

INTERNET LAW: CASES & PROBLEMS

PRIMARY DOCUMENTS APPENDIX

James Grimmelman
*Tessler Family Professor of
Digital and Information Law
Cornell Tech and Cornell Law School*

Thirteenth edition © 2023 James Grimmelman



www.semaphorepress.com

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) Case No.
 207.106.6.25 MAINTAINED BY JTAN.COM)
)
)

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
 21 U.S.C. §§ 841, 843, 846; 18 U.S.C. §§
 1956, 1957

Offense Description
 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

 , 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

 U.S. Magistrate Judge

Printed name and title


UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

- - - - - x
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 :
- - - - - x

TO BE FILED UNDER SEAL

AFFIDAVIT IN SUPPORT
OF A SEARCH WARRANT

EASTERN DISTRICT OF PENNSYLVANIA, ss.:

, 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] JUDGE
UNITE 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.

FILED
RICHARD W. NAGEL
CLERK OF COURT

17 FEB 24 PM 12:58

U.S. DISTRICT COURT
SOUTHERN DIST OHIO
WEST DIV CINCINNATI

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

)
IN RE APPLICATION OF THE)
UNITED STATES OF AMERICA FOR)
AN ORDER PURSUANT TO)
18 U.S.C. § 2703(d))

MISC. NO. **1:17MJ-150**

Filed Under Seal

APPLICATION OF THE UNITED STATES
FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)

The United States of America, moving by and through its undersigned counsel, respectfully submits under seal this *ex parte* application for an Order pursuant to 18 U.S.C. § 2703(d). The proposed Order would require Google, an Internet Service Provider located in Mountain View, CA, to disclose certain records and other information pertaining to the email account(s): bloodycivilian911@gmail.com and fadi4u67@gmail.com. The records and other information to be disclosed are described in Attachment A to the proposed Order. In support of this application, the United States asserts:

LEGAL BACKGROUND

1. Google is a provider of an electronic communications service, as defined in 18 U.S.C. § 2510(15), and/or a remote computing service, as defined in 18 U.S.C. § 2711(2). Accordingly, the United States may use a court order issued under § 2703(d) to require Google to disclose the items described in Part II of Attachment A. *See* 18 U.S.C. § 2703(c)(2) (Part II.A of Attachment A); 18 U.S.C. § 2703(c)(1) (Part II.B of Attachment A).

2. This Court has jurisdiction to issue the proposed Order because it is “a court of competent jurisdiction,” as defined in 18 U.S.C. § 2711. *See* 18 U.S.C. § 2703(d). Specifically,

the Court is a district court of the United States that has jurisdiction over the offense being investigated. *See* 18 U.S.C. § 2711(3)(A)(i).

3. A court order under § 2703(d) “shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d). Accordingly, the next section of this application sets forth specific and articulable facts showing that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are relevant and material to an ongoing criminal investigation.

THE RELEVANT FACTS

4. The United States is investigating the material support of designated foreign terrorist organizations. The investigation concerns possible violations of, *inter alia*, 18 U.S.C. § 2339A (Providing material support to terrorists).

5. The subject is being investigated for support of a designated foreign terrorist organization, namely the Islamic State or “ISIL”. The subject has operated multiple Twitter handles and communicated numerous messages in support of ISIL. In addition, through Twitter, the subject has been connected with other subjects of similar investigations. The subject’s original Twitter account was opened via the Google mail account, fadi4u67@gmail.com. The subject’s most recent Twitter account was opened via the Google mail account, bloodycivilian911@gmail.com.

REQUEST FOR ORDER

6. The facts set forth in the previous section show that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are

relevant and material to an ongoing criminal investigation. Specifically, these items will help the United States to identify and locate the individual(s) who are responsible for the events described above, and to determine the nature and scope of their activities. Accordingly, the United States requests that Google be directed to produce all items described in Part II of Attachment A to the proposed Order.

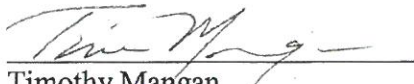
7. The United States further requests that the Order require Google not to notify any person, including the subscribers or customers of the account(s) listed in Part I of Attachment A, of the existence of the Order until further order of the Court. *See* 18 U.S.C. § 2705(b). This Court has authority under 18 U.S.C. § 2705(b) to issue “an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order.” *Id.* In this case, such an order would be appropriate because the requested Order relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the requested Order will seriously jeopardize the investigation, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or notify confederates. *See* 18 U.S.C. § 2705(b)(2), (3), (5). Some of the evidence in this investigation is stored electronically. If alerted to the investigation, the subjects under investigation could destroy that evidence, including information saved to their personal computers.

