EXHIBIT 1

F I L E

JUN I 0 2013

CLERK, U.S. DISTRICT COURT

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

MISC. NO. 1:13 EC 354

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 Lavabit LLC, an electronic communications

service provider and/or a remote computing service located in Dallas, TX, 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 Lavabit LLC

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 Lavabit LLC 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 Lavabit LLC may disclose this Order to an attorney for Lavabit LLC 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

June 10, 2013
Date

2

ATTACHMENT A

I.   The Account(s)

The Order applies to certain records and information associated with the following email account(s): ████████████████████████

II.   Records and Other Information to Be Disclosed

Lavabit LLC 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 inception 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 the registration Internet Protocol ("IP") address); 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 Lavabit LLC, and my official title is _____. I am a custodian of records for Lavabit LLC. 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 Lavabit LLC, 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 Lavabit LLC; and

    c.   such records were made by Lavabit LLC 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

EXHIBIT 2

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING THE) (Under Seal)
INSTALLATION AND USE OF A PEN)
REGISTER/TRAP AND TRACE DEVICE) 1:13 EC ᗁᑫ˥
ON AN ELECTRONIC MAIL ACCOUNT)

ORDER

This matter having come before the Court pursuant to an Application under 18 U.S.C.

§ 3122, by ▮▮▮▮▮▮▮, Assistant United States Attorney, an attorney for the Government

as defined by Fed. R. Crim. P. 1(b)(1), requesting an Order under 18 U.S.C. § 3123, authorizing

the installation and use of a pen register and the use of a trap and trace device or process

("pen/trap device") on all electronic communications being sent from or sent to the account

associated with ▮▮▮▮▮▮▮ that is registered to subscriber ▮▮▮▮▮ at

Lavabit, LLC (hereinafter referred to as the "SUBJECT ELECTRONIC MAIL ACCOUNT").

The Court finds that the applicant has certified that the information likely to be obtained by such

installation and use is relevant to an ongoing criminal investigation into possible violation(s) of

18 U.S.C. §§ 641, 793(d)-(e), and 798(a)(3) by ▮▮▮▮▮▮▮.

IT APPEARING that the information likely to be obtained by the pen/trap device is

relevant to an ongoing criminal investigation of the specified offense;

IT IS ORDERED, pursuant to 18 U.S.C. § 3123, that a pen/trap device may be installed

and used by Lavabit and the Federal Bureau of Investigation to capture all non-content dialing,

routing, addressing, and signaling information (as described and limited in the Application), sent

from or sent to the SUBJECT ELECTRONIC MAIL ACCOUNT, to record the date and time of

the initiation and receipt of such transmissions, to record the duration of the transmissions, and to

record user log-in data (date, time, duration, and Internet Protocol address of all log-ins) on the

1

SUBJECT ELECTRONIC MAIL ACCOUNT, all for a period of sixty (60) days from the date of such Order or the date the monitoring equipment becomes operational, whichever occurs later;

IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 3123(b)(2), that Lavabit shall furnish agents from the Federal Bureau of Investigation, forthwith, all information, facilities, and technical assistance necessary to accomplish the installation and use of the pen/trap device unobtrusively and with minimum interference to the services that are accorded persons with respect to whom the installation and use is to take place;

IT IS FURTHER ORDERED that the United States take reasonable steps to ensure that the monitoring equipment is not used to capture any "Subject:" portion of an electronic mail message, which could possibly contain content;

IT IS FURTHER ORDERED that Lavabit shall be compensated by the Federal Bureau of Investigation for reasonable expenses incurred in providing technical assistance;

IT IS FURTHER ORDERED that, in the event that the implementing investigative agency seeks to install and use its own pen/trap device on a packet-switched data network of a public provider, the United States shall ensure that a record is maintained which will identify: (a) any officer(s) who installed the device and any officer(s) who accessed the device to obtain information from the network; (b) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information; (c) the configuration of the device at the time of its installation and any subsequent modification thereof; and (d) any information which has been collected by the device. To the extent that the pen/trap device can be set to automatically record this information electronically, the record shall be maintained electronically throughout the installation and use of the pen/trap device. Pursuant to 18 U.S.C. § 3123(a)(3)(B), as amended, such record(s) shall be provided ex parte and under seal to this Court within 30 days of the termination of this Order, including any extensions thereof;

IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 3123(d), that this Order and the Application be sealed until otherwise ordered by the Court, and that copies of such Order may be

2

furnished to the Federal Bureau of Investigation, the United States Attorney's Office, and Lavabit;

IT IS FURTHER ORDERED that Lavabit shall not disclose the existence of the pen/trap device, or the existence of the investigation to any person, except as necessary to effectuate this Order, unless or until otherwise ordered by the Court.
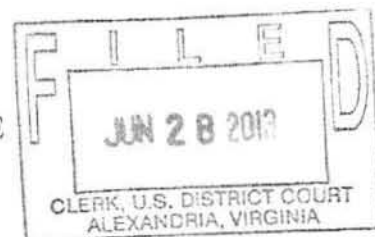
SO ORDERED:

/s/
Theresa Carroll Buchanan
United States Magistrate Judge

Hon. Theresa C. Buchanan
United States Magistrate Judge

Date: 6/28/13

EXHIBIT 3

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE APPLICATION)	
OF THE UNITED STATES OF AMERICA)	
FOR AN ORDER AUTHORIZING THE)	(Under Seal)
INSTALLATION AND USE OF A PEN)	
REGISTER/TRAP AND TRACE DEVICE)	1:13 EC 297
ON AN ELECTRONIC MAIL ACCOUNT)	

MOTION FOR ENTRY OF AN ORDER TO COMPEL

The United States, by and through its undersigned counsel, hereby requests the Court

enter an Order directing Lavabit, LLC, to comply with the Court's June 28, 2013 Pen

Register/Trap and Trace Order. In support of the motion the United States declares as follows:

1.   On June 28, 2013, at approximately 4 p.m., this Court entered an Order pursuant

to 18 U.S.C. § 3123 authorizing the installation and use of a pen register and the use of a trap and

trace device ("pen/trap device") on all electronic communications being sent from or sent to the

electronic mail account ████████████████. That e-mail account is controlled by Lavabit,

LLC.

2.   In its Order, the Court found that the information to be collected by the pen/trap

device would be relevant to an ongoing criminal investigation. In addition, the Court ordered

Lavabit "shall furnish agents from the Federal Bureau of Investigation, forthwith, all

information, facilities, and technical assistance necessary to accomplish the installation and use

of the pen/trap device."

3.   The Federal Bureau of Investigation served a copy of the Order on Lavabit that

same afternoon. A representative of Lavabit stated that it could not provide the requested

information because the user of the account had enabled Lavabit's encryption services, and thus

Lavabit would not provide the requested information. The representative of Lavabit indicated that Lavabit had the technical capability to decrypt the information but that Lavabit did not want to "defeat [its] own system."

4. The representative of Lavabit did not comply with the Order, and indicated he first wanted to seek legal advice.

5. The Pen Register and Trap and Trace Act gives this Court the authority to order a provider to assist the government in the execution of a lawful pen register or trap and trace order, including by providing information. Section 3122 of Title 18, United States Code, provides in part: "An order issued under this section-- ... shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under section 3124 of this title." Section 3124(a) provides, "Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire or electronic communication service... shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference... if such
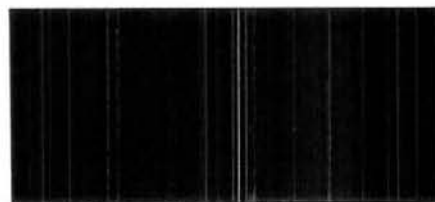
assistance is directed by a court order as provided in section 3123(b)(2) of this title." Section 3124(b) contains a similar provision governing trap and trace orders.

Wherefore, the United States requests an Order directing Lavabit to comply forthwith with the Court's June 28, 2013 Order.

Respectfully submitted,
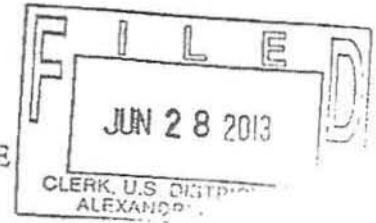NEIL H. MACBRIDE
United States Attorney

By:

Assistant United States Attorney

EXHIBIT 4

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE APPLICATION)	
OF THE UNITED STATES OF AMERICA)	
FOR AN ORDER AUTHORIZING THE)	(Under Seal)
INSTALLATION AND USE OF A PEN)	
REGISTER/TRAP AND TRACE DEVICE)	1:13 EC 297
ON AN ELECTRONIC MAIL ACCOUNT)	

ORDER COMPELLING COMPLIANCE FORTHWITH

WHEREAS, on June 28, 2013, at approximately 4:00 p.m., this Court entered an Order

pursuant to 18 U.S.C. § 3123 authorizing the installation and use of a pen register and the use of

a trap and trace device ("pen/trap device") on all electronic communications being sent from or

sent to the electronic mail account ██████████, which is an e-mail account

controlled by Lavabit, LLC ("Lavabit"); and

WHEREAS, this Court found that the information obtained by the pen/trap device would

be relevant to an ongoing criminal investigation; and

WHEREAS, the Court's Order directed that Lavabit "shall furnish agents from the

Federal Bureau of Investigation, forthwith, all information, facilities, and technical assistance

necessary to accomplish the installation and use of the pen/trap device;" and

WHEREAS, Lavabit informed the Federal Bureau of Investigation that the user of the

account had enabled Lavabit's encryption services and thus the pen/trap device would not collect

the relevant information; and

WHEREAS, Lavabit informed the FBI that it had the technological capability to obtain

the information but did not want to "defeat [its] own system;"

IT IS HEREBY ORDERED that Lavabit LLC is directed to comply forthwith with the Court's June 28, 2013 Order, and provide the Federal Bureau of Investigation with unencrypted data pursuant to the Order. To the extent any information, facilities, or technical assistance are under the control of Lavabit are needed to provide the FBI with the unencrypted data, Lavabit shall provide such information, facilities, or technical assistance forthwith.

Failure to comply with this Order shall subject Lavabit to any penalty within the power of the Court, including the possibility of criminal contempt of Court. TCB
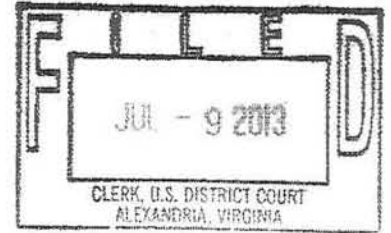
SO ORDERED.   6/28/13

_____
for
Theresa Carroll Buchanan
United States Magistrate Judge
Hon. Theresa C. Buchanan
United States Magistrate Judge

EXHIBIT 5

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE
APPLICATION OF THE UNITED
STATES OF AMERICA FOR AN ORDER
AUTHORIZING THE USE OF A PEN
REGISTER/TRAP AND TRACE DEVICE
ON AN ELECTRONIC MAIL ACCOUNT

)
)
)
)
)
)
)

FILED UNDER SEAL

No. 1:13EC297

**MOTION OF THE UNITED STATES
FOR AN ORDER TO SHOW CAUSE**

The United States, through the undersigned counsel, pursuant to Title 18, United States

Code, Section 401, hereby moves for the issuance of an order directing Ladar Levison, the owner

and operator of Lavabit LLC, an electronic communications service provider, to show cause why

Lavabit LLC has failed to comply with the orders entered June 28, 2013, in this matter and, as a

result, why this Court should not hold Mr. Levison and Lavabit LLC in contempt for its

disobedience and resistence to these lawful orders. The United States further requests that the

Court convene a hearing on this motion on July 16, 2013, at 10:00 a.m., and issue a summons

directing Mr. Levison to appear before this Court on that date. In support of this motion, the

United States represents:

1.   The United States is conducting a criminal investigation of ███████████

2. [REDACTED] On June 10, 2013, the United States obtained

an order pursuant to 18 U.S.C. § 2703(d) directing Lavabit LLC to provide, within ten days,

additional records and information about [REDACTED] email account. Mr. Levison received that

order on June 11, 2013. Mr. Levison responded by mail, which was not received by the

government until June 27, 2013. Mr. Levison provided very little of the information sought by

the June 10, 2013 order.

3.   On June 28, 2013, the United States obtained a pen register/trap and trace order on

[REDACTED] email account, a copy of which is attached together with the application for that

order.

4.   On June 28, 2013, FBI special agents met Mr. Levison at his residence in Dallas,

Texas, and discussed the prior grand jury subpoena served on Lavabit LLC and the pen register

order entered that day. Mr. Levison did not have a copy of the order when he spoke with the

agents, but he received a copy from the FBI within a few minutes of their conversation. Mr.

Levison told the agents that he would not comply with the pen register order and wanted to speak

to an attorney. It was unclear whether Mr. Levison would not comply with the order because it

was technically not feasible or difficult or because it was not consistent with his business practice

of providing secure, encrypted email service for his customers.

5.   On June 28, 2013, after this conversation with Mr. Levison, the United States obtained an Order Compelling Compliance Forthwith, which directed Lavabit to comply with the pen register order. Copies of that motion and order are attached.

6.   Since June 28, 2013, the FBI has made numerous attempts, without success, to speak and meet directly with Mr. Levison to discuss the pen register order and his failure to provide "all information, facilities, and technical assistance necessary to accomplish the installation and use of the pen/trap device" as required by that order. As of this date, Lavabit LLC has not complied with the order.

7.   The United States requests that the Court enter the attached proposed order directing Mr. Levison to show cause why Lavabit LLC has failed to comply with the pen register order and why, therefore, he should not be held in contempt. The United States requests that this show cause hearing be scheduled for July 16, 2013, at 10:00 a.m., and that a summons be issued directing Mr. Levison to appear before this Court on that date.

8.   The June 10, 2013 Section 2703(d) Order and the June 28, 2013 pen register order remain under seal. In addition, these orders provide that Lavabit LLC shall not disclose the existence of the governemnt's applications and the orders to the subscriber ▆▆▆▆ or to any other persons unless otherwise authorized to do so by court order, except that Lavabit LLC may disclose the orders to an attorney for the purpose of obtaining legal advice regarding these orders. The United States requests that these documents remain under seal, that the non-disclosure

provisions of the orders remain in effect, and that this motion and order and any subsequent

pleadings and/or proceedings regarding this motion also be sealed.

Respectfully submitted,

Neil H. MacBride
United States Attorney

By:

United States Attorney's Office
Justin W. Williams U.S. Attorney's Building
2100 Jamieson Avenue
Alexandria, Virginia 22314
Phone: 703-299-3700

PROPOSED
ORDER TO SHOW CAUSE

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE	) **UNDER SEAL**
APPLICATION OF THE UNITED	)
STATES OF AMERICA FOR AN ORDER	) No. 1:13EC297
AUTHORIZING THE USE OF A PEN	)
REGISTER/TRAP AND TRACE DEVICE	)
ON AN ELECTRONIC MAIL ACCOUNT	)

ORDER TO SHOW CAUSE

Upon motion of the United States pursuant to Title 18, United States Code, Section 401, good cause having been shown, IT IS HEREBY ORDERED:

1.   Ladar Levison, the owner and operator of Lavabit LLC, an electronic communications service provider, shall appear before this Court on July 16, 2013, at 10:00 a.m., at which time he shall show cause why Lavabit LLC has failed to comply with the orders entered June 28, 2013, in this matter and why this Court should not hold Mr. Levison and Lavabit LLC in contempt for its disobedience and resistence to these lawful orders;

2.   The Clerk's Office shall issue a summons for the appearance of Mr. Levison on July 16, 2013, at 10:00 a.m. The Clerk's Office shall provide the Federal Bureau of Investigation with a certified copy of the summons for service on Mr. Levison and Lavabit LLC.

3.   The Federal Bureau of Investigation shall serve the summons on Mr. Levison together with a copy of the Motion of the United States for an Order to Show Cause and a certified copy of this Order to Show Cause.

4.   The sealing and non-disclosure provisions of the June 10, 2013 Section 2703(d) order and the June 28, 2013 pen register order shall remain in full force and effect. Mr. Levison

and Lavabit LLC shall not disclose the existence of these applications, motions, and court orders, including this Order to Show Cause, to the subscriber or to any other persons unless otherwise authorized to do so by court order, except that Lavabit LLC may disclose the orders to an attorney for the purpose of obtaining legal advice regarding these orders.

