UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* THE CONTENTS OF THE SERVER ASSIGNED IP ADDRESS 207.106.6.25 MAINTAINED BY JTAN.COM	)	Case No.

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Pennsylvania *(identify the person or describe the property to be searched and give its location)*:
THE CONTENTS OF THE SERVER ASSIGNED IP ADDRESS 207.106.6.25 MAINTAINED BY JTAN.COM

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

SEE ATTACHED RIDER.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before _____
(not to exceed 10 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge [redacted]

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for ___ days *(not to exceed 30)*.
☐ until, the facts justifying, the later specific date of _____.

Date and time issued: _____

_____
Judge's signature

City and state: Philadelphia, PA

[redacted], U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of:

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the Court.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* THE CONTENTS OF THE SERVER ASSIGNED IP ADDRESS 207.106.6.25 MAINTAINED BY JTAN.COM	)	Case No.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

located in the Eastern District of Pennsylvania, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHED RIDER.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ❒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. §§ 841, 843, 846; 18 U.S.C. §§ 1956, 1957	drug trafficking/money laundering conspiracy

The application is based on these facts:

SEE ATTACHED RIDER

☑ Continued on the attached sheet.

❒ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

_____
Applicant's signature

[redacted], Special Agent, Federal Bureau of Investigation
Printed name and title

Sworn to before me and signed in my presence.

Date: September 9, 2013

_____
Judge's signature

City and state: Philadelphia, PA

[redacted] U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH WARRANT FOR THE PREMISES KNOWN AND DESCRIBED AS THE CONTENTS OF THE SERVER ASSIGNED IP ADDRESS 207.106.6.25 MAINTAINED BY JTAN.COM	:	**TO BE FILED UNDER SEAL** AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

EASTERN DISTRICT OF PENNSYLVANIA, ss.:

[redacted], being duly sworn, deposes and says:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I have been an FBI Special Agent for over 5 years. I am currently assigned to the computer intrusion squad in the FBI's New York Field Office. I have received extensive training regarding the use of computer technology to conduct criminal activity. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

2. I make this affidavit in support of an application for a warrant to search the contents of the server assigned IP address 207.106.6.25 (the "TARGET SERVER") maintained by JTAN.com, headquartered at 1302 Diamond Street, Sellersville, PA 18960 (the "Provider").

3. For the reasons detailed below, there is probable cause to believe that the TARGET SERVER contains evidence, fruits, and instrumentalities of narcotics trafficking and money laundering, in violation of Title 21, United States Code, Sections 841 and 846, and Title 18, United States Code, Sections 1956, 1957, and 2 (the "SUBJECT OFFENSES").

4. This affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement agents and civilian witnesses. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

STATUTORY PROVISIONS

5. 18 U.S.C. § 2703(b)(1)(A) allows the government to compel disclosure of all stored content and records or other information pertaining to a customer of an electronic communications service provider or remote computing service – without notice to the customer - pursuant to a search warrant issued using the procedures described in the Federal Rules of Criminal Procedure. Such an order may be issued by "any

district court of the United States (including a magistrate judge of such a court)" that "is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored." 18 U.S.C. § 2711(3)(A)(ii).

THE INVESTIGATION

Background on the Silk Road Website

6. This application stems from an ongoing investigation into an underground website used to sell illegal drugs known as "Silk Road." Silk Road provides an infrastructure similar to well-known online marketplaces such as Amazon Marketplace or eBay, allowing sellers and buyers to conduct transactions online. However, unlike such legitimate websites, Silk Road is dedicated to the sale of illegal narcotics and other black-market goods and services. 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.

7. The Silk Road website is specifically designed to facilitate the illegal commerce hosted on the site by ensuring absolute anonymity on the part of both buyers and sellers. The primary means by which the website protects the anonymity of its users is by operating on the "TOR" network. The TOR network is a special network of computers distributed around the world designed to conceal the true Internet protocol ("IP") addresses of the users of the network.[1] Every communication sent through the TOR network is bounced through numerous relays within the network, and wrapped in a layer of encryption at each relay, such that the end recipient of the communication has no way of tracing the communication back to its true originating IP address. In a similar fashion, the TOR network also enables websites to operate on the network in a manner that conceals the true IP address of the computer server hosting the website.

