

Exhibit J

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

18 MAG 9130

IN THE MATTER OF THE APPLICATION OF THE
UNITED STATES OF AMERICA FOR A SEARCH
WARRANT FOR INFORMATION AND DATA
ASSOCIATED WITH THE GRAVATAR PROFILE
URL
HTTPS://EN.GRAVATAR.COM/JOSHSCHULTE1
(INCLUDING THE WORDPRESS SITES
JOSHSCHULTE.WORDPRESS.COM AND
PRESUMPTIONOFLAVERY.WORDPRESS.COM);
STORED AT PREMISES CONTROLLED BY
AUTOMATTIC, INC.

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Automattic, Inc. ("Automattic")

The Federal Bureau of Investigation (the "FBI" or the "Investigative Agency")

1. **Warrant.** Upon an affidavit of Special Agent Jeff D. Donaldson of the FBI and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. §§ 2703(b)(1)(A) and 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds that there is probable cause to believe the Gravatar profile URL <https://en.gravatar.com/joshschulte1>, which includes the sites joshschulte.wordpress.com, presumptionofslavery.wordpress.com, and presumptionofinnocence.net, maintained at premises controlled by Automattic, which is headquartered at 60 29th Street #343, San Francisco, California 94110, contain evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, Automattic is hereby directed to provide to the Investigative Agency, within three days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A which shall not be

JAS_021323

transmitted to the Provider. The Government is required to serve a copy of this Warrant and Order on Automattic within one day of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which Automattic is capable of accepting service.

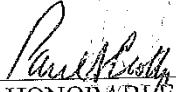
2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, danger to the physical safety of an individual, flight from prosecution, and/or intimidation of potential witnesses or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that Automattic shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of 30 days from the date of this Order, subject to extension upon application to the Court if necessary, except that Automattic may disclose this Warrant and Order to an attorney for Automattic for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on Automatic; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

10/16/2018
Date Issued

1039
Time Issued



THE HONORABLE PAUL A. CROTTY
United States District Judge
Southern District of New York

Attachment A

I. The Target Accounts and Execution of Warrant

This warrant is directed to Automattic, Inc. (“Automattic” or the “Provider”) and applies to all content and other information within Automattic’s possession, custody, or control that is associated with the Gravatar profile URL <https://en.gravatar.com/joshschulte1>, which includes the sites joshschulte.wordpress.com, presumptionofslavery.wordpress.com, and presumptionofinnocence.net, account with the user identification number 5b8c7b1fb405c187399aded3 and associated with the email account freejasonbourne@protonmail.com (collectively, the “**Target Accounts**”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to Automattic. Automattic is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, a copy of which shall not be transmitted to the Provider.

II. Information to be Produced by Automattic

To the extent within the Provider’s possession, custody, or control, the Provider is directed to produce the following information, from December 1, 2017 to present, associated with each

Target Account:

i. *Subscriber Information.* Any and all records showing subscriber information for the **Target Accounts**, including the username, email address, name, and telephone number associated with the **Target Accounts**.

ii. *Billing Information.* Any and all records showing reflecting any billings related to the **Target Accounts**.

iii. *Transactional Information.* Any and all transaction log data related to the **Target Accounts**, including the user's IP address, browser type, and operating system.

iv. *Site Creation, Posting, and Revision History Information.* Any and all records reflecting activity information related to the creation of a site and posting of revising information on the **Target Accounts**, including records showing the date and time at which the site was created, the IP address used to create the site or post information to the site, and posts, such as deleted posts, including for any other sites of any kind associated with the Gravatar assigned to the Target Account.

v. *Comment Information.* Any and all information about any comments posted on the **Target Accounts**.

vi. *Contact Information Associated with Domain Registration.* Any and all records reflecting any custom domain registrations for the **Target Accounts**.

vii. *Linked Accounts.* All accounts or Gravatars or accounts linked to the **Target Accounts** by common machine cookie, creation IP address, or recovery phone or email, and for such Gravatars, all records called for by sub-paragraphs i-vi. of this paragraph.

h. *Preserved Records.* Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of a scheme to disseminate classified and otherwise protected information, including through the use of contraband cellphones, software, and other devices, in violation of 18

U.S.C. §§ 401 (contempt of court), 793 (unlawful disclosure of classified information); 1030 (unauthorized computer access), 1503 and 1512 (obstruction of justice), 1791 (smuggling contraband into a federal detention facility) and 2252A (illegal acts related to child pornography); as well as conspiracies and attempts to violate these provisions and aiding and abetting these offenses, among other statutes (the “Subject Offenses”), including the following:

- a. Evidence of the identity(ies) of the user(s) of the **Target Accounts** and any and all cellphones (“Contraband Cellphones”) smuggled into the Metropolitan Correctional Center in New York, New York (the “MCC”) for Joshua Schulte or Omar Amanat, as well as other coconspirators in contact with the **Target Accounts** or the Contraband Cellphones;
- b. Evidence relating to the geolocation of the users of the **Target Accounts** or the Contraband Cellphones at times relevant to the Subject Offenses;
- c. Evidence relating to the participation in the Subject Offenses by Schulte, Amanat, and others using or in communication with the **Target Accounts** or the Contraband Cellphones;
- d. Evidence concerning financial institutions and transactions used by the users of the **Target Accounts** in furtherance of the Subject Offenses;
- e. Communications evidencing the Subject Offenses;
- f. Evidence of and relating to computers or other online accounts and facilities (such as additional email addresses) controlled or maintained by the user(s) of the Contraband Cellphones or **Target Accounts**; and
- g. Passwords or other information needed to access any such computers, accounts, or facilities.

18 MAG 9130

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE APPLICATION OF
THE UNITED STATES OF AMERICA FOR A
SEARCH WARRANT FOR INFORMATION AND
DATA ASSOCIATED WITH THE BUFFER
ACCOUNT WITH THE USER IDENTIFICATION
NUMBER 5B8C7B1FB405C1873
99ADCD3 AND ASSOCIATED WITH THE EMAIL
ACCOUNT
FREEJASONBOURNE@PROTONMAIL.COM;
STORED AT PREMISES CONTROLLED BY
BUFFER, INC.

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Buffer, Inc. ("Buffer")

The Federal Bureau of Investigation (the "FBI" or the "Investigative Agency")

1. **Warrant.** Upon an affidavit of Special Agent Jeff D. Donaldson of the FBI and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. §§ 2703(b)(1)(A) and 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds that there is probable cause to believe the Buffer account with the user identification number 5b8c7b1fb405c187399adcd3 and associated with the email account freejasonbourne@protonmail.com, maintained at premises controlled by Buffer, which is headquartered at 44 Tehama Street, San Francisco, California 94105, contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, Buffer is hereby directed to provide to the Investigative Agency, within three days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A which shall not be transmitted to the Provider. The Government is required to serve a copy of

JAS_021329

this Warrant and Order on Buffer within one day of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which Google is capable of accepting service.

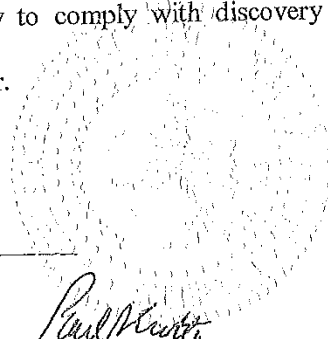
2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, danger to the physical safety of an individual, flight from prosecution, and/or intimidation of potential witnesses or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that Buffer shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of 30 days from the date of this Order, subject to extension upon application to the Court if necessary, except that Buffer may disclose this Warrant and Order to an attorney for Buffer for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on Buffer; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

10/24/2017
Date Issued

10³⁰ am
Time Issued


Paul A. Crotty
THE HONORABLE PAUL A. CROTTY
United States District Judge
Southern District of New York

Attachment A

I. The Target Accounts and Execution of Warrant

This warrant is directed to Buffer, Inc. (“Buffer” or the “Provider”) and applies to all content and other information within Buffer’s possession, custody, or control that is associated with the account with the user identification number 5b8c7b1fb405c187399adcd3 and associated with the email account freejasonbourne@protonmail.com (the “**Target Account**”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to Buffer. Buffer is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, a copy of which shall not be transmitted to the Provider.

II. Information to be Produced by Buffer

To the extent within the Provider’s possession, custody, or control, the Provider is directed to produce the following information, from December 1, 2017 to present, associated with each **Target Account**:

a. *Message content.* All messages sent to or from, stored in draft form in, or otherwise associated with the **Target Account**, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each message, the date and time at which each message was sent, and the size and length of each message).

b. *Images and Videos.* All pictures and videos posted and/or stored by an individual using the account, including metadata and geotags.

d. *Other Stored Electronic Information.* All records and other information stored by the **Target Account's** user(s).

e. *Subscriber and Payment Information.* All subscriber and payment information regarding the **Target Account**, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

f. *Transactional Records.* All transactional records associated with the **Target Account**, including any IP logs or other records of session times and durations.