5.   This Order, the Motion of the United States for an Order to Show Cause, and any subsequent pleadings and proceedings regarding this matter shall be placed under seal until further order of this Court.

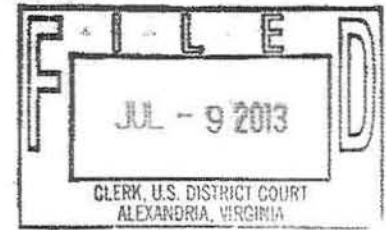Entered in Alexandria, Virginia, this _____ day of July, 2013

_____
Claude M. Hilton
United States District Judge

EXHIBIT 6

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE) **UNDER SEAL**
APPLICATION OF THE UNITED)
STATES OF AMERICA FOR AN ORDER) No. 1:13EC297
AUTHORIZING THE USE OF A PEN)
REGISTER/TRAP AND TRACE DEVICE)
ON AN ELECTRONIC MAIL ACCOUNT)

ORDER TO SHOW CAUSE

Upon motion of the United States pursuant to Title 18, United States Code, Section 401, good cause having been shown, IT IS HEREBY ORDERED:

1.   Ladar Levison, the owner and operator of Lavabit LLC, an electronic communications service provider, shall appear before this Court on July 16, 2013, at 10:00 a.m., at which time he shall show cause why Lavabit LLC has failed to comply with the orders entered June 28, 2013, in this matter and why this Court should not hold Mr. Levison and Lavabit LLC in contempt for its disobedience and resistence to these lawful orders;

2.   The Clerk's Office shall issue a summons for the appearance of Mr. Levison on July 16, 2013, at 10:00 a.m. The Clerk's Office shall provide the Federal Bureau of Investigation with a certified copy of the summons for service on Mr. Levison and Lavabit LLC.

3.   The Federal Bureau of Investigation shall serve the summons on Mr. Levison together with a copy of the Motion of the United States for an Order to Show Cause and a certified copy of this Order to Show Cause.

4.   The sealing and non-disclosure provisions of the June 10, 2013 Section 2703(d) order and the June 28, 2013 pen register order shall remain in full force and effect. Mr. Levison

and Lavabit LLC shall not disclose the existence of these applications, motions, and court orders, including this Order to Show Cause, to the subscriber or to any other persons unless otherwise authorized to do so by court order, except that Lavabit LLC may disclose the orders to an attorney for the purpose of obtaining legal advice regarding these orders.

5.   This Order, the Motion of the United States for an Order to Show Cause, and any subsequent pleadings and proceedings regarding this matter shall be placed under seal until further order of this Court.

Entered in Alexandria, Virginia, this _9th_ day of July, 2013

Claude M. Hilton
United States District Judge

- 2 -

EXHIBIT 7

UNITED STATES DISTRICT COURT
for the
Eastern District of Virginia

United States of America	)	
v.	)	
	)	
Ladar Levison	)	Case No. 1:13ec297
	)	
	)	
Defendant	)	

UNDER SEAL

SUMMONS IN A CRIMINAL CASE

YOU ARE SUMMONED to appear before the United States district court at the time, date, and place set forth below to answer to one or more offenses or violations based on the following document filed with the court:

☐ Indictment ☐ Superseding Indictment ☐ Information ☐ Superseding Information ☐ Complaint
☐ Probation Violation Petition ☐ Supervised Release Violation Petition ☐ Violation Notice ☒ Order of Court

Place:	401 Courthouse Square Alexandria, VA 22314	Courtroom No.:	800- Judge Hilton
		Date and Time:	7/16/13 @ 10:00 am

This offense is briefly described as follows:

See Attached Order

Date: _____07/09/2013_____

_____
Issuing officer's signature

███████████ – Deputy Clerk
Printed name and title

I declare under penalty of perjury that I have:

☐ Executed and returned this summons   ☐ Returned this summons unexecuted

Date: _____

A TRUE COPY, TESTE:
CLERK, U.S. DISTRICT COURT

███████████████████████
DEPUTY CLERK

_____
Printed name and title

EXHIBIT 8

13-1 / 13GJ2527 / 13 - 2451

United States District Court
for the
Eastern District of Virginia

SUBPOENA TO TESTIFY BEFORE THE GRAND JURY

TO: Ladar Norman Levison

██████████████████████████

Dallas, TX 75204

YOU ARE COMMANDED to appear and testify before the United States district court at the time, date, and place shown below to tesify before the court's grand jury. When you arrive, you must remain at the court until the judge or a court officer allows you to leave.

Place:	UNITED STATES DISTRICT COURT 401 Courthouse Square Alexandria, Virginia 22314	Date and Time:	July 16, 2013	9:30 AM

You must also bring with you the following documents, electronically stored information, or objects (blank if not applicable):

In addition to your personal appearance, you are directed to bring to the grand jury the public and private encryption keys used by lavabit.com in any SSL (Secure Socket Layer) or TLS (Transport Security Layer) sessions, including HTTPS sessions with clients using the lavabit.com web site and encrypted SMTP communications (or Internet communications using other protocols) with mail servers;

Any other information necessary to accomplish the installation and use of the pen/trap device ordered by Judge Buchanan on June 28, 2013, unobtrusively and with minimum interference to the services that are accorded persons with respect to whom the installation and use is to take place;

If such information is electronically stored or unable to be physically transported to the grand jury, you may provide a copy of the information to the Federal Bureau of Investigation. Provision of this information to the FBI does not excuse your personal appearance.

Date: July 11, 2013   CLERK OF COURT

                                                    ████████████████████████

                                                    _____
                                                    Signature of the Clerk or Deputy Clerk

The name, address, email, and telephone number of the United States attorney, or assistant United States attorney, who requests this subpoena, are:

████████████████████

Office of the United States Attorney
Justin W. Williams United States Attorney's Building
2100 Jamieson Avenue
Alexandria, Virginia 22314 (703) 299-3700

PROOF OF SERVICE

This subpoena for (name of individual or organization) Ladar Narman Levison
was received by me on (date) July 11, 2013   .

☒ I personally served the subpoena on the individual at (place) ███████████████
    Dallas, Texas   on (date) July 11, 2013   ; or

☐ I left the subpoena at the individual's residence or usual place of abode with (name)
    _____ , a person of suitable age and discretion who resides there, on
    (date)_____ , and mailed a copy to the individual's last known address; or

☐ I served the subpoena on (name of inidividual)_____ , who is
    designated by law to accept service of process on behalf of (name of organization)
    _____ on (date) _____ ; or

☐ I returned the subpoena unexecuted because_____ ; or

☐ Other (specify):

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

Date: July 11, 20.3

████████████████████████████
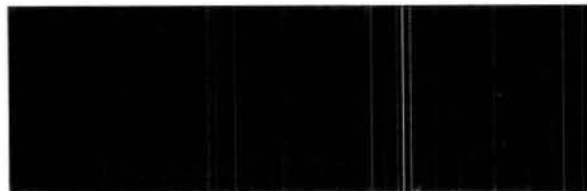
P.B.P. - Dallas
Server's address

Additional information regarding attempted services, etc:

EXHIBIT 9

UNDER SEAL   UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of	)
(Briefly describe the property to be searched or identify the person by name and address)	))
INFORMATION ASSOCIATED WITH ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮ THAT IS STORED AT PREMISES CONTROLLED BY LAVABIT, LLC	))))

Case No. 1:13SW522

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 _____Northern_____ District of _____Texas_____
(identify the person or describe the property to be searched and give its location):
See Attachment A

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

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 14 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
The Honorable Claude M. Hilton_____ .
                                  (name)

☐ 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: *July 16, 2013*   *Claude M. Hilton*
                                                                    Judge's signature

City and state: Alexandria, Virginia_____   ____The Honorable Claude M. Hilton, U.S. District Judge____
                                                                                                  Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with ███████████████ that is stored at premises controlled by Lavabit, LLC, a company that accepts service of legal process at ███████████████ Dallas, Texas, 75204.

ATTACHMENT B

Particular Things to be Seized

I.   Information to be disclosed by Lavabit, LLC (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

    a.   All information necessary to decrypt communications sent to or from the Lavabit e-mail account ███████████████ including encryption keys and SSL keys;

    b.   All information necessary to decrypt data stored in or otherwise associated with the Lavabit account ███████████

II.   Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. §§ ███████████████████, those violations involving ████████████ including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a.   All information necessary to decrypt communications sent to or from the Lavabit e-mail account ███████████████, including encryption keys and SSL keys;

b.   All information necessary to decrypt data stored in or otherwise associated with the Lavabit account ████████████████

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 Lavabit, LLC, and my

official title is _____. I am a custodian of records for Lavabit,

LLC. 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 Lavabit, LLC, 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 Lavabit, LLC; and

    c.   such records were made by Lavabit, LLC as a regular practice.

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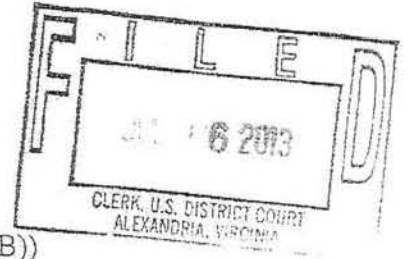
Rules of Evidence.

_____   _____

Date   Signature

EXHIBIT 10

UNDER SEAL

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

FILED

JUL 16 2013

CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

IN THE MATTER OF THE SEARCH OF)

INFORMATION ASSOCIATED WITH)

████████████████████████)

THAT IS STORED AT PREMISES)

CONTROLLED BY LAVABIT, LLC)

UNDER SEAL
(Local Rule 49(B))
No. 1:13sw522

ORDER TO SEAL

The UNITED STATES, pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, having moved to seal the application for a search warrant, the search warrant, the affidavit in support of the search warrant, the Motion to Seal, and proposed Order in this matter; and

The COURT, having considered the government's submissions, including the facts presented by the government to justify sealing; having found that revealing the material sought to be sealed would jeopardize an ongoing criminal investigation; having considered the available alternatives that are less drastic than sealing, and finding none would suffice to protect the government's legitimate interest in concluding the investigation; and having found that this legitimate government interest outweighs at this time any interest in the disclosure of the material; it is hereby

ORDERED, ADJUDGED, and DECREED that, the application for search warrant, the search warrant, the affidavit in support of the search warrant, Motion to Seal, and this Order be sealed until further Order by the Court. It is further ordered that law enforcement officers may serve a copy of the warrant on the occupant of the premises as required by Rule 41 of the Fed. R. of Crim. Proc.

Date: July 16, 2013
Alexandria, Virginia

Claude M. Hilton
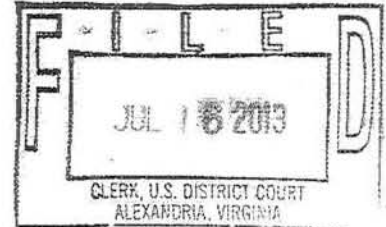The Honorable Claude M. Hilton
United States District Judge

EXHIBIT 11

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

IN RE: APPLICATION OF THE UNITED
STATES OF AMERICA FOR AN ORDER
PURSUANT TO 18 U.S.C. § 2705(b)

Case No. 1:13SW522
Filed Under Seal

FILED

JUL 16 2013

CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

ORDER

The United States has submitted an application pursuant to 18 U.S.C. § 2705(b),

requesting that the Court issue an Order commanding Lavabit, an electronic communications

service provider and/or a remote computing service, not to notify any person (including the

subscribers or customers of the account(s) listed in the search warrant) of the existence of the

attached search warrant until further order of the Court.

The Court determines that there is reason to believe that notification of the existence of

the attached warrant 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).

IT IS THEREFORE ORDERED under 18 U.S.C. § 2705(b) that Lavabit shall not

disclose the existence of the attached search warrant, or this Order of the Court, to the listed

subscriber or to any other person, unless and until otherwise authorized to do so by the Court,

except that Lavabit may disclose the attached search warrant to an attorney for Lavabit for the

purpose of receiving legal advice.

IT IS FURTHER ORDERED that the application and this Order are sealed until

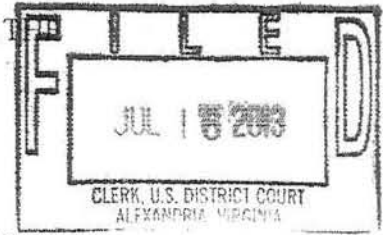otherwise ordered by the Court.

July 16, 2013
Date

Claude M. Hilton
The Honorable Claude M. Hilton
United States District Judge

EXHIBIT 12

IN THE UNITED STATES DISTRICT COURT FOR T̶H̶E̶

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE) **FILED UNDER SEAL**
APPLICATION OF THE UNITED)
STATES OF AMERICA FOR AN ORDER) No. 1:13EC297
AUTHORIZING THE USE OF A PEN)
REGISTER/TRAP AND TRACE DEVICE)
ON AN ELECTRONIC MAIL ACCOUNT)

SUPPLEMENT TO THE MOTION OF THE UNITED STATES
FOR AN ORDER TO SHOW CAUSE

The United States, through the undersigned counsel, submits the following additional

information in support of its show cause motion filed July 9, 2013:

1.   Following the issuance of the Court's Order to Show Cause, the government had a

meeting/conference call with Mr. Levison and his then counsel. Mr. Levison was in Dallas,

Texas, at the FBI field office, at the time, and his counsel from San Francisco, California, and

prosecutors and FBI agents from the Washington, D.C. field office participated by telephone. The

conference call was convened to discuss Mr. Levison's questions and concerns about the

installation and operation of a pen register on the targeted email account. Mr. Levison's

concerns focused primarily on how the pen register device would be installed on the Lavabit LLC

system, what data would be captured by the device, what data would be viewed and preserved by

the government. The parties also discussed whether Mr. Levison would be able to provide

"keys" for encrypted information.

2.   During the conference call, the FBI explained to Mr. Levison that the pen register

could be installed with minimal impact to the Lavabit LLC system, and the agents told Mr.

Levison that they would meet with him when they were ready to install the device and go over with him any of the technical details regarding the installation and use of the pen register. As for the data collected by the device, the agents assured Mr. Levison that the only data that the agents would review is that which is stated in the order and nothing more (*i.e.*, user log-in information and the date, time, and duration of the transmissions for the target account).

3. Lavabit LLC provides encryption service to paid users ███████████ Based on the conference call with Mr. Levison, the FBI is reasonably confident that with the encryption keys, which Mr. Levison can access, it would be able view in an un-encrypted format any encrypted information required to be produced through the use of the pen register.

4. Mr. Levison and his attorney did not commit to the installation and use of the pen register at the conclusion of the July 10 conference call. On July 11, 2013, counsel who participated in the conference call informed the government that she no longer represented Mr. Levison or Lavabit LLC. In addition, Mr. Levison indicated that he would not come to court unless the government paid for his travel.

5. On July 11, 2013, FBI agents served Mr. Levison with a grand jury subpoena directing him to appear before the grand jury in this district on July 16, 2013. As a grand jury witness, the government was responsible for making Mr. Levison's travel arrangements.

6. On July 11, 2013, the undersigned counsel sent Mr. Levison an email indicating that he has been served with a show cause order from this Court requiring his appearance on July 16, 2013, and a subpoena requiring his appearance on the same date before a federal grand jury. The email further advised Mr. Levison that he should contact the United States Attorney's Office as soon as possible to make his travel arrangements.

7.   On July 13, 2013, Mr. Levison, who was no longer represented by counsel. sent government prosecutors an email indicating that he would be able to collect the data required by the pen register and provide that data to the government after 60 days (the period of the pen register order). For this service, Mr. Levison indicated that the government would have to pay him $2000 for "developmental time and equipment" plus an additional $1500 if the government wanted the data "more frequently" than after 60 days.

8.   On July 13, 2013, the government responded to Mr. Levison's proposal. The prosecutors informed Mr. Levison that the pen register is a devise used to monitor ongoing email traffic on a real-time basis and providing the FBI with data after 60 days was not sufficient. Furthermore, prosecutors informed him that the statute authorizes the government to compensate a service provider for "reasonable expenses," and the amount he quoted did not appear to be reasonable. Mr. Levison responded by email stating that the pen register order, in his opinion, does not require real-time access (although this fact was discussed at length during the July 10 conference call). Moreover, he indicated that the cost of reissuing the "SSL certificate" (for encryption service) would be $2000. It was unclear in his email if this $2000 was an additional expense to be added to the $3500 previously claimed. Mr. Levison indicated that he would try to contact the person responsible for making his travel arrangements at the United States Attorney's office on Sunday afternoon.