8. The United States further requests that the Court order that this application and any resulting order be sealed until further order of the Court. As explained above, these

documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

Benjamin C. Glassman
UNITED STATES ATTORNEY



Timothy Mangan
Assistant United States Attorney
221 E. Fourth Street, Suite 400
Cincinnati, OH 45202

FILED
RICHARD W. NAGEL
CLERK OF COURT

17 FEB 24 PM 12:58

U.S. DISTRICT COURT
SOUTHERN DIST OHIO
WEST DIV CINCINNATI

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

)
IN RE APPLICATION OF THE)
UNITED STATES OF AMERICA FOR)
AN ORDER PURSUANT TO)
18 U.S.C. § 2703(d))

MISC. NO.

17 MJ -150

Filed Under Seal

ORDER

The United States has submitted an application pursuant to 18 U.S.C. § 2703(d), requesting that the Court issue an Order requiring Google, an electronic communications service provider and/or a remote computing service located in Mountain View, CA, to disclose the records and other information described in Attachment A to this Order.

The Court finds that the United States has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

The Court determines that there is reason to believe that notification of the existence of this Order will seriously jeopardize the ongoing investigation, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or notify confederates. *See* 18 U.S.C. § 2705(b)(2), (3), (5).

IT IS THEREFORE ORDERED, pursuant to 18 U.S.C. § 2703(d), that Google shall, within ten days of the date of this Order, disclose to the United States the records and other information described in Attachment A to this Order.

IT IS FURTHER ORDERED that Google shall not disclose the existence of the application of the United States, or the existence of this Order of the Court, to the subscribers of

the account(s) listed in Attachment A, or to any other person, unless and until otherwise authorized to do so by the Court, except that Google may disclose this Order to an attorney for Google for the purpose of receiving legal advice.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court.


United States Magistrate Judge

2/24/17
Date

ATTACHMENT A

I. The Account(s)

The Order applies to certain records and information associated with the following email account(s): bloodycivilian911@gmail.com and fadi4u67@gmail.com

II. Records and Other Information to Be Disclosed

Google is required to disclose the following records and other information, if available, to the United States for each account or identifier listed in Part I of this Attachment ("Account"), for the time period from 2014 to the present:

- A. The following information about the customers or subscribers of the Account:
1. Names (including subscriber names, user names, and screen names);
 2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
 3. Local and long distance telephone connection records;
 4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
 5. Length of service (including start date) and types of service utilized;
 6. Telephone or instrument numbers (including MAC addresses);
 7. Other subscriber numbers or identities (including temporarily assigned network addresses and registration Internet Protocol ("IP") addresses (including carrier grade natting addresses or ports)); and
 8. Means and source of payment for such service (including any credit card or bank account number) and billing records.
- B. All records and other information (not including the contents of communications) relating to the Account, including:
1. Records of user activity for each connection made to or from the Account, including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; and source and destination Internet Protocol addresses;
 2. Information about each communication sent or received by the Account, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers).

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS
PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google, and my official title is _____. I am a custodian of records for Google. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Google; and
- c. such records were made by Google as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature

UNITED STATES DISTRICT COURT
for the
Northern District of California

IN RE: DMCA SECTION 512(h)
SUBPOENA TO GITHUB, INC.

Civil Action No. 3:23-mc-80090-LJC

**SUBPOENA TO PRODUCE DOCUMENTS, INFORMATION, OR OBJECTS
OR TO PERMIT INSPECTION OF PREMISES IN A CIVIL ACTION**

To: GitHub, Inc., 88 Colin P Kelly Jr. St., San Francisco, California 94107

(Name of person to whom this subpoena is directed)

Production: **YOU ARE COMMANDED** to produce at the time, date, and place set forth below the following documents, electronically stored information, or objects, and to permit inspection, copying, testing, or sampling of the material: SEE ATTACHMENT A

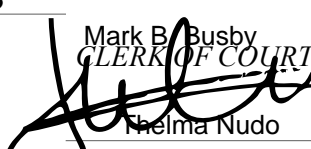

Place: Quinn Emanuel Urquhart & Sullivan, LLP 555 Twin Dolphin Drive, 5th Floor Redwood Shores, California 94065-2139	Date and Time: April 3, 2023 at 10:00 a.m.
---	---

Inspection of Premises: **YOU ARE COMMANDED** to permit entry onto the designated premises, land, or other property possessed or controlled by you at the time, date, and location set forth below, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

Place:	Date and Time:
--------	----------------

The following provisions of Fed. R. Civ. P. 45 are attached – Rule 45(c), relating to the place of compliance; Rule 45(d), relating to your protection as a person subject to a subpoena; and Rule 45(e) and (g), relating to your duty to respond to this subpoena and the potential consequences of not doing so.