g. *Customer Correspondence.* All correspondence with the subscriber or others associated with the **Target Account**, including complaints, inquiries, or other contacts with support services and records of actions taken.

h. *Preserved Records.* Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of a scheme to disseminate classified and otherwise protected information, including through the use of contraband cellphones, software, and other devices, in violation of 18 U.S.C. §§ 401 (contempt of court), 793 (unlawful disclosure of classified information); 1030 (unauthorized computer access), 1503 and 1512 (obstruction of justice), 1791 (smuggling contraband into a federal detention facility) and 2252A (illegal acts related to child pornography);

as well as conspiracies and attempts to violate these provisions and aiding and abetting these offenses, among other statutes (the "Subject Offenses"), including the following:

- a. Evidence of the identity(ies) of the user(s) of the **Target Account** and any and all cellphones ("Contraband Cellphones") smuggled into the Metropolitan Correctional Center in New York, New York (the "MCC") for Joshua Schulte or Omar Amanat, as well as other coconspirators in contact with the **Target Account** or the Contraband Cellphones;
- b. Evidence relating to the geolocation of the users of the **Target Account** or the Contraband Cellphones at times relevant to the Subject Offenses;
- c. Evidence relating to the participation in the Subject Offenses by Schulte, Amanat, and others using or in communication with the **Target Account** or the Contraband Cellphones;
- d. Evidence concerning financial institutions and transactions used by the users of the **Target Account** in furtherance of the Subject Offenses;
- e. Communications evidencing the Subject Offenses;
- f. Evidence of and relating to computers or other online accounts and facilities (such as additional email addresses) controlled or maintained by the user(s) of the Contraband Cellphones or **Target Account**; and
- g. Passwords or other information needed to access any such computers, accounts, or facilities.

18 MAG 9130

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE APPLICATION OF
THE UNITED STATES OF AMERICA FOR A
SEARCH WARRANT FOR INFORMATION AND
DATA ASSOCIATED WITH THE FACEBOOK
ACCOUNT WITH THE USER IDENTIFICATION
NUMBER 225303401359184; STORED AT
PREMISES CONTROLLED BY FACEBOOK, INC.

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Facebook, Inc. ("Facebook")

The Federal Bureau of Investigation (the "FBI" or the "Investigative Agency")

1. **Warrant.** Upon an affidavit of Special Agent Jeff D. Donaldson of the FBI and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. §§ 2703(b)(1)(A) and 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds that there is probable cause to believe the Facebook account with the user identification number 225303401359184, maintained at premises controlled by Facebook, which is headquartered at 1 Hacker Way, Menlo Park, California 94025, contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, Facebook is hereby directed to provide to the Investigative Agency, within three days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A which shall not be transmitted to the Provider. The Government is required to serve a copy of this Warrant and Order on Facebook within one day of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which Facebook is capable of accepting service.

JAS_021334

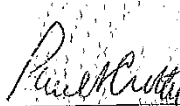
2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, danger to the physical safety of an individual, flight from prosecution, and/or intimidation of potential witnesses or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that Facebook shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of 30 days from the date of this Order, subject to extension upon application to the Court if necessary, except that Facebook may disclose this Warrant and Order to an attorney for Facebook for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on Facebook; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

16/26/2018
Date Issued

10:30 AM
Time Issued



THE HONORABLE PAUL A. CROTTY
United States District Judge
Southern District of New York

Attachment A

I. The Target Accounts and Execution of Warrant

This warrant is directed to Facebook, Inc. ("Facebook" or the "Provider") and applies to all content and other information within Facebook's possession, custody, or control that is associated with the account with the user identification number 225303401359184 (the "**Target Account**").

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to Facebook. Facebook is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, a copy of which shall not be transmitted to the Provider.

II. Information to be Produced by Facebook

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information, from December 1, 2017 to present, associated with each **Target Account**:

a. *Message Content*. All messages sent to or from, stored in draft form in, or otherwise associated with the **Target Account**, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each message, the date and time at which each message was sent, and the size and length of each message).

b. *Images and Videos*. All pictures and videos posted and/or stored by an individual using the account, including metadata and geotags.

c. *Address Book Information.* All friend list, address book, contact list, or similar information associated with the Target Account.

d. *Other Stored Electronic Information.* All records and other information stored by the **Target Account's** user(s), including but not limited to Facebook "wall" postings.

e. *Subscriber and Payment Information.* All subscriber and payment information regarding the **Target Account**, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

f. *Transactional Records.* All transactional records associated with the **Target Account**, including any IP logs or other records of session times and durations.