9.   On July 15, 2013, Mr. Levison spoke with the person responsible for making his travel arrangements. He was told that he was booked on a flight from Dallas, Texas, to Reagan National Airport departing that same evening. He also had a hotel reservation. Mr. Levison indicated that ██████████████████████████████████

10.   The proceeding before the Court today is to determine whether Lavabit LLC and Mr. Levison should be held in civil contempt. Civil contempt, as compared to criminal contempt under rule 42 of the Federal Rules of Criminal Procedure, is intended to coerce compliance with a court order. There are four elements to civil contempt: (1) the existence of valid order of which Lavabit LLC and Mr. Levison had actual or constructive knowledge; (2) the order was in the government's "favor"; (3) Lavabit LLC and Mr. Levison violated the terms of the order and had knowledge, or constructive knowledge, of such violation; and (4) the government suffered harm as a result. *In re Grand Jury Subpoena* (T-112), 597 F.3d 189, 202 (4th Cir. 2012).

11.   Here, each of these elements has been met. Lavabit LLC, through direct communication between the government and Mr. Levison, its owner and operator, has had actual knowledge of the pen register order and the subsequent June 28 order of the magistrate judge compelling compliance with that order. This Court's show cause order, which was personally served on Mr. Levison, provided further notice of the violation of those orders by Lavabit LLC. The government clearly has suffered harm in that it has lost 20 days of information as a result of non-compliance.

12.   Lavabit LLC may comply with the pen register order by simply allowing the FBI to install the pen register devise and provide the FBI with the encryption keys. If Lavabit LLC informs the Court it will comply with the order, the government will not seek sanctions. If, however, Mr. Levison informs the Court that Lavabit LLC will not comply, the government requests that the Court impose a fine of $1000 per day, commencing July 17, 2013, until Lavabit LLC fully complies with the pen register order.

13.   To the extent that Lavabit LLC takes the position that the pen register does not

authorize the production of the encryption keys, the government has asked the Court to authorize the seizure of that information pursuant to a warrant under Title 18, United States Code, Section 2703, thus rendering this argument moot.

14. The Court has sealed this proceeding. This pleading has also been filed under seal. The United States will hand deliver a copy of this pleading to Mr. Levison at today's hearing.

Respectfully submitted,

Neil H. MacBride

By

United States Attorney's Office
Justin W. Williams U.S. Attorney's Building
2100 Jamieson Avenue
Alexandria, Virginia 22314
Phone: 703-299-3700

EXHIBIT 13

```
 1                UNITED STATES DISTRICT COURT
                 EASTERN DISTRICT OF VIRGINIA
 2                   ALEXANDRIA DIVISION

 3    _____
                                      )
 4    IN THE MATTER OF THE            )
      APPLICATION OF THE UNITED       )  1:13 EC 297
 5    STATES OF AMERICA FOR AN        )
      ORDER AUTHORIZING THE           )  UNDER SEAL
 6    INSTALLATION AND USE OF A       )
      PEN REGISTER/TRAP AND TRACE     )  Alexandria, Virginia
 7    DEVICE ON AN ELECTRONIC         )  July 16, 2013
      MAIL ACCOUNT                    )  10:41 a.m.
 8    _____)

 9

10

11                   TRANSCRIPT OF HEARING

12         BEFORE THE HONORABLE CLAUDE M. HILTON

13              UNITED STATES DISTRICT JUDGE

14

15

16

17

18

19    APPEARANCES:

20    For the United States:   James Trump, Esq.
                               Andrew Peterson, Esq.
21                             Brandon Van Grack, Esq.
                               Michael Ben'Ary, Esq.
22
      For the Respondent:      Ladar Levison, Respondent
23
       Court Reporter:         Tracy L. Westfall, RPR, CMRS, CCR
24
      Proceedings reported by machine shorthand, transcript produced
25    by computer-aided transcription.
```

```
1                      P R O C E E D I N G S

2            THE CLERK:  In Re:  Case No. 1:13 EC 297.

3            MR. TRUMP:  Good morning, Judge.  Jim Trump on behalf

4    of the United States.  With me is Andy Peterson, Brandon

5    Van Grack from the United States Department of Justice,

6    Mr. Ben'Ary behind me, and Matt Braverman, special agent for the

7    FBI.

8            THE COURT:  All right.

9            MR. LEVISON:  Ladar Levison, the subject of the

10   summons.

11           THE COURT:  All right.  Mr. Trump.

12           MR. TRUMP:  Your Honor, we submitted our supplemental

13   paper this morning describing the communication we've had with

14   Lavabit, LLC, through Mr. Levison.  And I think, very simply, we

15   would like this Court to inquire of Mr. Levison whether he

16   intends to comply with the pen register order which would

17   require him to allow the FBI access to his server to install a

18   device which will extract data, filter that data, and provide

19   that data to the FBI, and to provide the FBI with the encryption

20   keys to the extent there is encrypted information, included

21   among within the body of information called for by the pen

22   register order.

23           As the Court is aware, and as we will provide with

24   Mr. Levison, we obtained a search warrant this morning from Your

25   Honor for the same encryption keys.  Thus, to the extent there's
```

1   any question as to whether Mr. Levison would be required to

2   provide these keys, it's now subject both to the pen register

3   order and the search warrant, the seizure warrant.

4   That's where we stand, Your Honor. If Mr. Levison

5   agrees to comply with the order, we would not seek any

6   sanctions. We would ask that he be directed to forthwith make

7   his servers available so the FBI can install that device and to

8   extract the encryption keys.

9   If, however, he informs the Court he is not willing to

10 comply with the order, we would ask the Court to impose

11 sanctions. We suggested in our pleading a thousand dollars a

12 day to be paid to the United States government until he

13 complies. If he doesn't comply with that sanction, then we

14 would be back in court seeking additional sanctions or charging

15 additional offenses.

16   THE COURT: All right. Mr. Levison.

17   MR. LEVISON: Good morning, Your Honor. I'm not sure

18 what order I should make these in, but I would like to request a

19 couple of things by motion.

20   I'd like to move that all of the nonsensitive portions

21 of the documents that were provided, i.e., everything except the

22 account in question, be unsealed. I believe it's important for

23 the industry and the people to understand what the government is

24 requesting by demanding that I turn over these encryption keys

25 for the entire service.

1   THE COURT: All right. What do you say to that,

2   Mr. Trump? Deal with the motions before I --

3   MR. TRUMP: What Mr. Levison is trying to do, Your

4   Honor, is invite industry to come in and litigate as a surrogate

5   for him the issue of whether the encryption keys are part and

6   parcel of the pen register order. And that's one of the reasons

7   we sought the search warrant, to make it clear, whether through

8   the search warrant or pen register order, he is required to

9   provide these keys.

10   We know he's been in contact with attorneys who also

11   represent industry groups and others who have litigated issues

12   like this in the WikiLeaks context and others. But we would

13   object to unsealing this matter because it's just Mr. --

14   THE COURT: And they've done that in connection with

15   the issuance of a pen register?

16   MR. TRUMP: They have litigated privacy-related issues

17   in the context of process under 2703. I'm not sure -- not a pen

18   register, but with respect to 2703.

19   But we discussed this issue with Mr. Levison and his

20   counsel by conference call. We indicated that the only data

21   that the government seeks is that which is required by the pen

22   register order. That it's just the basic header to e-mail

23   traffic, sender, recipient, time, duration, that sort of thing.

24   If Mr. Levison wants to object to providing the keys,

25   he can certainly object to doing that and then we can proceed

1   from there, but I don't think he's entitled to try to make this

2   a public proceeding to invite others in to litigate those issues

3   on his behalf.

4   THE COURT: All right. Well, I believe that to be

5   correct. I mean, this is a criminal investigation. A pen

6   register has been ordered and is here at issue, and any motion

7   to unseal that will be denied.

8   You said you had another motion, I believe?

9   MR. LEVISON: Yeah. My issue is only with the SSL

10   keys. So if that is litigated separately and that portion of

11   the proceeding is unsealed, I'm comfortable with that.

12   THE COURT: I don't understand what you're saying,

13   separate proceedings.

14   MR. LEVISON: Sorry. I have always agreed to the

15   installation of the pen register device. I have only ever

16   objected to turning over the SSL keys because that would

17   compromise all of the secure communications in and out of my

18   network, including my own administrative traffic.

19   THE COURT: Well, didn't my order already include that?

20   MR. LEVISON: I do not believe so, sir.

21   THE COURT: Did my initial order -- I don't recall at

22   the moment. Did my initial order recall the encrypted devices

23   with the installation of a pen register?

24   MR. TRUMP: The pen register, as issued, just required

25   all assistance, technical assistance, facilities, and

1   information, to facilitate the pen register.

2   This morning the search warrant required --

3   THE COURT: Yeah, but the search warrant's a different

4   matter now. That's not before me this morning. The only thing

5   that's before me this morning is the pen register.

6   MR. TRUMP: Correct.

7   THE COURT: So as I understand it, my initial order

8   ordered nothing but that the pen register be put in place.

9   MR. TRUMP: And all technical assistance, information,

10   and facilities necessary to implement the pen register. And

11   it's our position that without the encryption keys, the data

12   from the pen register will be meaningless. So to facilitate the

13   actual monitoring required by the pen register, the FBI also

14   requires the encryption keys.

15   THE COURT: Well, that could be, but I don't know that

16   I need -- I don't know that I need to reach that because I've

17   issued a search warrant for that.

18   MR. TRUMP: Correct, Your Honor. That the -- to avoid

19   litigating this issue, we asked the Court to enter the seizure

20   warrant.

21   THE COURT: Well, what I'm saying is if he agrees that

22   the pen register be established, and that the only thing he

23   doesn't want to do in connection with the pen register is to

24   give up the encryption device or code --

25   MR. LEVISON: I've always maintained that.

1   THE COURT: -- so we've got no issue here. You're

2   ready to do that?

3   MR. LEVISON: I've been ready to do that since Agent

4   Howard spoke to me the first time.

5   THE COURT: All right. So that ends our --

6   MR. TRUMP: Well, then we have to inquire of

7   Mr. Levison whether he will produce the encryption keys pursuant

8   to the search warrant that Your Honor just signed.

9   THE COURT: But I can't deal with that this morning,

10   can I?

11   MR. TRUMP: Well, it's the same issue. You could ask

12   him, Your Honor. We can serve him with the warrant and ask him

13   if he's going to comply rather than --

14   MR. LEVISON: Your Honor, I've also been issued a

15   subpoena demanding those same keys, which I brought with me in

16   the event that we would have to address that subpoena.

17   THE COURT: I don't know, Mr. Trump. I don't think I

18   want to get involved in asking him. You can talk with him and

19   see whether he's going to produce them or not and let him tell

20   you. But I don't think I ought to go asking what he's going to

21   do and what he's not going to do because I can't take any action

22   about it anyway.

23   If he does not comply with the subpoena, there are

24   remedies for that one way or another.

25   MR. TRUMP: Well, the original pen register order was

1   followed by a compulsion order from Judge Buchanan. The

2   compulsion order required the encryption keys to be produced.

3   So, yes, part of the show cause order is to require

4   compliance both with the pen register order and the compulsion

5   order issued by Judge Buchanan.

6   And that order, which was attached to the show cause

7   order, states, "To the extent any information, facilities, or

8   technical assistance are under the control of Lavabit are needed

9   to provide the FBI with the encrypted data, Lavabit shall

10 provide such information, facilities, or technical assistance

11 forthwith."

12   MR. LEVISON: I would object to that statement. I

13 don't know if I'm wording this correctly, but what was in that

14 order to compel was a statement that was incorrect.

15   Agent Howard seemed to believe that I had the ability

16 to encrypt the e-mail content stored on our servers, which is

17 not the case. I only have the keys that govern communications

18 into and out of the network, and those keys are used to secure

19 the traffic for all users, not just the user in question.

20   So the statement in that order compelling me to decrypt

21 stuff and Agent Howard stating that I have the ability to do

22 that is technically false or incorrect. There was never an

23 explicit demand that I turn over these keys.

24   THE COURT: I don't know what bearing that would have,

25 would it? I mean, I don't have a problem -- Judge Buchanan

1 issued an order in addition to mine, and I'm not sure I ought to

2 be enforcing Judge Buchanan's order.

3   My order, if he says that he will produce or allow the

4 installation of the pen register, and in addition I have issued

5 a search warrant for the codes that you want, which I did this

6 morning, that's been entered, it seems that this issue is over

7 as far as I'm concerned except I need to see that he allows the

8 pen register and complies with the subpoena.

9   MR. TRUMP: Correct.

10   THE COURT: If he doesn't comply -- if he doesn't

11 comply with the subpoena, then that has -- I have to address

12 that.

13   MR. TRUMP: Right.

14   THE COURT: But right now there's nothing for me to

15 address here unless he is not telling me correctly about the pen

16 register.

17   MR. TRUMP: Well, we can -- Your Honor, if we can talk

18 to Mr. Levison for five minutes, we can ask him whether he will

19 honor the warrant that you just issued.

20   MR. LEVISON: Before we do that, can I --

21   THE COURT: Well, what can I do about it if he doesn't,

22 if he tells you he's not going to? You've got the right to go

23 out and search and get it.

24   MR. TRUMP: Well, we can't get the information without

25 his assistance. He's the only who knows and has possession of

1 it. We can't take it from him involuntarily.

2   MR. LEVISON: If I may, sir, my other --

3   THE COURT: Wait just a second.

4   You're trying to get me ahead. You're trying to get me

5 to deal with a contempt before there's any contempt, and I have

6 a problem with that.

7   MR. TRUMP: I'm trying to avoid contempt altogether,

8 Your Honor.

9   THE COURT: I know you are. And I'd love for you-all

10 to get together and do that. I don't want to deal with it

11 either. But I don't think we can sit around and agree that

12 there's going to be a default and I will address it before it

13 occurs.

14   MR. TRUMP: I'm just trying to figure out whether

15 there's going to be a default. We'll take care of that, Judge.

16   THE COURT: You can. I think the way we've got to do

17 this -- and I'll listen to you. I'm cutting you off, I know,

18 but I'll listen to you in a minute.

19   The way we have to do this, the hearing that's before

20 me this morning on this issue of the pen register, that's been

21 resolved, or so he's told me. I don't know whether you want to

22 continue this one week and see if he complies with that, which I

23 guess would be prudent to do, or a few days for him to comply

24 with the pen register. Then we will wait and see what happens

25 with the subpoena.

1   Because as far as my pen register order is concerned,

2 he says he's going to comply with it. So that issue's over and

3 done with. The next issue will be whether or not he complies

4 with the subpoena. And I don't know and I don't want to

5 presume, and I don't want him to represent to me what he intends

6 to do when he can very well go home and decide he's going to do

7 something different.

8   When that warrant is served, we'll know what he's going

9 to do. I think we've got -- I don't see another way to do it.

10   MR. TRUMP: That's fine, Your Honor. We will serve the

11 warrant on him as soon as we conclude this hearing, and we'll

12 find out whether he will provide the keys or not.

13   THE COURT: Okay. Now, did you want to say anything

14 else?

15   MR. LEVISON: Well, I mean, I've always maintained that

16 all the government needs to do is contact me and set up an

17 appointment to install that pen register. So I don't know why

18 there has never been any confusion about my willingness to

19 install it. I've only ever objected to the providing of those

20 keys which secure any sensitive information going back and

21 forth.

22   But my motion, and I'm not sure if it's relevant or not

23 because it deals more with the issue of the subpoena demanding

24 the keys and for what will be the forthcoming search warrant,

25 would be a continuance so that I can retain counsel to address

1   that particular issue.

2   THE COURT: Well, I mean, there's nothing before me

3   with that. I've issued the subpoena. Whatever happens with

4   that, that's -- you're trying to get me to do what Mr. Trump

5   wanted to do and to arrange this beforehand.