8. Another means by which the Silk Road website protects the anonymity of its users is by requiring all transactions to be paid for through the use of "Bitcoins." Bitcoins are a virtually untraceable, decentralized, peer-to-peer form of electronic currency having no association with banks or governments. In order to acquire Bitcoins in the first

[1] Every computer attached to the Internet is assigned a unique numerical identifier known as an Internet protocol or "IP" address. A computer's IP address can be used to determine its physical location and, in turn, to identify the user of the computer.

instance, a user typically must purchase them from a Bitcoin "exchanger." Bitcoin exchangers accept payments of currency in some conventional form (cash, wire transfer, etc.) and exchange the money for a corresponding amount of Bitcoins (based on a fluctuating exchange rate); and, similarly, they will accept payments of Bitcoin and exchange the Bitcoins for conventional currency. Once a user acquires Bitcoins from an exchanger, the Bitcoins are kept in an anonymous "wallet" controlled by the user, designated simply by a string of letters and numbers. The user can then use the Bitcoins to conduct anonymous financial transactions by transferring Bitcoins from his or her wallet to the wallet of another Bitcoin user. All Bitcoin transactions are recorded on a public ledger known as the "Blockchain"; however, the ledger only reflects the movement of funds between anonymous wallets and therefore cannot by itself be used to determine the identities of the persons involved in the transactions. Those operating Silk Road charge a commission, in the form of Bitcoins, for every sale conducted through the site.

9. Since November of 2011, law enforcement agents participating in this investigation have made over 70 individual purchases of controlled substances from various vendors on the Silk Road Underground Website. The substances purchased have been various Schedule I and II drugs, including ecstasy, cocaine, heroin, LSD, and others. As of April 2013, at least 56

samples of these purchases have been laboratory-tested, and, of these, 54 have shown high purity levels of the drug the item was advertised to be on Silk Road. Based on the postal markings on the packages in which the drugs arrived, these purchases appear to have been filled by vendors located in over ten different countries, including the United States.

Seizure of the Silk Road Server

10. Earlier this year, the FBI located the server hosting the Silk Road website (the "Silk Road Web Server") in a foreign country. Through a Mutual Legal Assistance Treaty request, the FBI received an image of the contents of the Silk Road Web Server on or about July 29, 2013. An FBI computer forensic team has analyzed the contents of the Silk Road Web Server and fully confirmed that the server is hosting the Silk Road website.

11. Among other data, the Silk Road Web Server contains databases used to run the Silk Road website, including databases of vendor postings, transaction records, private messages between users, and other data reflecting user activity. In analyzing the configuration of the Silk Road Web Server, the FBI has discovered that the server regularly purges data from these databases older than 60 days. Thus, the image of the Silk Road Web Server possessed by the FBI contains data reflecting only 60 days of user activity, counting back from the date the server was imaged.

12. However, the FBI has also discovered computer code on the Silk Road Web Server that periodically backs up data from the server and exports that data to another server. Testing of this backup script has revealed the IP address of the server to which this backup data is exported – namely, the IP address of the TARGET SERVER. Based on analysis of the backup script, it does not appear that previously backed-up data is deleted when new back-ups are made. Therefore, I believe it is likely that the TARGET SERVER contains records of user activity on the Silk Road website spanning a much longer date range than the data kept on the Silk Road Web Server.

13. Based on publicly available IP address registration records, I have learned that the TARGET SERVER is controlled by a server hosting company named JTAN.com. Based on information obtained from a representative of JTAN.com, I have learned the following:

a. JTAN.com allows its customers to lease servers through its service with complete anonymity. Accordingly, JTAN.com does not ask its customers for verified identification information, and it allows its customers to pay anonymously through the use of Bitcoins.

b. The JTAN.com customer associated with the TARGET SERVER has paid for the TARGET SERVER using Bitcoins; and, in communicating with JTAN.com customer support, the customer has

communicated exclusively through TOR. These facts further corroborate that the TARGET SERVER is associated with Silk Road, given that the owner of Silk Road is clearly familiar with TOR and receives revenue from the site in the form of Bitcoins.

c. The TARGET SERVER is physically maintained at a server storage facility, specifically, Windstream Communications Conshohocken Data Center, located at 1100 East Hector Street, Lee Park, Suite 500, Conshohocken, Pennsylvania.

d. However JTAN.com has administrative access to the TARGET SERVER. In response to the FBI's inquiry concerning the server, JTAN.com has electronically preserved the contents of the TARGET SERVER and can produce this data to the FBI in response to the search warrant sought herein.

Request to Search the Contents of the Target Server

14. Based on the foregoing, I believe that the TARGET SERVER will contain back-ups of data from the Silk Road Web Server, including but not limited to back-ups of data reflecting vendor postings, transactional records, private messages between users, and other user activity on the Silk Road website. Based on my familiarity with the data stored on the Silk Road Web Server, I believe that this back-up data will reflect the details of numerous narcotics transactions conducted through the Silk Road website, and the use of Bitcoins to launder the proceeds from these transactions. Likewise, I believe the data

will contain numerous private messages between users of the site that may enable the FBI to identify particular users, potentially including the administrators of the website and the most prominent drug dealers operating on it.