g. *Customer Correspondence.* All correspondence with the subscriber or others associated with the **Target Account**, including complaints, inquiries, or other contacts with support services and records of actions taken.

h. *Preserved Records.* Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of a scheme to disseminate classified and otherwise protected information, including through the use of contraband cellphones, software, and other devices, in violation of 18 U.S.C. §§ 401 (contempt of court), 793 (unlawful disclosure of classified information); 1030 (unauthorized computer access), 1503 and 1512 (obstruction of justice), 1791 (smuggling

contraband into a federal detention facility) and 2252A (illegal acts related to child pornography); as well as conspiracies and attempts to violate these provisions and aiding and abetting these offenses, among other statutes (the “Subject Offenses”), including the following:

- a. Evidence of the identity(ies) of the user(s) of the **Target Account** and any and all cellphones (“Contraband Cellphones”) smuggled into the Metropolitan Correctional Center in New York, New York (the “MCC”) for Joshua Schulte or Omar Amanat, as well as other coconspirators in contact with the **Target Account** or the Contraband Cellphones;
- b. Evidence relating to the geolocation of the users of the **Target Account** or the Contraband Cellphones at times relevant to the Subject Offenses;
- c. Evidence relating to the participation in the Subject Offenses by Schulte, Amanat, and others using or in communication with the **Target Account** or the Contraband Cellphones;
- d. Evidence concerning financial institutions and transactions used by the users of the **Target Account** in furtherance of the Subject Offenses;
- e. Communications evidencing the Subject Offenses;
- f. Evidence of and relating to computers or other online accounts and facilities (such as additional email addresses) controlled or maintained by the user(s) of the Contraband Cellphones or **Target Account**; and
- g. Passwords or other information needed to access any such computers, accounts, or facilities.

18 MAG 9 130

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE APPLICATION OF
THE UNITED STATES OF AMERICA FOR A
SEARCH WARRANT FOR INFORMATION AND
DATA ASSOCIATED WITH THE EMAIL
ACCOUNTS JOSHSCULTE1@GMAIL.COM,
FREEJASONBOURNE@GMAIL.COM,
JOHN12GALT21@GMAIL.COM; STORED AT
PREMISES CONTROLLED BY GOOGLE, INC.

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Google, Inc. ("Google")

The Federal Bureau of Investigation (the "FBI" or the "Investigative Agency")

1. **Warrant.** Upon an affidavit of Special Agent Jeff D. Donaldson of the FBI and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. §§ 2703(b)(1)(A) and 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds that there is probable cause to believe the email accounts **joshschulte1@gmail.com, freejasonbourne@gmail.com, and john12galt21@gmail.com,** maintained at premises controlled by Google, Inc., which is headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043, contain evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, Google is hereby directed to provide to the Investigative Agency, within three days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A which shall not be transmitted to the Provider. The Government is required to serve a copy of this Warrant and Order on Google within one day of the date of issuance. The Warrant and Order may be served

JAS_021339

via electronic transmission or any other means through which Google is capable of accepting service.

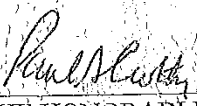
2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, danger to the physical safety of an individual, flight from prosecution, and/or intimidation of potential witnesses or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that Google shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of 30 days from the date of this Order, subject to extension upon application to the Court if necessary, except that Google may disclose this Warrant and Order to an attorney for Google for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on Google; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

10/26/2018
Date Issued

10 30 AM
Time Issued



THE HONORABLE PAUL A. CROTTY
United States District Judge
Southern District of New York

Attachment A

I. The Target Accounts and Execution of Warrant

This warrant is directed to Google, Inc. (“Google” or the “Provider”) and applies to all content and other information within Google’s possession, custody, or control that is associated with the following accounts (the “Target Accounts”):

joshschulte1@gmail.com,
freejasonbourne@gmail.com, and
john12galt21@gmail.com,

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to Google. Google is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, a copy of which shall not be transmitted to the Provider.