6   MR. LEVISON: Well, I don't know if I have to appear

7   before that grand jury right now and give the keys over or face

8   arrest. I'm not a lawyer so I don't understand the procedure.

9   THE COURT: I don't know either. You need to have --

10 it would be wise to have a lawyer.

11   MR. LEVISON: Okay.

12   THE COURT: I don't know what's going to happen. I

13 don't know. They haven't served the warrant yet. I have no

14 idea. Don't know what's going to happen with it. You'll just

15 have to figure that out, and it be wise to have a lawyer to do

16 it, I would think.

17   MR. LEVISON: I guess while I'm here in regards to the

18 pen register, would it be possible to request some sort of

19 external audit to ensure that your orders are followed to the

20 letter in terms of the information collected and preserved?

21   THE COURT: No. The law provides for those things, and

22 any other additional or extra monitoring you might want or think

23 is appropriate will be denied, if that's what you're requesting.

24   MR. LEVISON: Okay. I mean, it requests that the

25 government return to the Court records --

1   THE COURT: You need to talk to a lawyer about what the

2 law requires for the issuance of a pen register.

3   MR. LEVISON: They can handle that separately. That's

4 fine.

5   THE COURT: The law sets out what is done in that

6 regard. Your lawyer can fill you in if you want to know.

7   MR. LEVISON: I've always been willing to accept the

8 device. I just have some concern about ensuring that it's used

9 properly.

10   THE COURT: Should we continue this to some specific

11 date to see that he complies with the pen register?

12   MR. TRUMP: We can, Your Honor. It's a moot issue

13 without the encryption keys.

14   THE COURT: Well, that is a practical matter --

15   MR. TRUMP: That's a practical --

16   THE COURT: -- but I don't think it is a moot issue. I

17 mean, you-all have got the right to go in and put on that pen

18 register. He says that he will do it. That's all that I've

19 ordered.

20   Now, the other business about ordering that, Judge

21 Buchanan made an order that he's going to have to supply what

22 you say is the encryption codes to make the information useful.

23 I don't know. I didn't enter that order. I have trouble making

24 that connection.

25   If you're going to -- I don't know whether you want to

1   do something in front of Judge Buchanan or not.

2   MR. LEVISON: You see, Judge, though that I've always

3   been willing. They just didn't feel the need to set up an

4   appointment.

5   THE COURT: What do you want me to do with this case?

6   You want me to continue it? You want me to say it's moot right

7   now and just end it?

8   MR. TRUMP: No. I think we can continue it. I don't

9   know Mr. Levison's schedule. It can be done within hours of his

10 return to Dallas.

11   THE COURT: Of course he can. You want to continue it

12 till a week from Friday?

13   MR. TRUMP: Or a week from today.

14   MR. LEVISON: I'm not available within hours of my

15 return, but I can meet with you on Thursday.

16   THE COURT: Let's continue it a week from Friday.

17   MR. TRUMP: A week from Friday.

18   THE COURT: What date's that? The --

19   THE CLERK: 26th.

20   THE COURT: The 26th?

21   MR. LEVISON: Acceptable to me.

22   THE COURT: We'll continue it to the 26th, and that's

23 for determining whether or not that pen register has been

24 installed as you request.

25   We can make it 10 o'clock.

1   MR. LEVISON: I'll remember 10:00 instead of 10:30 this

2 time.

3   THE COURT: All right. Thank you.

4   All right. Thank you-all. We'll adjourn till tomorrow

5 morning at 9:30.

6   * * *

7   (Proceedings concluded at 11:02 a.m.)

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

CERTIFICATION

I certify, this 17th day of September 2013, that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter to the best of my ability.

/s/

_____

Tracy Westfall, RPR, CMRS, CCR

EXHIBIT 14

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division
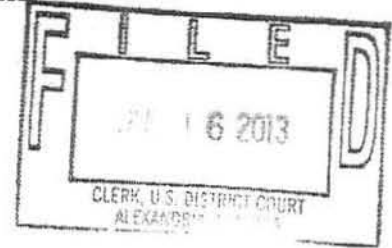
IN THE MATTER OF THE   )
APPLICATION OF THE UNITED)
STATES AUTHORIZING THE USE OF)
A PEN REGISTER/TRAP AND TRACE)   Criminal No. 1:13EC297
DEVICE ON AN ELECTRONIC MAIL)
ACCOUNT   )
)

ORDER

This matter comes before the Court on the Government's Motion that Ladar Levinson, the owner and operator of Lavabit, LLC show cause as to why Lavabit, LLC has failed to comply with the Court's Order of June 28, 2013 and why this Court should not hold Mr. Levinson and Lavabit, LLC in contempt, and Ladar Levinson's oral Motion To Unseal. For the reasons stated from the bench, it is hereby

ORDERED that Ladar Levinson's Motion To Unseal is DENIED and this matter is continued to Friday, July 26, 2013 at 10:00 a.m. for further proceedings.

CLAUDE M. HILTON
UNITED STATES DISTRICT JUDGE

Alexandria, Virginia
July 16 , 2013

EXHIBIT 15

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division
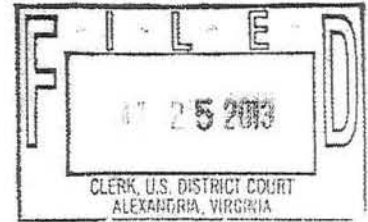
IN THE MATTER OF THE APPLICATION OF THE UNITED STATES AUTHORIZING THE USE OF A PEN REGISTER/TRAP AND TRACE DEVICE ON AN ELECTRONIC MAIL ACCOUNT	**FILED UNDER SEAL** No. 1:13EC297	
IN THE MATTER OF THE SEARCH AND SEIZURE OF INFORMATION ASSOCIATED WITH ████████████████ THAT IS STORED AND CONTROLLED AT PREMISES CONTROLLED BY LAVABIT LLC	No. 1:13SW522	
In re Grand Jury	No. 13-1	

MOTION TO QUASH SUBPOENA AND SEARCH WARRANT AND MEMORANDUM OF LAW IN SUPPORT OF MOTION

Lavabit LLC ("Lavabit") and Mr. Ladar Levinson ("Mr. Levinson") move this Court to quash the grand jury subpoena and search and seizure warrant served on them by the Federal Bureau of Investigation and the Office of the United States Attorney (collectively "Government").

BACKGROUND

Lavabit is an encrypted email service provider. As such, Lavabit's business model focuses on providing private and secure email accounts to its customers. Lavabit uses various encryption methods, including secured socket layers ("SSL"), to protect its users' privacy. Lavabit maintains an encryption

1

key, which may be used by authorized users decrypt data and communications from its server ("Master Key"). The Government has commanded Lavabit, by a subpoena[1] and a search and seizure warrant, to produce the encryption keys and SSL keys used by lavabit.com in order to access and decrypt communications and data stored in one specific email address ███████████████████ ("Lavabit Subpoena and Warrant").

ARGUMENT

If the Government gains access to Lavabit's Master Key, it will have unlimited access to not only ██████████████ ("Email Account"), but all of the communications and data stored in each of Lavabit's 400,000 email accounts. None of these other users' email accounts are at issue in this matter. However, production of the Master Key will compromise the security of these users. While Lavabit is willing to cooperate with the Government regarding the Email Account, Lavabit has a duty to maintain the security for the rest of its customers' accounts. The Lavabit Subpoena and Warrant are not narrowly tailored to seek only data and communications relating to the Email Account in question. As a result, the Lavabit Subpoena and Warrant are unreasonable under the Fourth Amendment.

a. The Lavabit Subpoena and Warrant Essentially Amounts to a General Warrant.

---

[1] The grand jury subpoena not only commanded Mr. Levinson to appear before this Court on July 16, 2013, but also to bring Lavabit's encryption keys. Mr. Levinson's subpoena to appear before the grand jury was withdrawn, but the government continues to seek the encryption keys. Lavabit is only seeking to quash the Court's command that Mr. Levinson provide the encryption keys.

2

Though the Lavabit Subpoena and Warrant superficially appears to be narrowly tailored, in reality, it operates as a general warrant by giving the Government access to every Lavabit user's communications and data. It is not what the Lavabit Subpoena and Warrant defines as the boundaries for the search, but the *method* of providing access for the search which amounts to a general warrant.

It is axiomatic that the Fourth Amendment prohibits general warrants. *Andresen v. Maryland*, 427 U.S. 463, 480 (1976). Indeed "it is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment." *Payton v. New York*, 445 U.S. 573, 583 (1980) (footnote omitted). To avoid general warrants, the Fourth Amendment requires that "the place to be searched" and "the persons or things to be seized" be described with particularity. *United States v. Moore*, 775 F. Supp. 2d 882, 898 (E.D. Va. 2011) (quoting *United States v. Grubbs*, 547 U.S. 90, 97 (2006)).

The Fourth Amendment's particularity requirement is meant to "prevent[] the seizure of one thing under a warrant describing another." *Andresen*, 427 U.S. at 480. This is precisely the concern with the Lavabit Subpoena and Warrant and, in this circumstance, the particularity requirement will not protect Lavabit. By turning over the Master Key, the Government will have the ability to search each and every "place," "person [and] thing" on Lavabit's network.

3

The Lavabit Subpoena and Warrant allows the Government to do a "general, exploratory rummaging" through any Lavabit user account. *See id.* (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)) (describing the issue with general warrants "is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings"). Though the Lavabit Subpoena and Warrant is facially limited to the Email Address, the Government would be able to seize communications, data and information from any account once it is given the Master Key.

There is nothing other than the "discretion of the officer executing the warrant" to prevent an invasion of other Lavabit user's accounts and private emails. *See id.* at 492 (quoting Stanford v. Texas, 379 U.S. 476, 485 (1965)) (explaining that the purpose of the particularity requirement of the Fourth Amendment is to ensure, with regards to what is taken that, "nothing is left to the discretion of the officer executing the warrant.") (internal citation omitted). Lavabit has no assurance that any searches conducted utilizing the Master Key will be limited solely to the Email Account. *See Groh v. Ramirez*, 540 U.S. 551, 561-62 (2004) (citing *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 532 (1967)) (noting that a particular warrant is to provide individuals with assurance "of the lawful authority of the executing officer, his need to search, and the *limits* of his power to search) (emphasis added). Lavabit has a duty to its customers to protect their accounts from the possibility of unlawful intrusions by third parties, including government entities.

As the Lavabit Subpoena and Warrant are currently framed they are invalid as they operate as a general warrant, allowing the Government to search individual users not subjection to this suit, without limit.

b. The Lavabit Subpoena and Warrant Seeks Information that Is Not Material to the Investigation.

Because of the breadth of Warrant and Subpoena, the Government will be given access to data and communications that are wholly unrelated to the suit. The Government, by commanding Lavabit's encryption keys, is acquiring access to 400,000 user's private accounts in order to gain information about one individual. 18 U.S.C. § 2703(d) states that a court order may be issued for information "relevant and material to an ongoing criminal investigation." However, the Government will be given unlimited access, through the Master Key, to several hundred thousand user's information, all of who are not "material" to the investigation. *Id.*

Additionally, the Government has no probable cause to gain access to the other users accounts. "The Fourth Amendment...requires that a warrant be no broader than the probable cause on which it is based." *Moore*, 775 F. Supp. 2d at 897 (quoting *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006)). Probable cause here is based on the activities of the individual linked to the Email Address. Other Lavabit users would be severely impacted by the Government's access to the Master Key and have not been accused of wrongdoing or criminal activity in relation to this suit. Their privacy interests should not suffer because of the alleged misdeeds of another Lavabit user.

c. Compliance with Lavabit Subpoena and Warrant Would Cause an Undue Burden.

As a non-party and unwilling participant to this suit, Lavabit has already incurred legal fees and other costs in order to comply with the Court's orders. Further compliance, by turning over the Master Key and granting the Government access to its entire network, would be unduly burdensome. *See* 18 U.S.C. § 2703(d) (stating that "the service provider may [move to] quash or modify [an] order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an *undue burden* on such provider.") (emphasis added).

The recent case of *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. 2703(d)* ("*Twitter*") addresses similar issues. 830 F. Supp. 2d 114 (E.D. Va. 2011). In that case, the Petitioners failed to allege "a personal injury cognizable by the Fourth Amendment." *Id.* at 138. However, Lavabit's circumstances are distinguishable. The Government, in pursuit of information date and communications related to the Email Address, has caused and will continue to cause injury to Lavabit. Not only has Lavabit expended a great deal of time and money in attempting to cooperate with the Government thus far, but, Lavabit will pay the ultimate price—the loss of its customers' trust and business—should the Court require that the Master Key be turned over. Lavabit's business, which is founded on the preservation of electronic privacy, could be destroyed if it is required to produce its Master Key.

Lavabit is also a fundamentally different entity than Twitter, the business at issue in *Twitter*. The Twitter Terms of Service specifically allowed user information to be disseminated. *Id.* at 139. Indeed, the very purpose of Twitter is for users to publically post their musings and beliefs on the Internet. In contrast, Lavabit is dedicated to keeping its user's information private and secure. Additionally, the order in *Twitter* did not seek "content information" from Twitter users, as is being sought here. *Id.* The Government's request for Lavabit's Master Key gives it access to data and communications from 400,000 email secure accounts, which is much more sensitive information that at issue in the *Twitter*.

The Government is attempting, in complete disregard of the Fourth Amendment, to penetrate a system that was founded for the sole purpose of privacy. *See Katz v. United States*, 389 U.S. 347, 360 (1967) (stating that "the touchstone of Fourth Amendment analysis is whether a person has a constitutionally protected reasonable expectation of privacy") (internal citations omitted). For Lavabit to grant the Government unlimited access to every one of its user's accounts would be to disavow its duty to its users and the principals upon which it was founded. Lavabit's service will be rendered devoid of economic value if the Government is granted access to its secure network. The Government does not have any proper basis to request that Lavabit blindly produce its Master Key and subject all of its users to invasion of privacy.

Moreover, the Master Key itself is an encryption developed and owned by Lavabit. As such it is valuable proprietary information and Lavabit has a

7

reasonable expectation in protecting it. Because Lavabit has a reasonable expectation of privacy for its Master Key, the Lavabit Subpoena and Warrant violate the Fourth Amendment. *See Twitter*, 830 F. Supp. 2d at 141 (citing *United States v. Calandra*, 414 U.S. 338, 346 (1974)) (noting "The grand jury is...without power to invade a legitimate privacy interest protected by the Fourth Amendment" and that "a grand jury's subpoena...will be disallowed if it is far too sweeping in its terms to be...reasonable under the Fourth Amendment.").

CONCLUSION

For the foregoing reasons, Lavabit and Mr. Levinson respectfully move this Court to quash the search and seizure warrant and grand jury subpoena. Further, Lavabit and Mr. Levinson request that this Court direct that Lavabit does not have to produce its Master Key. Alternatively, Lavabit and Mr. Levinson request that they be given an opportunity to revoke the current encryption key and reissue a new encryption key at the Government's expense. Lastly, Lavabit and Mr. Levinson request that, if they is required to produce the Master Key, that they be reimbursed for its costs which were directly incurred in producing the Master Key, pursuant to 18 U.S.C. § 2706.