Date: 3/28/2023


 Mark B. Busby
 CLERK OF COURT

 Thelma Nudo
 Signature of Clerk or Deputy Clerk

OR

Attorney's signature

The name, address, e-mail address, and telephone number of the attorney representing *(name of party)* _____
 Twitter, Inc. _____, who issues or requests this subpoena, are:
 Rachel Herrick Kassabian, 555 Twin Dolphin Drive, 5th Floor, Redwood Shores, California 94065-2139, rachelkassabian@quinnemanuel.com,
 (650) 801-5000

Notice to the person who issues or requests this subpoena

If this subpoena commands the production of documents, electronically stored information, or tangible things or the inspection of premises before trial, a notice and a copy of the subpoena must be served on each party in this case before it is served on the person to whom it is directed. Fed. R. Civ. P. 45(a)(4).

Civil Action No. 3:23-mc-80090-LJC

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)

I received this subpoena for *(name of individual and title, if any)* _____
on *(date)* _____ .

I served the subpoena by delivering a copy to the named person as follows: _____

_____ on *(date)* _____ ; or

I returned the subpoena unexecuted because: _____
_____ .

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also
tendered to the witness the fees for one day’s attendance, and the mileage allowed by law, in the amount of
\$ _____ .

My fees are \$ _____ for travel and \$ _____ for services, for a total of \$ _____ 0.00 _____ .

I declare under penalty of perjury that this information is true.

Date: _____

Server’s signature

Printed name and title

Server’s address

Additional information regarding attempted service, etc.:

Federal Rule of Civil Procedure 45 (c), (d), (e), and (g) (Effective 12/1/13)**(c) Place of Compliance.**

(1) For a Trial, Hearing, or Deposition. A subpoena may command a person to attend a trial, hearing, or deposition only as follows:

- (A) within 100 miles of where the person resides, is employed, or regularly transacts business in person; or
- (B) within the state where the person resides, is employed, or regularly transacts business in person, if the person
 - (i) is a party or a party's officer; or
 - (ii) is commanded to attend a trial and would not incur substantial expense.

(2) For Other Discovery. A subpoena may command:

- (A) production of documents, electronically stored information, or tangible things at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person; and
- (B) inspection of premises at the premises to be inspected.

(d) Protecting a Person Subject to a Subpoena; Enforcement.

(1) Avoiding Undue Burden or Expense; Sanctions. A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.

(2) Command to Produce Materials or Permit Inspection.

(A) *Appearance Not Required.* A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

(B) *Objections.* A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

- (i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection.
- (ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

(3) Quashing or Modifying a Subpoena.

(A) *When Required.* On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:

- (i) fails to allow a reasonable time to comply;
- (ii) requires a person to comply beyond the geographical limits specified in Rule 45(c);
- (iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or
- (iv) subjects a person to undue burden.

(B) *When Permitted.* To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:

- (i) disclosing a trade secret or other confidential research, development, or commercial information; or

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.

(C) *Specifying Conditions as an Alternative.* In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

- (i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and
- (ii) ensures that the subpoenaed person will be reasonably compensated.

(e) Duties in Responding to a Subpoena.

(1) Producing Documents or Electronically Stored Information. These procedures apply to producing documents or electronically stored information:

(A) *Documents.* A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

(B) *Form for Producing Electronically Stored Information Not Specified.* If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

(C) *Electronically Stored Information Produced in Only One Form.* The person responding need not produce the same electronically stored information in more than one form.

(D) *Inaccessible Electronically Stored Information.* The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) Claiming Privilege or Protection.

(A) *Information Withheld.* A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

- (i) expressly make the claim; and
- (ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

(B) *Information Produced.* If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

(g) Contempt.

The court for the district where compliance is required—and also, after a motion is transferred, the issuing court—may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena or an order related to it.

ATTACHMENT A
DOCUMENTS TO BE PRODUCED UNDER SUBPOENA

1. All identifying information, including the name(s), address(es), telephone number(s), email address(es), social media profile data, and IP address(es), for the user(s) associated with the following GitHub username: FreeSpeechEnthusiast. Please include all identifying information provided when this account was established, as well as all identifying information provided subsequently for billing or administrative purposes.
2. All identifying information, including the name(s), address(es), telephone number(s), email address(es), social media profile data, and IP address(es), for the users who posted, uploaded, downloaded or modified the data at the following URL:

<https://github.com/FreeSpeechEnthusiast/PublicSpace>

January 4, 2016

Recipient Information:

Wikimedia Foundation, Inc.
Wikimedia Commons
C/O Copyright Agent for Notice of Claims of Copyright Infringement
Lila Tretikov, Designated Agent
Wikimedia Foundation
c/o CT Corporation System
legal@wikimedia.org

Sent via: Email

DMCA Notice of Copyright Infringement

Dear Wikimedia Foundation, Inc.

I, [REDACTED] certify under penalty of perjury, that I am an agent authorized to act on behalf of the owner of certain intellectual property rights.