II. Information to be Produced by Google

To the extent within the Provider’s possession, custody, or control, the Provider is directed to produce the following information, from May 8, 2017 to present, associated with each **Target Accounts**:

a. *Email Content.* All emails sent to or from, stored in draft form in, or otherwise associated with the **Target Accounts**, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email);

b. *Subscriber and Payment Information.* All subscriber and payment information regarding the **Target Accounts**, including Google Payments information associated with the **Target Accounts**, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services used, means and source of payment, and payment history.

c. *Address Book Information.* All address book, contact list, or similar information associated with the **Target Accounts**.

d. *Photos and Videos.* All videos uploaded by the user of the **Target Accounts**, whether publicly displayed or not, and all associated metadata.

e. *Playlists and Channels.* All playlists, channels followed, discussions, and postings, whether public or private, and all associated metadata, relating to the **Target Accounts**.

f. *Transactional Records.* All transactional records associated with the **Target Accounts**, including any IP logs or other records of session times and durations.

g. *Search History.* All search history associated with the **Target Accounts**.

h. *Cookies.* Any and all cookies associated with or used by any computer or web browser associated with the **Target Accounts**, including the IP addresses, dates, and times associated with the recognition of any such cookie.

i. *Customer correspondence.* All correspondence with the subscriber(s) or others associated with the **Target Accounts**, including complaints, inquiries, or other contacts with support services and records of actions taken.

j. *Google Drive, PlusOne, and Google Plus.* All information associated with these services, including the names of all Circles and the accounts grouped into them.

k. *Location History*. All location information associated with the **Target Accounts**.

l. *Linked Accounts*. All accounts linked to the **Target Accounts** (including where linked by machine cookie or other cookie, creation or login IP address, recovery email or phone number, AOL account ID, Android ID, Google ID, SMS, Apple ID, or otherwise).

m. *Google Docs*. All Google Docs data associated with the **Target Accounts**.

n. *Google Calendar*. All Google Calendar data associated with the Target Account

o. *Preserved Records*. Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of a scheme to disseminate classified and otherwise protected information, including through the use of contraband cellphones, software, and other devices, in violation of 18 U.S.C. §§ 401 (contempt of court), 793 (unlawful disclosure of classified information), 1030 (unauthorized computer access), 1503 and 1512 (obstruction of justice), and 1791 (smuggling contraband into a federal detention facility) and 2252A (illegal acts related to child pornography); as well as conspiracies and attempts to violate these provisions and aiding and abetting these offenses, among other statutes (the "Subject Offenses"), including the following:

a. Evidence of the identity(ies) of the user(s) of the **Target Accounts** and any and all cellphones ("Contraband Cellphones") smuggled into the Metropolitan Correctional Center in

New York, New York (the "MCC") for Joshua Schulte or Omar Amanat, as well as other co-conspirators in contact with the **Target Accounts** or the Contraband Cellphones;

b. Evidence relating to the geolocation of the users of the **Target Accounts** or the Contraband Cellphones at times relevant to the Subject Offenses;

c. Evidence relating to the participation in the Subject Offenses by Schulte, Amanat, and others using or in communication with the **Target Accounts** or the Contraband Cellphones;

d. Evidence concerning financial institutions and transactions used by the users of the **Target Accounts** in furtherance of the Subject Offenses;

e. Communications evidencing the Subject Offenses;

f. Evidence of and relating to computers or other online accounts and facilities (such as additional email addresses) controlled or maintained by the user(s) of the Contraband Cellphones or **Target Accounts**; and

g. Passwords or other information needed to access any such computers, accounts, or facilities.

18 MAG 9130

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE APPLICATION OF
THE UNITED STATES OF AMERICA FOR A
SEARCH WARRANT FOR INFORMATION AND
DATA ASSOCIATED WITH THE TWITTER
ACCOUNT @FREEJASONBOURNE; STORED AT
PREMISES CONTROLLED BY TWITTER, INC.

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Twitter, Inc. ("Twitter")

The Federal Bureau of Investigation (the "FBI" or the "Investigative Agency")

1. **Warrant.** Upon an affidavit of Special Agent Jeff D. Donaldson of the FBI and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. §§ 2703(b)(1)(A) and 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds that there is probable cause to believe the Twitter account @freejasonbourne, maintained at premises controlled by Twitter, which is headquartered at 1355 Market Street, Suite 900, San Francisco, California 94103, contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, Twitter is hereby directed to provide to the Investigative Agency, within three days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A which shall not be transmitted to the Provider. The Government is required to serve a copy of this Warrant and Order on Twitter within one day of the date of issuance. The Warrant and Order may be served

JAS_021430

via electronic transmission or any other means through which Twitter is capable of accepting service.