LAVABIT LLC
By Counsel

Jesse R. Binnall, VSB# 79292
Bronley & Binnall, PLLC
10387 Main Street, Suite 201
Fairfax, Virginia 22030

8
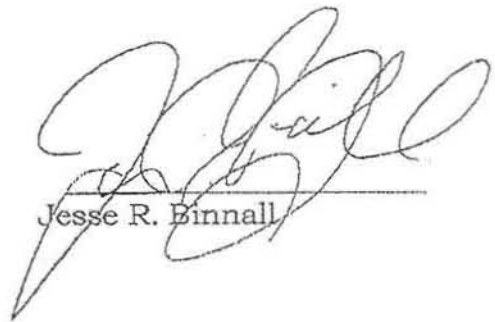
(703) 229-0335 Telephone
(703) 537-0780- Facsimile
jbinnall@bblawonline.com
Counsel for Lavabit LLC

Certificate of Service

I certify that on this 25ᵗʰ day of July, 2013, this Motion to Quash Subpoena and Search Warrant and Memorandum of Law in Support was hand delivered to the person at the addresses listed below:

United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314

Jesse R. Binnall

EXHIBIT 16

IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES AUTHORIZING THE USE OF A PEN REGISTER/TRAP AND TRACE DEVICE ON AN ELECTRONIC MAIL ACCOUNT	**FILED UNDER SEAL** No. 1:13EC297
IN THE MATTER OF THE SEARCH AND SEIZURE OF INFORMATION ASSOCIATED WITH ███████████████ THAT IS STORED AND CONTROLLED AT PREMISES CONTROLLED BY LAVABIT LLC	No. 1:13SW522
In re Grand Jury	No. 13-1

MOTION FOR UNSEALING OF SEALED COURT RECORDS AND REMOVAL OF NON-DISCLOSURE ORDER AND MEMORANDUM OF LAW IN SUPPORT OF MOTION

Lavabit, LLC ("Lavabit") and Mr. Ladar Levinson ("Mr. Levinson") (collectively "Movants") move this Court to unseal the court records concerning the United States government's attempt to obtain certain encryption keys and lift the non-disclosure order issued to Mr. Levinson. Specifically, Movants request the unsealing of all orders and documents filed in this matter before the Court's issuance of the July 16, 2013 Sealing Order ("Sealing Order"); (2) all orders and documents filed in this matter after the issuance of the Sealing Order; (3) all grand jury subpoenas and search and seizure warrants issued before or after issuance of the Sealing Order; and (4) all documents filed in

1

connection with such orders or requests for such orders (collectively, the "sealed documents"). The Sealing Order is attached as Exhibit A. Movants request that all of the sealed documents be unsealed and made public as quickly as possible, with only those redactions necessary to secure information that the Court deems, after review, to be properly withheld.

BACKGROUND

Lavabit was formed in 2004 as a secure and encrypted email service provider. To ensure security, Lavabit employs multiple encryption schemes using complex access keys. Today, it provides email service to roughly 400,000 users worldwide. Lavabit's corporate philosophy is user anonymity and privacy. Lavabit employs secure socket layers ("SSL") to ensure the privacy of Lavabit's subscribers through encryption. Lavabit possesses a master encryption key to facilitate the private communications of its users.

On July 16, 2013, this Court entered an Order pursuant to 18 U.S.C. 2705(b), directing Movants to disclose all information necessary to decrypt communications sent to or from and data stored or otherwise associated with the Lavabit e-mail account ████████████████, including SSL keys (the "Lavabit Order"). The Lavabit Order is attached as Exhibit B. The Lavabit Order precludes the Movants from notifying any person of the search and seizure warrant, or the Court's Order in issuance thereof, except that Lavabit was permitted to disclose the search warrant to an attorney for legal advice.

ARGUMENT

In criminal trials there is a common law presumption of access to judicial records, like the sealed documents in the present case. Despite the government's legitimate interests, it cannot meet its burden and overcome this presumption because it has not explored reasonable alternatives. Furthermore, the government's notice preclusion order constitutes a content-based restriction on free speech by prohibiting public discussion of an entire topic based on its subject matter.

I.   THE FIRST AMENDMENT AND NON-DISCLOSURE ORDERS

The Stored Communications Act ("SCA") authorizes notice preclusion to any person of a § 2705(b) order's existence, but only if the Court has reason to believe that notification will result in (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction or tampering with evidence; (4) intimidating of potential witnesses; or (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial. § 2705(b)(1)-(5). Despite this statutory authority, the § 2705(b) gag order infringes upon freedom of speech under the First Amendment, and should be subjected to constitutional case law.

The most searching form of review, "strict scrutiny", is implicated when there is a content-based restriction on free speech. *R.A.V. v. City of St. Paul, Minn.*, 505 U.S. 377, 403 (1992). Such a restriction must be necessary to serve a compelling state interest and narrowly drawn to achieve that end. *Id.* The Lavabit Order's non-disclosure provision is a content-based restriction that is not narrowly tailored to achieve a compelling state interest.

3

a. The Lavabit Order Regulates Mr. Levinson's Free Speech

The notice preclusion order at issue here limits Mr. Levinson's speech in that he is not allowed to disclose the existence of the § 2705(b) order, or the underlying investigation to any other person including any other Lavabit subscriber. This naked prohibition against disclosure can fairly be characterized as a regulation of pure speech. *Bartnicki v. Vopper*, 532 U.S. 514, 526 (2001). A regulation that limits the time, place, or manner of speech is permissible if it serves a significant governmental interest and provides ample alternative channels for communication. *See Cox v. New Hampshire*, 312 U.S. 569, 578 (1941) (explaining that requiring a permit for parades was aimed at policing the streets rather than restraining peaceful picketing). However, a valid time, place, and manner restriction cannot be based on the content or subject matter of the speech. *Consol. Edison Co. of New York v. Pub. Serv. Comm'n of New York*, 447 U.S. 530, 536 (1980).

The gag order in the present case is content-based because it precludes speech on an entire topic, namely the search and seizure warrant and the underlying criminal investigation. *See id.* at 537 ("The First Amendment's hostility to content-based regulation extends...to prohibition of public discussion of an entire topic"). While the nondisclosure provision may be viewpoint neutral on its face, it nevertheless functions as a content-based restriction because it closes off an "entire topic" from public discourse.

It is true that the government has a compelling interest in maintaining the integrity of its criminal investigation ███████████. However, Mr.

4

Levinson has been unjustly restrained from contacting Lavabit subscribers who could be subjected to government surveillance if Mr. Levinson were forced to comply the Lavabit Order. Lavabit's value is embodied in its complex encryption keys, which provide its subscribers with privacy and security. Mr. Levinson has been unwilling to turn over these valuable keys because they grant access to his entire network. In order to protect Lavabit, which caters to thousands of international clients, Mr. Levinson needs some ability to voice his concerns, garner support for his cause, and take precautionary steps to ensure that Lavabit remains a truly secure network.

b. The Lavabit Order Constitutes A Prior Restraint On Speech

Besides restricting content, the § 2705(b) non-disclosure order forces a prior restraint on speech. It is well settled that an ordinance, which makes the enjoyment of Constitutional guarantees contingent upon the uncontrolled will of an official, is a prior restraint of those freedoms. *Shuttlesworth v. Birmingham*, 394 U.S. 147, 150-151 (1969); *Staub v. City of Baxley*, 355 U.S. 313, 322 (1958). By definition, a prior restraint is an immediate and irreversible sanction because it "freezes" speech. *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 559 (1976). In the present case, the Lavabit Order, enjoins Mr. Levinson from discussing these proceedings with any other person. The effect is an immediate freeze on speech.

The Supreme Court of the United States has interpreted the First Amendment as providing greater protection from prior restraints. *Alexander v. United States*, 509 U.S. 544 (1993). Prior restraints carry a heavy burden for

5

justification, with a presumption against constitutional validity. *Capital Cities Media, Inc. v. Toole*, 463 U.S. 1303, 1305 (1983); *Carroll v. Princess Anne*, 393 U.S. 175, 181 (1968); *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 70 (1963). Here, the government and the Court believe that notification of the search warrant's existence will seriously jeopardize the investigation, by giving targets an opportunity to flee or continue flight from prosecution, will destroy or tamper with evidence, change patterns of behavior, or notify confederates. *See* Lavabit Order. However, the government's interest in the integrity of its investigation does not automatically supersede First Amendment rights. *See Landmark Communications, Inc. v. Virginia*, 435 U.S. 829, 841 (1978) (holding the confidentiality of judicial review insufficient to justify encroachment on the freedom of speech).

In the present case, the government has a legitimate interest in tracking the account ███████████████████. However, if Lavabit were forced to surrender its master encryption key, the government would have access not only to this account, but also every Lavabit account. Without the ability to disclose government access to users' encrypted data, public debate about the scope and justification for this secret investigatory tool will be stifled. Moreover, innocent Lavabit subscribers will not know that Lavabit's security devices have been compromised. Therefore the § 2705(b) non-disclosure order should be lifted to provide Mr. Levinson the ability to ensure the value and integrity of Lavabit for his other subscribers.

II. THE LAW SUPPORTS THE RIGHT OF PUBLIC ACCESS TO THE SEALED DOCUMENTS

Despite any statutory authority, the Lavabit Order and all related documents were filed under seal. The sealing of judicial records imposes a limit on the public's right of access, which derives from two sources, the First Amendment and the common law. *Va. Dep't of State Police v. Wash. Post*, 386 F.3d 567, 575 (4th Cir. 2004); *See Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 580 (press and public have a First Amendment right of attend a criminal trial); *Press-Enterprise Co. v. Superior Court*, 478 U.S. 1, 2 (1986) (right of access to preliminary hearing and transcript).

a. The Common Law Right Of Access Attaches To The Lavabit Order

For a right of access to a document to exist under either the First Amendment or the common law, the document must be a "judicial record." *Baltimore Sun Co. v. Goetz*, 886 F.2d 60, 63–64 (4th Cir. 1989). Although the Fourth Circuit Court of Appeals has never formally defined "judicial record", it held that § 2703(d) orders and subsequent orders issued by the court are judicial records because they are judicially created. *In re U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d)*, 707 F.3d 283, 290 (4th Cir. 2013) ("*Twitter*"). The § 2705(b) order in the present case was issued pursuant to § 2703(d) and can properly be defined as a judicial record. Although the Fourth Circuit has held there is no First Amendment right to access § 2703(d) orders, it held that the common law presumption of access attaches to such documents. *Twitter*, 707 F.3d at 291.

The underlying investigation in *Twitter*, involved a § 2703(d) order, which directed Twitter to provide personal information, account information, records, financial data, direct messages to and from email addresses, and Internet Protocol addresses for eight of its subscribers. *In re: § 2703(d) Order*, 787 F. Supp. 2d 430, 435 (E.D. Va. 2011). Citing the importance of investigatory secrecy and integrity, the court in that case denied the petitioners Motion to Unseal, finding no First Amendment or common law right to access. *Id.* at 443.

Unlike Twitter, whose users publish comments on a public forum, subscribers use Lavabit for its encrypted features, which ensure security and privacy. In *Twitter* there was no threat that any user would be subject to surveillance other than the eight users of interest to the government. However, a primary concern in this case is that the Lavabit Order provides the government with access to every Lavabit account.

Although the secrecy of SCA investigations is a compelling government interest, the hundreds of thousands of Lavabit subscribers that would be compromised by the Lavabit Order are not the subjects of any justified government investigation. Therefore access to these private accounts should not be treated as a simple corollary to an order requesting information on one criminal subject. The public should have access to these orders because their effect constitutes a seriously concerning expansion of grand jury subpoena power.

To overcome the common law presumption of access, a court must find that there is a "significant countervailing interest" in support of sealing that

outweighs the public's interest in openness. *Twitter*, 707 F.3d at 293. Under the common law, the decision to seal or grant access to warrant papers is within the discretion of the judicial officer who issued the warrant. *Media General Operations, Inc. v. Buchanan*, 417 F.3d 424, 429 (4th Cir. 2005). If a judicial officer determines that full public access is not appropriate, she must consider alternatives to sealing, which may include granting some public access or releasing a redacted version of the documents. *Id.*

In *Twitter* the court explained that because the magistrate judge individually considered the documents, and redacted and unsealed certain documents, he satisfied the procedural requirements for sealing. *Twitter*, 707 F.3d at 294. However, in the present case, there is no evidence that alternatives were considered, that documents were redacted, or that any documents were unsealed. Once the presumption or access attaches, a court cannot seal documents or records indefinitely unless the government demonstrates that some significant interest heavily outweighs the public interest in openness. *Wash. Post*, 386 F.3d at 575. Despite the government's concerns, there are reasonable alternatives to an absolute seal that must be explored in order to ensure the integrity of this investigation.

b. There Is No Statutory Authority To Seal The § 2705(d) Documents

There are no provisions in the SCA that mention the sealing of orders or other documents. In contrast, the Pen/Trap Statute authorizes electronic surveillance and directs that pen/trap orders be sealed "until otherwise

ordered by the court". 18 U.S.C. §§ 3121-27. Similarly, the Wiretap Act, another surveillance statute, expressly directs that applications and orders granted under its provisions be sealed. 18 U.S.C. § 2518(8)(b). The SCA's failure to provide for sealing is not a congressional oversight. Rather, Congress has specifically provided for sealing provisions when it desired. Where Congress includes particular language in one section of a statute but omits it in another, it is generally assumed that Congress acts intentionally. *Keene Corp. v. United States*, 508 U.S. 200, 208 (1993). Therefore, there is no statutory basis for sealing an application or order under the SCA that would overcome the common law right to access.

c. Privacy Concerns Demand A Common Law Public Right Of Access To The Sealed Documents

The leaking of classified government practices by Edward Snowden and the ensuing mass surveillance scandal have sparked an intense national and international debate about government surveillance, privacy rights and other traditional freedoms. It is concerning that suppressing Mr. Levinson's speech and pushing its subpoena power to the limits, the government's actions may be viewed as accomplishing another unfounded secret infringement on personal privacy. A major concern is that this could cause people worldwide to abandon American service providers in favor of foreign businesses because the United States cannot be trusted to regard privacy.[1] It is in the best interests of the Movant's and the government that the documents in this matter not be

---

[1] *See* Dan Roberts, *NSA Snooping: Obama Under Pressure as Senator Denounces 'Act of Treason'*, The Guardian, June 10, 2013, http://www.guardian.co.uk/world/2013/jun/10/obama-pressured-explain-nsa-surveillance.

10

shrouded in secrecy and used to further unjustified surveillance activities and to suppress public debate.

CONCLUSION

For the foregoing reasons, Lavabit respectfully moves this Court to unseal the court records concerning the United States government's attempt to obtain certain encryption keys and lift the non-disclosure order issued on Mr. Levinson. Alternatively, Lavabit requests that all of the sealed documents be redacted to secure only the information that the Court deems, after review, to be properly withheld.

LAVABIT LLC
By Counsel

Jesse R. Binnall, VSB# 79292
Bromley & Binnall, PLLC
10387 Main Street, Suite 201
Fairfax, Virginia 22030
(703) 229-0335 Telephone
(703) 537-0780- Facsimile
jbinnall@bblawonline.com
Counsel for Lavabit LLC

Certificate of Service

I certify that on this ___25th___ day of July, 2013, this Motion For Unsealing Of Sealed Court Records And Removal Of Non-Disclosure Order And Memorandum Of Law In Support was hand delivered to the person at the addresses listed below:

████████████████████

United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314

████████████████

Jesse R. Binnall

12

EXHIBIT 17

IN THE UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF VIRGINIA

ALEXANDRIA DIVISION

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES AUTHORIZING THE USE OF A PEN REGISTER/TRAP AND TRACE DEVICE ON AN ELECTRONIC MAIL ACCOUNT	NO. 1:13 EC 297
IN THE MATTER OF THE SEARCH AND SEIZURE OF INFORMATION ASSOCIATED WITH ███████ THAT IS STORED AND CONTROLLED AT PREMISES CONTROLLED BY LAVABIT LLC	NO. 1:13 SW 522
IN RE GRAND JURY SUBPOENA	NO. 13-1
	UNDER SEAL

**RESPONSE OF THE UNITED STATES IN OPPOSITION
TO LAVABIT'S MOTION TO QUASH SUBPOENA AND
MOTION TO FOR UNSEALING OF SEALED COURT RECORDS**

INTRODUCTION

This Court has ordered Lavabit, LLC to provide the government with the

technical assistance necessary to implement and use a pen register and trap and trace

device ("pen-trap device"). A full month after that order, and after an order to compel

compliance, a grand jury subpoena, and a search warrant for that technical assistance,

Lavabit has still not complied. Repeated efforts to seek that technical assistance from

Lavabit's owner have failed. While the government continues to work toward a mutually

acceptable solution, at present there does not appear to be a way to implement this

Court's order, as well as to comply with the subpoena and search warrant, without requiring Lavabit to disclose an encryption key to the government. This Court's orders, search warrant, and the grand jury subpoena all compel that result, and they are all lawful. Accordingly, Lavabit's motion to quash the search warrant and subpoena should be denied.

Lavabit and its owner have also moved to unseal all records in this matter and lift the order issued by the Court preventing them from disclosing a search warrant issued in this case. Because public discussion of these records would alert the target and jeopardize an active criminal investigation, the government's compelling interest in maintaining the secrecy and integrity of that investigation outweighs any public right of access to, or interest in publicly discussing, those records, and this motion should also be denied.