15. Given that the TARGET SERVER is used to store back-up data from the Silk Road Web Server, I believe it is likely that the TARGET SERVER is used in other ways to support the operation of Silk Road and will contain other data relevant to the investigation. Such data may include, for example:

a. Computer programs and other files used in connection with administering the Silk Road website, which may reveal, among other things, the IP addresses of additional computers associated with Silk Road, or other information that could be used to identify and locate such computers;

b. Data reflecting the use of the TOR network or other technological methods (such as encryption or proxy services) to evade monitoring or detection by law enforcement;

c. Encryption keys, passwords, or similar access devices that may be necessary to access data relating to Silk Road;

d. Communications between the user of the TARGET SERVER and any accomplices, confederates or aiders and abettors; and

e. Other information that may assist law enforcement in determining the identity and location of the user of the TARGET SERVER or his/her accomplices, confederates or aiders and abettors, including but not limited to: IP addresses, names, addresses, phone numbers, e-mail accounts, social networking accounts, website registration accounts, credit card accounts, bank accounts, and payment records.

16. Finally, based on my training and experience, I believe it is likely that the TARGET SERVER will contain records of logins to the TARGET SERVER, which may reveal the IP address(es) of the owner of Silk Road or anyone else with access to the server.

17. Accordingly, I believe that the TARGET SERVER is likely to contain the categories of evidence set forth in Attachment A.

SEARCH PROCEDURE

18. The search warrant requested herein will be transmitted to JTAN.com, which will be directed to produce a digital copy of the contents of the TARGET SERVER. Law enforcement personnel will then review this content information for evidence or fruits of the SUBJECT OFFENSES, as specified in Section II of Attachment A.

19. It is further respectfully requested this Court issue an order precluding JTAN.com from giving notice to its

subscriber. Because the government is using a search warrant, there is no duty to notify the customer. Sending a copy to JTAN.com, the place where the warrant is to be executed, is sufficient. However, because the disclosure of the existence of this warrant to the subscriber could result in the destruction of evidence, I request that the Court issue an order under 18 U.S.C. § 2705(b), precluding JTAN.com from giving notice to its subscriber.

CONCLUSION

20. Based on the foregoing, I respectfully request that the Search Warrant sought herein issue pursuant to Rule 41 of the Federal Rules of Criminal Procedure.

Dated: Philadelphia, Pennsylvania
September 9, 2013

[redacted]ent
Federal Bureau of Investigation

Sworn to before me on
September 9, 2013

HON. [redacted]
UNITE[redacted]JUDGE
EASTERN DISTRICT OF PENNSYLVANIA

Attachment A

Property to Be Searched

This warrant applies to the contents of the server assigned IP address 207.106.6.25 (the "TARGET SERVER") maintained by JTAN.com, headquartered at 1302 Diamond Street, Sellersville, PA 18960 (the "Provider").

Particular Things to Be Seized

I. Search Procedure

This warrant will be transmitted to the Provider's personnel, who will be directed to produce the contents of the TARGET SERVER to law enforcement personnel. Upon receipt of the production, law enforcement personnel will review the data produced to locate the items described in Section II below.

II. Information to Be Seized by the Government

The information to be seized by the Government includes all data from the TARGET SERVER that contains or constitutes evidence, fruits, or instrumentalities of narcotics trafficking and money laundering, in violation of Title 21, United States Code, Sections 841, 843, and 846, and Title 18, United States Code, Sections 1956, 1957, and 2 (the "SUBJECT OFFENSES"), including any evidence concerning the following:

a. an underground website operating a marketplace for illegal drugs and other illegal goods and services (the "TARGET WEBSITE"), including but not limited to role of the user(s) of the TARGET SERVER in administering the website;

b. the purchase or sale of illegal narcotics through the TARGET WEBSITE;

c. the use of Bitcoins or any other means to launder the proceeds of narcotics trafficking; and

d. computer programs or files used to administer the TARGET WEBSITE;

e. the IP addresses of other computers associated with the TARGET WEBSITE, or other information that could be used to identify and locate these computers;

f. the use of the TOR network or other technological methods (such as encryption or proxy services) to evade monitoring or detection by law enforcement;

g. passwords, encryption keys, and other access devices that may be necessary to access any data pertaining to the TARGET WEBSITE ;

h. communications between the user of the TARGET SERVER and any accomplices, confederates or aiders and abettors;

i. any information that may assist law enforcement in determining the identity and location of the user of the TARGET SERVER or his/her accomplices, confederates or aiders and abettors, including but not limited to: IP addresses, names, addresses, phone numbers, e-mail accounts, social networking accounts, website registration accounts, credit card accounts, bank accounts, and payment records; and

j. any other evidence of the SUBJECT OFFENSES.