I have a good faith belief that the items or materials listed below are not authorized by law for use by the above named domain name owner or their agents and therefore infringes the copyright owner's rights. I hereby demand that you act expeditiously to remove or disable access to the material or items claimed to be infringing.

My contact information is as follows:

Garvey Schubert Barer
[REDACTED], Attorney
[REDACTED]
Seattle, WA 98101
Phone: 206-[REDACTED]
Email: trademarks@gsblaw.com

Allegedly Infringing items or materials:

The infringing content includes unauthorized use of our client, Bernie 2016, Inc.'s logos and images.

Infringing material that I demand be disabled or removed in consideration of the above:

https://commons.wikimedia.org/wiki/File:Bernie_Sanders_2016_logo.svg
https://upload.wikimedia.org/wikipedia/commons/d/dd/Bernie_Sanders_2016_logo.svg
https://upload.wikimedia.org/wikipedia/commons/archive/d/dd/20151025203909%21Bernie_Sanders_2016_logo.svg
https://commons.wikimedia.org/wiki/File:Bernie_Sanders_2016_logo.png
https://upload.wikimedia.org/wikipedia/commons/d/d4/Bernie_Sanders_2016_logo.png
https://upload.wikimedia.org/wikipedia/commons/archive/d/d4/20150809230127%21Bernie_Sanders_2016_logo.png
https://commons.wikimedia.org/wiki/File:Bernie_Sanders_2016_logo_with_year.svg

https://upload.wikimedia.org/wikipedia/commons/f/f8/Bernie_Sanders_2016_logo_with_year.svg
https://upload.wikimedia.org/wikipedia/commons/archive/f/f8/20151025204133%21Bernie_Sanders_2016_logo_with_year.svg
https://commons.wikimedia.org/wiki/File:Bernie_Sanders_2016_Pride.jpg
https://upload.wikimedia.org/wikipedia/commons/8/8a/Bernie_Sanders_2016_Pride.jpg
<https://commons.wikimedia.org/wiki/File:FEELTHEBERN.png>
<https://upload.wikimedia.org/wikipedia/commons/b/b5/FEELTHEBERN.png>
<https://upload.wikimedia.org/wikipedia/commons/archive/b/b5/20151022003214%21FEELTHEBERN.png>
<https://commons.wikimedia.org/wiki/File:FEELTHEBERN.svg>
<https://upload.wikimedia.org/wikipedia/commons/6/6d/FEELTHEBERN.svg>

Location of ORIGINAL WORKS:

<https://berniesanders.com/>
<https://store.berniesanders.com/>
<https://store.berniesanders.com/collections/feel-the-bern>
<https://store.berniesanders.com/collections/feel-the-bern/products/feel-the-bern-car-magnet>

My electronic signature follows:

Sincerely,
/ [REDACTED] /
Attorney

15 January 2016

Lila Tretikov, Designated Agent
Wikimedia Foundation, Inc.
c/o CT Corporation System
818 West Seventh Street
Los Angeles, California 90017
legal@wikimedia.org

DMCA Copyright Infringement Counter Notification

Dear Ms. Tretikov,

this letter is a formal response to a claim of copyright infringement against material published on the website Wikimedia Commons at <<https://commons.wikimedia.org>> as listed below. I believe the claims of copyright infringement are inaccurate and should be rejected because the material in question does not contain a sufficient amount of original and creative artistic or graphic authorship upon which to support a copyright claim and therefore belongs in the public domain and as a result may be reproduced by anyone.

This communication to you is a DMCA counter notification letter as defined in 17 USC 512(g)(3).

I declare, under penalty of perjury, that I have a good faith belief that the material was removed or disabled as a result of mistake or misidentification.

I ask that the Wikimedia Foundation, upon receipt of this counter notification, restore the material in dispute, unless the complainant files suit against me within ten (10) days, pursuant to 17 USC 512(g)(2)(B).

Identification of the material and its location before it was removed:

- https://commons.wikimedia.org/wiki/File:Bernie_Sanders_2016_logo.svg
- https://commons.wikimedia.org/wiki/File:Bernie_Sanders_2016_logo.png
- https://commons.wikimedia.org/wiki/File:Bernie_Sanders_2016_logo_with_year.svg
- https://commons.wikimedia.org/wiki/File:Bernie_Sanders_2016_Pride.jpg
- <https://commons.wikimedia.org/wiki/File:FEELTHEBERN.png>
- <https://commons.wikimedia.org/wiki/File:FEELTHEBERN.svg>

My name, address, and telephone number are:

Tomasz Kozlowski

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

I hereby consent to the jurisdiction of the Federal District Court for the San Francisco, California judicial district.

I agree to accept service of process from the complainant.

Best regards,

Tomasz Kozlowski