TECHNICAL BACKGROUND

Pen registers and trap and trace devices

To investigate Internet communications, Congress has permitted law enforcement to employ two surveillance techniques—the pen register and the trap and trace device— that permit law enforcement to learn information about an individual's communications. *See* 18 U.S.C. §§ 3121-27 ("Pen-Trap Act"). These techniques, collectively known as a "pen-trap," permit law enforcement to learn facts about e-mails and other communications as they are sent—but not to obtain their content. *See, e.g., United States v. Forrester*, 512 F.3d 500, 509-13 (9th Cir. 2008) (upholding government's use of a pen-trap that "enabled the government to learn the to/from addresses of Alba's e-mail

2

messages, the IP addresses of the websites that Alba visited and the total volume of information sent to or from his account").

The Pen-Trap Act "unambiguously authorize[s] the use of pen registers and trap and trace devices on e-mail accounts." *In Matter of Application of U.S. For an Order Authorizing the Installation & Use of a Pen Register & a Trap & Trace Device on E-Mail Account,* 416 F. Supp. 2d 13, 14 (D.D.C. 2006) (Hogan, J.) ("*Hogan Order*"). It authorizes both the installation of a "device," meaning, a separate computer attached to the provider's network, and also a "process," meaning, a software program run on the provider. *Id.* at 16; 18 U.S.C. § 3127.

Secure Socket Layer (SSL) or Transport Layer Security (TLS) Encryption

Encrypting communications sent across the Internet is a way to ensure that only the sender and receiver of a communication can read it. Among the most common methods of encrypting Web and e-mail traffic is Secure Socket Layer (SSL), which is also called Transport Layer Security (TLS) encryption. "The Secure Socket Layer ('SSL') is one method for providing some security for Internet communications. SSL provides security by establishing a secure channel for communications between a web browser and the web server; that is, SSL ensures that the messages passed between the client web browser and the web server are encrypted." *Disney Enterprises, Inc. v. Rea,* No. 1:12-CV-687, 2013 WL 1619686 *9 (E.D. Va. Apr. 11, 2013); *see also Stambler v. RSA Sec., Inc.,* 2003 WL 22749855 *2-3 (D. Del. 2003) (describing SSL's technical operation).

As with most forms of encryption, SSL relies on the use of large numbers known as "keys." Keys are parameters used to encrypt or decrypt data. Specifically, SSL

encryption employs public-key cryptography, in which both the sender and receiver each have two mathematically linked keys: a "public" key and a "private" key. "Public" keys are published, but "private" keys are not. Sending an encrypted message to someone requires knowing his or her public key; decrypting that message requires knowing his or her private key.

When Internet traffic is encrypted with SSL, capturing non-content information on e-mail communication from a pen-trap device is possible only after the traffic is decrypted. Because Internet communications closely intermingle content with non-content, pen-trap devices by necessity scan network traffic but exclude from any report to law enforcement officers all information relating to the subject line and body of the communication. *See* 18 U.S.C. § 3127; *Hogan Order,* 416 F. Supp. 2d at 17-18. A pen-trap device, by definition, cannot expose to law enforcement officers the content of any communication. *See id.*

FACTS

The information at issue before the court is relevant to an ongoing criminal investigation of ████████████ for violations of numerous federal statutes.████████

██

4

A. Section 2703(d) Order

The criminal investigation has revealed that ███████ has utilized and continues to utilize an e-mail account, ███████████████████ obtained through Lavabit, an electronic communications service provider. ████████████████████████████████ ██ ██ ██ On June 10, 2013, the United States obtained an order pursuant to 18 U.S.C. § 2703(d) directing Lavabit to provide, within ten days, additional records and information about ███████ e-mail account. Lavabit's owner and operator, Mr. Ladar Levison, provided very little of the information sought by the June 10, 2013 order.

B. Pen-Trap Order

On June 28, 2013, the Honorable Theresa C. Buchanan entered an Order pursuant to 18 U.S.C. § 3123 authorizing the installation and use of pen-trap device on all electronic communications being sent from or sent to the electronic mail account ████████████████ ("Pen-Trap Order"). The Pen-Trap Order authorized the government to capture all (i) "non-content" dialing, routing, addressing, and signaling information sent to or from ███████████████ and (ii) to record the date and time of the initiation and receipt of such transmissions, to record the duration of the transmissions, and to record user log-in data on the ████████████████ all for a period of sixty days. Judge Buchanan further ordered Lavabit to furnish agents of the Federal Bureau of Investigation ("FBI"), "forthwith, all information, facilities, and technical assistance necessary to accomplish the installation and use of the pen-trap

device." Pen-Trap Order at 2. The government was also ordered to "take reasonable steps to ensure that the monitoring equipment is not used to capture any" content-related information. *Id.* Pursuant to 18 U.S.C. § 3123(d), Judge Buchanan ordered that the Pen-Trap Order and accompanying application be sealed. *Id.*

Later on June 28, 2013, two FBI Special Agents served a copy of the Pen-Trap Order on Mr. Levison. Mr. Levison informed the FBI Special Agents that emails were encrypted as they were transmitted to and from the Lavabit server as well as when they were stored on the Lavabit server. In addition, decryption keys would be necessary to access any e-mails. Mr. Levison did not provide the keys to the Agents in that meeting. In an email to Mr. Levison on July 6, 2013, a FBI Special Agent re-affirmed the nature of the information requested in the pen-trap order. In a response on the same day, Levison claimed "we don't record this data".

C. Compliance Order

Mr. Levison did not comply with the Pen-Trap Order. Accordingly, in the evening of June 28, 2013, the government obtained an Order Compelling Compliance Forthwith from U.S. Magistrate Judge Theresa C. Buchanan ("Compliance Order"). The Compliance Order directed Lavabit to comply with the Pen-Trap Order and to "provide the Federal Bureau of Investigation with unencrypted data pursuant to the Order." Lavabit was further ordered to provide "any information, facilities, or technical assistance are under the control of Lavabit [that] are needed to provide the FBI with the unencrypted data." Compliance Order at 2. The Compliance Order indicated that failing to comply would subject Lavabit to any penalty in the power of the court, "including the possibility of criminal contempt of Court." *Id.*

D. Order to Show Cause

Mr. Levison did not comply with the Compliance Order. On July 9, 2013, this Court ordered Mr. Levison to appear on July 16, 2013, to show cause why Lavabit has failed to comply with the Pen-Trap Order and Compliance Order.

The following day, on July 10, 2013, the United States Attorney's Office arranged a conference call involving the United States Attorney's Office, the FBI, Mr. Levison and Mr. Levison's attorney at the time, Marcia Hofmann. During this call, the parties discussed implementing the pen-trap device in light of the encryption in place on the target e-mail account. The FBI explained, and Mr. Levison appeared to agree, that to install the pen-trap device and to obtain the unencrypted data stream necessary for the device's operation the FBI would require (i) access to Lavabit's server and (ii) encryption keys.

E. Grand Jury Subpoena

On July 11, 2013, the United States Attorney's Office issued a grand jury subpoena for Mr. Levison to testify in front of the grand jury on July 16, 2013. The subpoena instructed Mr. Levison to bring to the grand jury his encryption keys and any other information necessary to accomplish the installation and use of the pen-trap device pursuant to the Pen-Trap Order.[1] The FBI attempted to serve the subpoena on Mr. Levison at his residence. After knocking on his door, the FBI Special Agents witnessed Mr. Levison exit his apartment from a back door, get in his car, and drive away. Later in the evening, the FBI successfully served Mr. Levison with the subpoena.

---

[1] The grand jury subpoena was subsequently sealed on July 16, 2013.

On July 13, 2013, Mr. Levison sent an e-mail to Assistant United States Attorney ███████████ stating, in part:

> In light of the conference call on July 10th and after subsequently reviewing the requirements of the June 28th order I now believe it would be possible to capture the required data ourselves and provide it to the FBI. Specifically the information we'd collect is the login and subsequent logout date and time, the IP address used to connect to the subject email account and the following non-content headers (if present) from any future emails sent or received using the subject account. The headers I currently plan to collect are: To, Cc, From, Date, Reply-To, Sender, Received, Return-Path, Apparently-To and Alternate-Recipient. Note that additional header fields could be captured if provided in advance of my implementation effort.
>
> $2,000 in compensation would be required to cover the cost of the development time and equipment necessary to implement my solution. The data would then be collected manually and provided at the conclusion of the 60 day period required by the Order. I may be able to provide the collected data intermittently during the collection period but only as my schedule allows. If the FBI would like to receive the collected information more frequently I would require an additional $1,500 in compensation. The additional money would be needed to cover the costs associated with automating the log collection from different servers and uploading it to an an FBI server via "scp" on a daily basis. The money would also cover the cost of adding the process to our automated monitoring system so that I would notified automatically if any problems appeared.

The e-mail again confirmed that Lavabit is capable of providing the means for the FBI to install the pen-trap device and obtain the requested information in an unencrypted form. AUSA ███████ replied to Mr. Levison's e-mail that same day, explaining that the proposal was inadequate because, among other things, it did not provide for real-time transmission of results, and it was not clear that Mr. Levison's request for money constituted the "reasonable expenses" authorized by the statute.

F. Search Warrant & 2705(b) Non-Disclosure Order

On July 16, 2013, this Court issued a search warrant to Lavabit for (i) "[a]ll information necessary to decrypt communications sent to or from the Lavabit e-mail account ███████████████, including encryption keys and SSL keys" and (ii)

8

"[a]ll information necessary to decrypt data stored in or otherwise associated with the Lavabit account ███████████████████" Pursuant to 18 U.S.C. § 2705(b), the Court ordered Lavabit to not disclose the existence of the search warrant upon determining that "there is reason to believe that notification of the existence of the . . . warrant will seriously jeopardize the investigation, including by giving target an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or notify confederates." July 16, 2013 Order ("Non-Disclosure Order") at 1.

G. Rule 49 Sealing Order

The search warrant and accompanying materials were further sealed by the Court on July 16, 2013, pursuant to a Local Rule 49(B) ("Rule 49 Order"). In the Rule 49 Order, the Court found that "revealing the material sought to be sealed would jeopardize an ongoing criminal investigation." The sealing order was further justified by the Court's consideration of "available alternatives that are less drastic than sealing, and finding none would suffice to protect the government's legitimate interest in concluding the investigation; and having found that this legitimate government interest outweighs at this time any interest in the disclosure of the material." Rule 49 Order at 1.

H. Show Cause Hearing

At the Show Cause Hearing on July 16, 2013, Mr. Levison made an oral motion to unseal the proceedings and related filings. The government objected since unsealing the proceedings would jeopardize the ongoing criminal investigation of ██████. The Court denied Mr. Levison's motion. Mr. Levison subsequently indicated to the Court that he would permit the FBI to place a pen-trap device on his server. The government requested that the Court further order Mr. Levison to provide his SSL keys since placing

9

a pen-trap device on Lavabit's server would only provide encrypted information that would not yield the information required under the Pen-Trap Order. The government noted that Lavabit was also required to provide the SSL keys pursuant to the search warrant and grand jury subpoena. The Court determined that the government's request for the SSL keys was premature given that Mr. Levison had offered to place the pen-trap device on his server and the Court's order for a show cause hearing was only based on the failure to comply with the Pen-Trap Order. Accordingly, the Court scheduled a hearing for July 26, 2013, to determine whether Lavabit was in compliance with the Pen-Trap Order after a pen-trap device was installed.

I. Motion to Unseal and Lift Non-Disclosure Order

On July 25, 2013, Mr. Levison filed two motions—a Motion for Unsealing of Sealed Court Records ("Motion to Unseal") and a Motion to Quash Subpoena and Search Warrant ("Motion to Quash"). In the motions, Mr. Levison confirms that providing the SSL keys to the government would provide the data required under the Pen-Trap Order in an unencrypted form. Nevertheless, he refuses to provide the SSL keys. In order to provide the government with sufficient time to respond, the hearing was rescheduled for August 1, 2013.

On a later date, and after discussions with Mr. Levison, the FBI installed a pen-trap device on Lavabit's Internet service provider, which would capture the same information as if a pen-trap device was installed on Lavabit's server. Based on the government's ongoing investigation, it is clear that due to Lavabit's encryption services the pen-trap device is failing to capture data related to all of the e-mails sent to and from the account as well as other information required under the Pen-Trap Order. During

10

Lavabit's over one month of noncompliance with this Court's Pen-Trap Order, █████

███
███
███

ARGUMENT

I. **THE SEARCH WARRANT AND THE GRAND JURY SUBPOENA ARE LAWUL AND REQUIRE LAVABIT TO PRODUCE THE SSL KEYS**

  A. *The search warrant and grand jury subpoena are valid because they merely re-state Lavabit's pre-existing legal duty, imposed by the Pen-Trap Order, to produce information necessary to accomplish installation of the pen-trap device.*

The motion of Lavabit and Mr. Levison (collectively "Lavabit") to quash both the grand jury subpoena and the search warrant should be denied because the subpoena and warrant merely re-state and clarify Lavabit's obligation under the Pen-Trap Act to provide that same information. In total, four separate legal obligations currently compel Lavabit to produce the SSL keys:

1. The Pen-Trap Order pursuant to the Pen Register and Trap and Trace Device Act (18 U.S.C. §§ 3121-27);

2. The Compliance Order compelling compliance forthwith with the Pen-Trap Order;

3. The July 16, 2013, grand jury subpoena; and

4. The July 16, 2013, search warrant, issued by this Court under the Electronic Communications Privacy Act ("ECPA").

The Pen-Trap Act authorizes courts to order providers such as Lavabit to disclose "information" that is "necessary" to accomplish the implementation or use of a pen-trap. *See* 18 U.S.C. §§ 3123(b)(2); 3124(a); 3124(b). Judge Buchanan, acting under that authority, specifically required in the Pen-Trap Order that: "IT IS FURTHER

11

ORDERED, pursuant to 18 U.S.C. § 3123(b)(2), that Lavabit shall furnish agents from the Federal Bureau of Investigation, forthwith, all information, facilities, and technical assistance necessary to accomplish the installation and use of the pen/trap device unobtrusively and with minimum interference." Pen-Trap Order at 2.

In this case, the SSL keys are "information... necessary to accomplish the installation and use of the [pen-trap]" because all other options for installing the pen-trap have failed. In a typical case, a provider is capable of implementing a pen-trap by using its own software or device, or by using a technical solution provided by the investigating agency; when such a solution is possible, a provider need not disclose its key. *E.g., In re Application of the U.S. for an Order Authorizing the Use of a Pen Register and Trap On [XXX] Internet Serv. Account/User Name [xxxxxxx@xxx.com]*, 396 F. Supp. 2d 45, 49 (D. Mass. 2005) (suggesting language in a pen-trap order "to impose upon the internet service providers the necessity of making sure that they configure their software in such a manner as to disclose only that which has been authorized"). In this case, given Lavabit's use of SSL encryption and Lavabit's lack of a software solution to implement the pen-trap on behalf the government, neither the government nor Mr. Levison have been able to identify such a solution.

Because the search warrant and grand jury subpoena require nothing that the Pen-Trap Act does not already require, they are not unreasonably burdensome. Moreover, a court's constitutional authority to require a telecommunications provider to assist the government in implementing a pen-trap device is well-established. *See United States v. New York Tel. Co.*, 434 U.S. 159, 168-69 (1977) (in a pre-Pen-Trap Act case, holding that district court had the authority to order a phone company to assist in the installation of a

12

pen-trap, and "no claim is made that it was in any way inconsistent with the Fourth Amendment.").

> B. *Lavabit's motion to quash the search warrant must be denied because there is no statutory authority for such motions, and the search warrant is lawful in any event.*

>> 1. Lavabit lacks authority to move to suppress a search warrant.

Lavabit lacks authority to ask this Court to "quash" a search warrant before it is executed. The search warrant was issued under Title II of ECPA, 18 U.S.C. §§ 2701-2712. ECPA allows providers such as Lavabit to move to quash *court orders*, but does not create an equivalent procedure to move to quash search warrants. 18 U.S.C. § 2703(d). The lack of a corresponding motion to quash or modify a search warrant means that there is no statutory authority for such motions. *See* 18 U.S.C. § 2708 ("[t]he remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter."); *cf. In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F. Supp. 2d 114, 128-29 (E.D. Va. 2011) (holding that the lack of a specific provision in ECPA permitting users to move to quash court orders requires "the Court [to] infer that Congress deliberately declined to permit [such] challenges.").