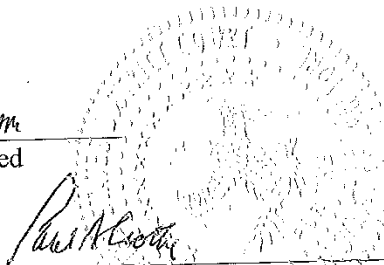
2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, danger to the physical safety of an individual, flight from prosecution, and/or intimidation of potential witnesses or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that Twitter shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of 30 days from the date of this Order, subject to extension upon application to the Court if necessary, except that Twitter may disclose this Warrant and Order to an attorney for Twitter for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on Twitter; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

10/26/18
Date Issued

10 30 am
Time Issued



Paul A. Crotty
THE HONORABLE PAUL A. CROTTY
United States District Judge
Southern District of New York

Attachment A

I. The Target Account and Execution of Warrant

This warrant is directed to Twitter, Inc. (“Twitter” or the “Provider”) and applies to all content and other information within Twitter’s possession, custody, or control that is associated with the account @freejasonbourne (the “**Target Account**”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to Twitter. Twitter is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, a copy of which shall not be transmitted to the Provider.

II. Information to be Produced by Twitter

To the extent within the Provider’s possession, custody, or control, the Provider is directed to produce the following information, from December 1, 2017 to present, associated with the **Target Account**:

a. *Profile Information.* Any personal profile page information, including but not limited to biographical entries, photographs, and location information for the user of the **Target Account**.

b. *Tweet Information.* Any tweets and related information, including any “favorite” or “retweet” information, any “mentions,” any lists in the “Connect” tab of other users who have responded to any tweets from the **Target Account**, and “Tweet With Location” information.

c. *Photographs/Images*. Any photographs or images associated with the **Target Account**, including any galleries of photographs or images shared by the **Target Account**, even if those photographs or images were uploaded from another service.

d. *Link Information*. Any websites to which the **Target Account** has linked, as well as any information concerning how often those links have been clicked.

e. *Associated Users*. Any lists of other users who are “following” or who are “followed” by each Subject Account, any groups of users or “lists” that the **Target Account** follows or is followed by, and any recommendations of users to follow, such as any “Who To Follow” lists.

f. *Direct Messages*. Any direct messages sent to or by the **Target Account**, and any related information.

g. *Subscriber and Billing Information*. Any records (1) showing identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses; (2) concerning the date on which the account was created, the IP address of the user at the time of account creation, the current status of the account (e.g., active or closed), the length of service, and the types of services used by the subscriber; and (3) reflecting the subscriber’s means and source of payment, including any credit card or bank account number.

h. *Search Information*. Any records concerning searches performed by the **Target Account**.

i. *Third-party Information*. Any records reflecting third-party websites with which the **Target Account** is connected.

j. *Transactional Information.* Any records of transactional information about the use of the **Target Account** on its system, including records of login (i.e., session) times and durations and the methods used to connect to the account (such as logging into the account through the Provider's website).

k. *Customer Correspondence.* Any records of any customer-service contacts with or about the subscribers, including any inquiries or complaints concerning the subscriber's account.

l. *Preserved Records.* Any preserved copies of the foregoing categories of records with respect to the **Target Account**.

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of a scheme to disseminate classified and otherwise protected information, including through the use of contraband cellphones, software, and other devices, in violation of 18 U.S.C. §§ 401 (contempt of court), 793 (unlawful disclosure of classified information); 1030 (unauthorized computer access), 1503 and 1512 (obstruction of justice), 1791 (smuggling contraband into a federal detention facility) and 2252A (illegal acts related to child pornography); as well as conspiracies and attempts to violate these provisions and aiding and abetting these offenses, among other statutes (the "Subject Offenses"), including the following:

a. Evidence of the identity(ies) of the user(s) of the **Target Account** and any and all cellphones ("Contraband Cellphones") smuggled into the Metropolitan Correctional Center in

New York, New York (the "MCC") for Joshua Schulte or Omar Amanat, as well as other coconspirators in contact with the **Target Account** or the Contraband Cellphones;

b. Evidence relating to the geolocation of the users of the **Target Account** or the Contraband Cellphones at times relevant to the Subject Offenses;

c. Evidence relating to the participation in the Subject Offenses by Schulte, Amanat, and others using or in communication with the **Target Account** or the Contraband Cellphones;

d. Evidence concerning financial institutions and transactions used by the users of the **Target Account** in furtherance of the Subject Offenses;

e. Communications evidencing the Subject Offenses;

f. Evidence of and relating to computers or other online accounts and facilities (such as additional email addresses) controlled or maintained by the user(s) of the Contraband Cellphones or **Target Account**; and

g. Passwords or other information needed to access any such computers, accounts, or facilities.