the Tarbell Declaration, which described the use of

[18] *See* Fuzz Testing, available at http://en.wikipedia.org/wiki/Fuzz_testing (last accessed September 20, 2014).

valid login credentials for undercover accounts to enter the site. Based on my review of the Nginx access logs provided in discovery, I know that a valid login to the site is recorded as follows:

GET/silkroad/user/f01861c317

where "f01861c317" corresponds with a user identification number stored in the MySQL database contained in the server image. The 19-line excerpt provided by the Government contains no such requests indicating a valid login to the site.

42. If, as the Government asserts, there are no additional records of the activity described in ¶¶ 7-8 of the Tarbell Declaration, then the "miscellaneous entries" described therein never occurred.

### 3. *Mtime of Server Data Provided in Item 1 of Discovery Predates Initial Imaging of Silk Road Server*

43. According to the government's March 21, 2014, letter (Ex. 1), Item 1 of discovery contains the initial image of the Silk Road Server captured in July 2013, with IP address 193.107.86.49 (the allegedly "leaked" IP). According to the Tarbell Declaration, at ¶ 9, an official request was made to Icelandic authorities June 12, 2013, to "covertly image the contents of the Subject Server." This is confirmed by a June 12, 2013, letter to the Reykjavik Metropolitan Police from Assistant United States Attorney Serrin Turner.[19] According to Tarbell, "[a]fter obtaining the necessary court order under Icelandic law, the RMP imaged the Subject Server on July 23, 2013." Tarbell Decl. ¶ 12.

44. However, footnote 7 of the Tarbell Declaration states that several months *earlier*, a lead had been developed on a different server in Iceland with IP address 193.107.84.4 (hereinafter "the .4 server"). By letter of request to Icelandic authorities

[19] Attached to the Tarbell Declaration as Exhibit A.

dated February 28, 2013, U.S. law enforcement requested, *inter alia* that Icelandic authorities obtain traffic data for the server and covertly image it after consulting with the FBI. [20] By the time the requested information was produced by Icelandic authorities, the Silk Road server was no longer hosted at the server with IP address ending in .4, and "[a]s a result, the FBI did not request that Icelandic authorities proceed with imaging [the .4 server.]"[21]

45. The Tarbell Declaration states, "[t]he RMP provided a copy of the image of the [.49 Server] to the FBI on or about July 29, 2013." Tarbell Decl. at ¶ 13. It fails to mention that the .4 server images were nevertheless provided to U.S. law enforcement at that time. The government's September 23, 2014, letter to defense counsel provides:

> Icelandic authorities had already imaged the contents of [the .4] server by this time, on or about June 6, 2013. Although the Government did not ask Icelandic authorities to share the image of [the .4] server, Icelandic authorities included the image on the same device on which it produced the image of the SR Server to the Government on or about July 29, 2013.

Thus, according to the modification time of the .4 server images and the timeline provided in the Tarbell Declaration, the .4 server was imaged on June 6, 2013, prior to obtaining permission from the Icelandic Courts.

46. As discussed ante in ¶ 20, the "mtime" or modification time of a file indicates how old the data in the file is, *i.e.* when it was last modified.

47. The "images" provided to US law enforcement by the Republic of Iceland are actually ".tar.gz" compressed archive files. This type of compressed archive file is

[20] Letter attached to the Tarbell Declaration as Exhibit B.
[21] *See* Tarbell Declaration, at ¶ 9, n. 7.

commonly referred to as a "tarball." It is convenient to store files in this format because multiple files can be grouped into one for easier portability and storage.

48. There are a total of 4 tarballs in the first item of discovery: home, var, all, and orange21 – all contained in .tar.gz files. The mtime for orange21.tar.gz is consistent with the July 23, 2013 image date. However, the other 3 tarballs have an mtime of June 6, 2013, as shown below[22]:

```
root       30720 Jun  6  2013 home·tar·gz
root   737095680 Jun  6  2013 var·tar·gz
root  1728276480 Jun  6  2013 all·tar·gz
root 22360048285 Jul 23  2013 orange21·tar·gz
```

The modification date of the tarballs is consistent with an imaging date of June 6, 2013, a full six weeks before the July 23, 2013, imaging of the .49 Server, a fact never mentioned in the Tarbell Declaration.

## V. *Other Inconsistencies In the Government's Version*

49. Agent Tarbell states, "[t]he subject IP address was independently identified solely by . . . examining the traffic data sent back from the Silk Road website when we interacted with its user login interface." Tarbell Decl. at footnote 7. Yet, that claim is inconsistent with language in the June 12, 2013, letter to the Reykjavik Metropolitan Police, which indicates that analysis of traffic logs from the server assigned IP address

[22] This is a slightly modified version of the output from the Unix command "ls –ltr". ls is a unix program that is used to list the contents of a folder. When executed with the "-l" option, the program gives file information in its long listing format. This information includes, among other things, the modification time of the files in the directory.

193.107.84.4 may have aided law enforcement in determining the location of the .49 server.[23]

50. The Government's March 21, 2014, discovery letter (Ex. 1) indicates that item 9 in discovery contains an image of the Silk Road marketplace server captured in September 2013. By letter dated September 26, 2013,[24] U.S. Law Enforcement officials requested that Icelandic authorities reimage the .49 server and provide the contents to the FBI. However, the discovery materials contain no such image, which according to the government's September 23, 2014, letter, was in error.

## VI. Conclusion

51. As set forth above, there are a number of factual issues in dispute that need to be resolved:

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

(2) the account by former Special Agent Tarbell in his Declaration differs in important respects from the government's June 12, 2013, letter to Icelandic authorities. For example, that letter (which is Exhibit A to the government's opposition papers) suggests the possibility of an alternative method for the government's identifying and locating the Silk Road Server;

---

[23] On September 18, 2014 defense counsel was provided with traffic logs for the .49, .4, and .34 servers. At this stage of review, it does not appear that the .4 logs contain any information that could have aided law enforcement in determining the location of the .49 server. Given the short period of time to review this information prior to filing, counsel reserves the right to file supplemental briefing based on the continued review of this material.

[24] Attached to the Tarbell Declaration as Exhibit D.

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

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

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

52. These discrepancies between former Special Agent Tarbell's claims and the forensic reality of the discovery cannot be resolved without an evidentiary hearing.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief. 28 U.S.C. §1746. Executed September 30, 2014.

Joshua J. Horowitz

JOSHUA J. HOROWITZ