>> 2. The search warrant complies with the Fourth Amendment and is not general.

The Fourth Amendment requires that a search warrant "particularly describe[e] the place to be searched, and the persons or things to be seized." U.S. Const. Am. IV. This "particularity requirement is fulfilled when the warrant identifies the items to be seized by their relation to designated crimes and when the description of the items leaves

nothing to the discretion of the officer executing the warrant." *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010).

The July 16, 2013, search warrant's specification easily meets this standard, and therefore is not impermissibly general. It calls for only:

> a. All information necessary to decrypt communications sent to or from the Lavabit e-mail account ██████████████████ including encryption keys and SSL keys;
>
> b. All information necessary to decrypt data stored in or otherwise associated with the Lavabit account ██████████████████

That specification leaves nothing to discretion; it calls for encryption and SSL keys and nothing else.

Acknowledging this specificity, Lavabit nonetheless argues that the warrant "operates as a general warrant by giving the Government access to every Lavabit user's communications and data." Mot. to Quash at 3. To the contrary, the warrant does not grant the government the legal authority to access *any* Lavabit user's communications or data. After Lavabit produces its keys to the government, Federal statutes, such as the Wiretap Act and the Pen-Trap Act, will continue to limit sharply the government's authority to collect any data on any Lavabit user—except for the one Lavabit user whose account is currently the subject of the Pen-Trap Order. *See* 18 U.S.C. § 2511(1) (punishing as a felony the unauthorized interception of communications); § 3121 (criminalizing the use of pen-trap devices without a court order). It cannot be that a search warrant is "general" merely because it gives the government a tool that, *if abused contrary to law,* could constitute a general search. Compelling the owner of an apartment building to unlock the building's front door so that agents can search one apartment is not

14

a "general search" of the entire apartment building—even if the building owner imagines that undisciplined agents will illegally kick down the doors to apartments not described in the warrant.

C. *Lavabit's motion to quash the subpoena must be denied because compliance would not be unreasonable or oppressive*

A grand jury subpoena "may order the witness to produce any books, papers, documents, data, or other objects the subpoena designates," but the court "may quash or modify the subpoena if compliance would be unreasonable or oppressive." Fed. R. Crim. P. 17(c)(1) & (2); *see In re Grand Jury, John Doe No. G.J.2005-2,* 478 F.3d 581, 585 (4th Cir. 2007) (recognizing courts may quash subpoenas that are "abusive or harassing").[2]

Lavabit argues the subpoena should be quashed because it "grant[s] the Government unlimited access to every one of its user's accounts." Mot. to Quash at 7. As explained above, the subpoena does no such thing: It merely reaffirms Lavabit's existing obligation to provide information necessary to implement this Court's Pen-Trap Order on a single Lavabit customer's e-mail account. The Pen-Trap Order further restricts the government's access by preventing the government from collecting the content of that Lavabit customer's e-mail communications.

Lavabit also argues that it will lose customers' trust and business if it they learn that Lavabit provided the SSL keys to the government. But Lavabit finds itself in the position of having to produce those keys only because, more than a month after the Pen-Trap Order, Lavabit has failed to assist the government to implement the pen-trap device.

---

[2] Lavabit cites 18 U.S.C. § 2703(d) as authority for its motion to quash, but that section by its terms only permits motions to quash court orders issued under that same section.

Any resulting loss of customer "trust" is not an "unreasonable" burden if Lavabit's customers trusted that Lavabit would refuse to comply with lawful court orders. All providers are statutorily required to assist the government in the implementation of pen-traps, *see* 18 U.S.C. § 3124(a), (b), and requiring providers to comply with that statute is neither "unreasonable" nor "oppressive." In any event, Lavabit's privacy policy tells its customers that "Lavabit will not release any information related to an individual user *unless legally compelled to do so.*" *See* http://lavabit.com/privacy_policy.html (emphasis added).

Finally, once court-ordered surveillance is complete, Lavabit will be free to change its SSL keys. Vendors sell new SSL certificates for approximately $100. *See, e.g.,* GoDaddy LLC, SSL Certificates, https://www.godaddy.com/ssl/ssl-certificates.aspx. Moreover, Lavabit is entitled to compensation "for such reasonable expenses incurred in providing" assistance in implementing a pen-trap device. 18 U.S.C. § 3124(c).

II. THE NON-DISCLOSURE ORDER IS CONSISTENT WITH THE FIRST AMENDMENT BECAUSE IT IS NARROWLY TAILORED TO SERVE WHAT ALL PARTIES AGREE IS A COMPELLING GOVERNMENT INTEREST

Lavabit has asked the Court to unseal all of the records sealed by this Court's Order to Seal, and to lift the Court's Order dated July 16, 2013, directing Lavabit not to disclose the existence of the search warrant the Court signed that day ("Non-Disclosure Order"). Motion for Unsealing of Sealed Court Records and Removal of Non-Disclosure Order ("Mot. to Unseal") at 1-2. Lavabit, however, has not identified (and cannot) any compelling reason sufficient to overcome what even Lavabit concedes is the government's compelling interest in maintaining the secrecy and integrity of its active investigation ███████████. Moreover, the restrictions are narrowly tailored to restrict

16

Lavabit from discussing only a limited set of information disclosed to them as part of this investigation. Because there is no reason to jeopardize the criminal investigation, this motion must be denied.

A.   *The Non-Disclosure Order survives even strict scrutiny review by imposing necessary but limited secrecy obligations on Lavabit*

The United States does not concede that strict scrutiny must be applied in reviewing the Non-Disclosure Order. There is no need to decide this issue, however, because the Non-Disclosure Order is narrowly tailored to advance a compelling government interest, and therefore easily satisfies strict scrutiny.

The Government has a compelling interest in protecting the integrity of on-going criminal investigations. *Virginia Dep't of State Police v. Wash. Post*, 386 F.3d 567, 579 (4th Cir. 2004) ("We note initially our complete agreement with the general principle that a compelling governmental interest exists in protecting the integrity of an ongoing law enforcement investigation"); *Branzburg v. Hayes*, 408 U.S. 665, 700 (1972) ("requirements ... that a State's interest must be 'compelling' ...are also met here. As we have indicated, the investigation of crime by the grand jury implements a fundamental governmental role of securing the safety of the person and property of the citizen ...."). Indeed, it is "obvious and unarguable that no government interest is more compelling than the security of the Nation." *Haig v. Agee*, 453 U.S. 280, 307 (1981) (internal quotation marks omitted); *see also Dep't of the Navy v. Egan*, 484 U.S. 518, 527 (1988) ("This Court has recognized the Government's 'compelling interest' in withholding national security information from unauthorized persons in the course of executive business"). Likewise, here, the United States clearly has a compelling interest in ensuring that the target of lawful surveillance is not aware that he is being monitored.

17

United States v. Aguilar, 515 U.S. 593, 606 (1995) (holding that a statute prohibiting disclosure of a wiretap was permissible under the First Amendment, in part because "[w]e think the Government's interest is quite sufficient to justify the construction of the statute as written, without any artificial narrowing because of First Amendment concerns"). As the Non-Disclosure Order makes clear, publicizing "the existence of the [search] warrant 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."

Lavabit acknowledges that "the government has a compelling interest in maintaining the integrity of its criminal investigation of ███████████". Mot. to Unseal at 4; *id.* at 6 ("the government has a legitimate interest in tracking" ███████████ account); *id.* at 8 ("the secrecy of [Stored Communications Act] investigations is a compelling government interest"). In spite of this recognition, Lavabit states it intends to disclose the search warrant and order should the Court grant the Motion to Unseal. *Id.* at 5 ("Mr. Levinson needs some ability to voice his concerns [and] garner support for his cause"); *id.* at 6. Disclosure of electronic surveillance process *before the electronic surveillance has finished*, would be unprecedented and defeat the very purpose of the surveillance. Such disclosure would ensure that ███████████, along with the public, would learn of the monitoring of ██ e-mail account and take action to frustrate the legitimate monitoring of that account.

The Non-Disclosure Order is narrowly tailored to serve the government's compelling interest of protecting the integrity of its investigation. The scope of information that Lavabit may not disclose could hardly be more narrowly drawn: "the

18

existence of the attached search warrant" and the Non-Disclosure Order itself.

Restrictions on a party's disclosure of information obtained through participation in confidential proceedings stand on a different *and firmer* constitutional footing from restrictions on the disclosure of information obtained by independent means. *Seattle Times Co. v. Rhinehart,* 467 U.S. 20, 33 (1984) (order prohibiting disclosure of information learned through judicial proceeding "is not the kind of classic prior restraint that requires exacting First Amendment scrutiny"); *Butterworth v. Smith,* 494 U.S. 624, 632 (1990) (distinguishing between a witness' "right to divulge information of which he was in possession before he testified before the grand jury" with "information which he may have obtained as a result of his participation in the proceedings of the grand jury"); *see also Hoffman-Pugh v. Keenan,* 338 F.3d 1136, 1140 (10th Cir. 2003) (finding prohibition on disclosing information learned through grand jury process, as opposed to information person already knew, does not violate First Amendment). In *Rhinehart,* the Court found that "control over [disclosure of] the discovered information does not raise the same specter of government censorship that such control might suggest in other situations." 467 U.S. at 32.

Further, the Non-Disclosure Order is temporary. The nondisclosure obligation will last only so long as necessary to protect the government's ongoing investigation.

> B.   *The Order neither forecloses discussion of an "entire topic" nor constitutes an unconstitutional prior restraint on speech*

The limitation imposed here does not close off from discussion an "entire topic," as articulated in *Consolidated Edison.* Mot. to Unseal at 4. At issue in that case was the constitutionality of a state commission's order prohibiting a regulated utility from including inserts in monthly bills that discussed *any* controversial issue of public policy,

such as nuclear power. *Consolidated Edison Co. of New York v. Pub. Serv. Comm'n of New York*, 447 U.S. 530, 532 (1980). The Non-Disclosure Order, by contrast, precludes a single individual, Mr. Levison, from discussing a narrow set of information he did not know before this proceeding commenced, in order to protect the integrity of an ongoing criminal investigation. *Cf. Doe v. Mukasey*, 549 F.3d 861, 876 (2d Cir. 2009) ("although the nondisclosure requirement is triggered by the content of a category of information, that category, consisting of the fact of receipt of [a National Security Letter] and some related details, is far more limited than the broad categories of information that have been at issue with respect to typical content-based restrictions."). Mr. Levison may still discuss everything he could discuss before the Non-Disclosure Order was issued.

Lavabit's argument that the Non-Disclosure Order, and by extension all § 2705(b) orders, are unconstitutional prior restraints is likewise unavailing. Mot. To Unseal at 5-6. As argued above, the Non-Disclosure Order is narrowly tailored to serve compelling government interests, and satisfies strict scrutiny. *See supra*, Part II.A. Regardless, the Non-Disclosure Order does not fit within the two general categories of prior restraint that can run afoul of the First Amendment: licensing regimes in which an individual's right to speak is conditioned upon prior approval from the government, *see City of Lakewood v. Plain Dealer Publishing Co.*, 486 U.S. 750, 757 (1988), and injunctions restraining certain speech and related activities, such as publishing defamatory or scandalous articles, showing obscene movies, and distributing leaflets, *see Alexander v. United States*, 509 U.S. 544, 550 (1993). A prior restraint denies a person the ability to express viewpoints or ideas they could have possessed without any government involvement. Section 2705(b) orders, by contrast, restrict a recipient's ability to disclose limited

information that the recipient only learned from the government's need to effectuate a legitimate, judicially sanctioned form of monitoring. Such a narrow limitation on information acquired only by virtue of an official investigation does not raise the same concerns as other injunctions on speech. *Cf. Rhinehart*, 467 U.S. at 32, *Doe v. Mukasey*, 549 F.3d at 877 ("[t]he non-disclosure requirement" imposed by the national security letter statute "is not a typical prior restraint or a typical content-based restriction warranting the most rigorous First Amendment scrutiny").

III. NO VALID BASIS EXISTS TO UNSEAL DOCUMENTS THAT, IF MADE PUBLIC PRE-MATURELY, WOULD JEOPARDIZE AN ON-GOING CRIMINAL INVESTIGATION

A.   Any common law right of access is outweighed by the need to protect the integrity of the investigation.

Lavabit asserts that the common law right of access necessitates reversing this Court's decision to seal the search warrant and supporting documents. Mot. to Unseal at 7-10. The presumption of public access to judicial records, however, is "qualified," *Balt. Sun Co. v. Goetz*, 886 F.2d 60, 65 (4th Cir. 1989), and rebuttable upon a showing that the "public's right of access is outweighed by competing interests," *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d)*, 707 F.3d 283, 290 (4th Cir. 2013) ("*Twitter*"). In addition to considering substantive interests, a judge must also consider procedural alternatives to sealing judicial records. *Twitter*, 707 F.3d at 294. "Adherence to this procedure serves to ensure that the decision to seal materials will not be made lightly and that it will be subject to meaningful appellate review." *Va. Dep't of State Police v. Wash. Post*, 386 F.3d 567, 576 (4th Cir. 2004). This standard is met easily here.

"[T]he common law does not afford as much substantive protection to the interests of the press and the public as does the First Amendment." *Twitter*, 707 F.3d at 290 (internal quotation marks omitted). With respect to the substantive equities at stake, the United States' interest in maintaining the secrecy of a criminal investigation to prevent the target of the surveillance from being alerted and altering behavior to thwart the surveillance clearly outweighs any public interest in learning about specific acts of surveillance. *Id.* at 294 (rejecting common law right of access because, *inter alia*, the sealed documents "set forth sensitive non-public facts, including the identity of targets and witnesses in an ongoing criminal investigation"). "Because secrecy is necessary for the proper functioning of the criminal investigation" prior to indictment, "openness will frustrate the government's operations." *Id.* at 292. Lavabit concedes that ensuring "the secrecy of [Stored Communications Act] investigations," like this, "is a *compelling government interest*." Mot. to Unseal at 8 (emphasis added). Lavabit does not, however, identify any compelling interests to the contrary. Far from presenting "a seriously concerning expansion of grand jury subpoena power," as Lavabit's contents, *id.*, a judge issued the Pen-Trap Order, which did not authorize monitoring of any Lavabit e-mail account other than ▮▮▮▮▮▮

In addition, the Court satisfied the procedural prong. It "considered the available alternatives that are less drastic than sealing, and [found] none would suffice to protect the government's legitimate interest in concluding the investigation." Rule 49 Order.

The Fourth Circuit's decision in *Twitter* is instructive. That case arose from the Wikileaks investigation of Army Pfc. Bradley Manning. Specifically, the government obtained an order pursuant to 18 U.S.C. § 2703(d) directing Twitter to disclose electronic

communications and account and usage information pertaining to three subscribers. When apprised of this, the subscribers asserted that a common law right of access required unsealing records related to the § 2703(d) order. The Fourth Circuit rejected this claim, finding that the public's interest in the Wikileaks investigation and the government's electronic surveillance of internet activities did not outweigh "the Government's interests in maintaining the secrecy of its investigation, preventing potential suspects from being tipped off, or altering behavior to thwart the Government's ongoing investigation." 707 F.3d at 293. "The mere fact that a case is high profile in nature," the Fourth Circuit observed, "does not necessarily justify public access." *Id.* at 294. Though *Twitter* involved a § 2703(d) order, rather than a § 2705(b) order, the Court indicated this is a distinction without a difference. *Id.* at 294 (acknowledging that the concerns about unsealing records "accord" with § 2705(b)). Given the similarities between *Twitter* and the instant case—most notably the compelling need to protect otherwise confidential information from public disclosure and the national attention to the matter—there is no compelling rationale currently before the Court necessitating finding that a common law right of access exists here.

B.   *Courts have inherent authority to seal ECPA process*

Lavabit asserts that this Court must unseal the Non-Disclosure Order because 18 U.S.C. § 2705(b) does not explicitly reference the sealing of non-disclosure orders issued pursuant to that section. Mot. to Unseal at 9-10. As an initial matter, the Court has inherent authority to seal documents before it. *In re Knight Pub. Co.*, 743 F.2d 231, 235 (4th Cir. 1984) ("[t]he trial court has supervisory power over its own records and may, in its discretion, seal documents if the public's right of access is outweighed by competing

interests"); *see also Media General Operations, Inc. v. Buchanan*, 417 F3d. 424, 430 (4th Cir. 2005); *United States v. U.S. Dist. Court*, 407 U.S. 297, 321 (1972) ("a warrant application involves no public or adversary proceedings: it is an ex parte request before a magistrate or judge."). In addition, the Court here exercised its authority to seal pursuant to Local Rule 49(B), the validity of which Lavabit does not contest.

Even if the Court did not have this authority, Lavabit's reading of § 2705(b) must be rejected, because it would gut the essential function of non-disclosure orders and thereby disregard Congress' clear intent in passing § 2705. The Section allows courts to delay notification pursuant to § 2705(a) or issue a non-disclosure order pursuant to § 2705(b) upon finding that disclosure would risk enumerated harms, namely danger to a person's life or safety, flight from prosecution, destruction of evidence, intimidation of witnesses, or seriously jeopardizing an investigation. 18 U.S.C. §§ 2705(a)(2)(A)-(E), (b)(1)-(5). It would make no sense for Congress to purposefully authorize courts to limit disclosure of sensitive information while simultaneously intending to allow the same information to be publicly accessible in an unsealed court document.

Finally, the implications Lavabit attempts to draw from the mandatory sealing requirements of 18 U.S.C. §§ 2518(8)(b) and 3123(a)(3)(B) are mistaken. While Lavabit characterizes those statutes as granting courts the authority to seal Wiretap Act and pen-trap orders, courts already had that authority. Those statutes have another effect: they removed discretion from courts by *requiring* that courts seal Wiretap Act orders and pen-trap orders. *See* 18 U.S.C. § 2518(8)(b) ("Applications made and orders granted under this chapter *shall be sealed* by the judge") (emphasis added); *id.* § 3123(a)(3)(B) ("The record maintained under subparagraph (A) *shall be provided ex parte and under seal* to

24

the court") (emphasis added). Congress' decision to leave that discretion in place in other situations does not mean that Congress believed that only Wiretap Act and pen-trap orders may be sealed.

      C.   *Supposed privacy concerns do not compel a common law right of access to the sealed documents.*

Lavabit's brief ends with an argument that privacy interests require a common law right of access. Mot. to Unseal at 10-11. Lavabit, however, offers no legal basis for this Court to adopt such a novel argument, nor do the putative policy considerations Lavabit references outweigh the government's compelling interest in preserving the secrecy of its ongoing criminal investigation. Indeed, the most compelling interest currently before the Court is ensuring that the Court's orders requiring that Mr. Levison and Lavabit comply with legitimate monitoring be implemented forthwith and without additional delay, evasion, or resistance by Mr. Levison and Lavabit.

CONCLUSION

For the foregoing reasons, Lavabit's motions should be denied. Furthermore, the Court should enforce the Pen-Trap Order, Compliance Order, search warrant, and grand jury subpoena by imposing sanctions until Lavabit complies.

Respectfully Submitted,

NEIL H. MACBRIDE
United States Attorney

By:

Assistant United States Attorney
United States Attorney's Office
2100 Jamieson Ave.
Alexandria, VA 22314

703-299-3700

26

CERTIFICATE OF SERVICE

I hereby certify that on July 31, 2013, I e-mailed a copy of the foregoing

document to Lavabit's Counsel of Record:

Jesse R. Binnall
Bronley & Binnall, PLLC
10387 Main Street, Suite 201
Fairfax, VA 22030

███████████████████

███████████████████████████

Assistant United States Attorney
United States Attorney's Office
2100 Jamieson Ave.
Alexandria, VA 22314

████████████████████

703-299-3700

27

EXHIBIT 18

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES AUTHORIZING THE USE OF A PEN REGISTER/TRAP AND TRACE DEVICE ON AN ELECTRONIC MAIL ACCOUNT	) NO. 1:13 EC 297
IN THE MATTER OF THE SEARCH AND SEIZURE OF INFORMATION ASSOCIATED WITH ▮▮▮▮▮▮▮▮ THAT IS STORED AND CONTROLLED AT PREMISES CONTROLLED BY LAVABIT, LLC	) NO. 1:13 SW 522
IN RE GRAND JURY SUBPOENA	) NO. 13-1
	) **UNDER SEAL**
	) Alexandria, Virginia August 1, 2013 10:00 a.m.

TRANSCRIPT OF HEARING

BEFORE THE HONORABLE CLAUDE M. HILTON

UNITED STATES DISTRICT JUDGE

<u>APPEARANCES</u>:

For the United States: James Trump, Esq.
                           Michael Ben'Ary, Esq.
                           Josh Goldfoot, Esq.

For the Respondent: Jesse R. Binnall, Esq.

Court Reporter: Tracy L. Westfall, RPR, CMRS, CCR
Proceedings reported by machine shorthand, transcript produced
by computer-aided transcription.

```
 1                    P R O C E E D I N G S

 2         THE CLERK:  In re:  Case Nos. 1:13 EC 297, 1:13 SW 522,

 3    and Grand Jury No. 13-1.

 4         MR. TRUMP:  Good morning.  Jim Trump on behalf of the

 5    United States.

 6         THE COURT:  Good morning.

 7         MR. BINNALL:  Good morning, Your Honor.  Jesse Binnall

 8    on behalf of Lavabit and Mr. Levison.

 9         THE COURT:  All right.

10         MR. BINNALL:  May it please the Court.  We're before

11    the Court today on two separate motions, a motion to quash the

12    requirement of Lavabit to produce its encryption keys and the

13    motion to unseal and lift the nondisclosure requirements of

14    Mr. Levison.

15         Your Honor, the motion to quash in this arises because

16    the privacy of users is at -- of Lavabit's users are at stake.

17    We're not simply speaking of the target of this investigation.

18    We're talking about over 400,000 individuals and entities that

19    are users of Lavabit who use this service because they believe

20    their communications are secure.

21         By handing over the keys, the encryption keys in this

22    case, they necessarily become less secure.  In this case it is

23    true that the face of the warrant itself does limit the

24    documents or -- and communications to be viewed and the specific

25    metadata to be viewed to the target of the case,
```

1   However, there is a lack of any sort of check or

2   balance in order to ensure that the -- that the encrypted data

3   of other Lavabit users remain secure. The encryption in this

4   case doesn't protect only content. It protects login data and

5   the other -- some of the other metadata involved in this case.

6   We believe that this is not the least restrictive means

7   in order to provide the government the data that they are

8   looking for. Specifically --

9   THE COURT: You have two different encryption codes,

10   one for the logins and the messages that are transmitted. You

11   have another code that encrypts the content of the messages,

12   right?

13   MR. BINNALL: Your Honor, I believe that that is true.

14   From my understanding of the way that this works is

15   that there is one SSL key. That SSL key is what is issue in

16   this case, and that SSL key specifically protects the

17   communication, the over -- the breadth of the communication

18   itself from the user's actual computer to the server to make

19   sure that the user is communicating with exactly who the user

20   intends to be communicating with, the server.

21   And that's one of the things that SSL does. It ensures

22   that you're talking to the right person via e-mail and there's

23   not a so-called man in the middle who's there to take that

24   message away.

25   THE COURT: Does that key also contain the code of the

1   message and interpret the message as well?

2   MR. BINNALL: My understanding is that it does, Your

3   Honor, but because that's not my technical expertise, I'm not

4   going to represent to the Court anything on that one way or

5   another. But my understanding is there is one general key here

6   that is at issue.

7   THE COURT: Well, why would you set up such? I mean, a

8   telephone, you've got telephone numbers and --

9   MR. BINNALL: Correct.

10   THE COURT: -- those can be traced very easily without

11 any look at the content of the message that's there. You-all

12 could have set up something the same way.

13   MR. BINNALL: We could have, Your Honor. Actually, if

14 you're to --

15   THE COURT: So if anybody's -- you're blaming the

16 government for something that's overbroad, but it seems to me

17 that your client is the one that set up the system that's

18 designed not to protect that information, because you know that

19 there needs to be access to calls that go back and forth to one

20 person or another. And to say you can't do that just because

21 you've set up a system that everybody has to -- has to be

22 unencrypted, if there's such a word, that doesn't seem to me to

23 be a very persuasive argument.

24   MR. BINNALL: I understand the Court's point, and this

25 is the way that I understand why it's done that way.

1   There's different security aspects involved for people

2   who want to protect their privacy, and there certainly is the

3   actual content of the message themselves. That's certainly what

4   I would concede is the highest security interest.

5   But there's also the security interest to make sure

6   that they're communicating with who you want to be communicating

7   with. That is equally of a concern for privacy issues because

8   that is, at the end of the day, one of the things that secures

9   the content of the message.

10   In this case it is true that most Internet service

11   providers do log, is what they call it, a lot of the metadata

12   that the government wants in this case without that necessarily

13   being encrypted, things such as who something is going to, who

14   it's going from, the time it's being sent, the IP address from

15   which it is being sent.

16   Lavabit code is not something that you buy off the

17   shelf. It is code that was custom made. It was custom made in

18   order to secure privacy to the largest extent possible and to be

19   the most secure way possible for multiple people to communicate,

20   and so it has chosen specifically not to log that information.

21   Now, that is actually information that my client has

22   offered to start logging with the particular user in this case.

23   It is, however, something that is quite burdensome on him. It

24   is something that would be custom code that would take between

25   20 to 40 hours for him to be able to produce. We believe that

1   is a better alternative than turning over the encryption key

2   which can be used to get the data for all Lavabit users.

3   I hope that addresses the Court's concern kind of with

4   regard to the metadata and why it is not more -- why Lavabit

5   hasn't created an encryption system that may honestly be more

6   within the mainstream, but this is a provider that specifically

7   was started in order to have to protect privacy interests more

8   than the average Internet service provider.

9   THE COURT: I can understand why the system was set up,

10 but I think the government is -- government's clearly entitled

11 to the information that they're seeking, and just because

12 you-all have set up a system that makes that difficult, that

13 doesn't in any way lessen the government's right to receive that

14 information just as they would from any telephone company or any

15 other e-mail source that could provide it easily. Whether

16 it's -- in other words, the difficulty or the ease in obtaining

17 the information doesn't have anything to do with whether or not

18 the government's lawfully entitled to the information.

19   MR. BINNALL: It is -- and we don't disagree that the

20 government is entitled to the information. We actually --

21   THE COURT: Well, how are we going to get it? I'm

22 going to have to deny your motion to quash. It's just not

23 overbroad. The government's asking for a very narrow, specific

24 bit of information, and it's information that they're entitled

25 to.

1   Now, how are we going to work out that they get it?

2   MR. BINNALL: Your Honor, what I would still say is the

3 best method for them to get it is, first of all, there be some

4 way for there to be some sort of accountability other than just

5 relying on the government to say we're not going to go outside

6 the scope of the warrant.

7   This is nothing that is, of course, personal against

8 the government and the, you know, very professional law

9 enforcement officers involved in this case. But quite simply,

10 the way the Constitution is set up, it's set up in a way to

11 ensure that there's some sort of checks and balances and

12 accountability.

13   THE COURT: What checks and balances need to be set up?

14   MR. BINNALL: Well --

15   THE COURT: Suggest something to me.

16   MR. BINNALL: I think that the least restrictive means

17 possible here is that the government essentially pay the

18 reasonable expenses, meaning in this case my client's extensive

19 labor costs to be capped at a reasonable amount.

20   THE COURT: Has the government ever done that in one of

21 these pen register cases?

22   MR. BINNALL: Not that I've found, Your Honor.

23   THE COURT: I don't think so. I've never known of one.

24   MR. BINNALL: And Your Honor's certainly seen more of

25 these than I have.

1   THE COURT: So would it be reasonable to start now with

2 your client?

3   MR. BINNALL: I think everyone would agree that this is

4 an unusual case. And that this case, in order to protect the

5 privacy of 400,000-plus other users, some sort of relatively

6 small manner in which to create a log system for this one user

7 to give the government the metadata that they're looking for is

8 the least restrictive mean here, and we can do that in a way

9 that doesn't compromise the security keys.

10   This is actually a way that my client --

11   THE COURT: You want to do it in a way that the

12 government has to trust you --

13   MR. BINNALL: Yes, Your Honor.

14   THE COURT: -- to come up with the right data.

15   MR. BINNALL: That's correct, Your Honor.

16   THE COURT: And you won't trust the government. So why

17 would the government trust you?

18   MR. BINNALL: Your Honor, because that's what the basis

19 of Fourth Amendment law says is more acceptable, is that the

20 government is the entity that you really need the checks and

21 balances on.

22   Now, my --

23   THE COURT: I don't know that the Fourth Amendment says

24 that. This is a criminal investigation.

25   MR. BINNALL: That is absolutely correct.

1   THE COURT: A criminal investigation, and I don't know

2   that the Fourth Amendment says that the person being

3   investigated here is entitled to more leeway and more rights

4   than the government is. I don't know.

5   MR. BINNALL: There certainly is a balance of power

6   there. I, of course, am not here to represent the interest of

7   ███████████████   I'm here specifically looking over my client who

8   has sensitive data --

9   THE COURT: I understand. I'm trying to think of

10   working out something. I'm not sure you're suggesting anything

11   to me other than either you do it and the government has to

12   trust you to give them whatever you want to give them or you

13   have to trust the government that they're not going to go into

14   your other files.

15   Is there some other route?

16   MR. BINNALL: I would suggest that the government --

17   I'm sorry -- that the Court can craft an order to say that we

18   can -- that we should work in concert with each other in order

19   to come up with this coding system that gives the government all

20   of the metadata that we can give them through this logging

21   procedure that we can install in the code, and then using that

22   as a least restrictive means to see if that can get the

23   government the information that they're looking for on the

24   specific account.

25   THE COURT: How long does it take to install that?

1   MR. BINNALL: I mean, 20, 40 hours. So I would suggest

2   that would probably be a week to a week and a half, Your Honor,

3   although I would be willing to talk to my client to see if we

4   can get that expedited.

5   THE COURT: To install it?

6   MR. BINNALL: Well, to write the code.

7   THE COURT: You don't have a code right at the moment.

8   You would have to write something?

9   MR. BINNALL: That's correct. And the portion of the

10   government's brief that talks about the money that he was

11   looking for is that reasonable expense for him basically to do

12   nothing for that period of time but write code to install in

13   order to take the data from ██████████ and put it in a way that

14   the government will see the logged metadata involved.

15   THE COURT: All right. I think I understand your

16   position. I don't think you need to argue this motion to

17   unseal. This is a grand jury matter and part of an ongoing

18   criminal investigation, and any motion to unseal will be denied.

19   MR. BINNALL: If I could have the Court's attention

20   just on one issue of the nondisclosure provision of this. And I

21   understand the Court's position on this, but there is other

22   privileged communications if the Court would be so generous as

23   to allow me very briefly to address that issue?

24   There's other First Amendment considerations at issue

25   with not necessarily just the sealing of this, but what

1   Mr. Levison can disclose and to whom he may disclose it.

2   The First Amendment, of course, doesn't just cover

3   speech and assembly, but the right to petition for a redress of

4   grievances. We're talking about a statute here, and, honestly,

5   a statute that is very much in the public eye and involving

6   issues that are currently pending before Congress.

7   I think the way that the order currently is written,

8   besides being --

9   THE COURT: You're talking about the sealing order?

10   MR. BINNALL: I'm talking about the sealing order and

11 the order that prohibits Mr. Levison from disclosing any

12 information.

13   Now, we don't want to disclose -- we have no intention

14 of disclosing the target, but we would like to be able to, for

15 instance, talk to members of the legislature and their staffs

16 about rewriting this in a way that's --

17   THE COURT: No. This is an ongoing criminal

18 investigation, and there's no leeway to disclose any information

19 about it.

20   MR. BINNALL: And so at that point it will remain with

21 only Mr. Levison and his lawyers, and we'll keep it at that.

22   THE COURT: Let me hear from Mr. Trump.

23   Is there some way we can work this out or something

24 that I can do with an order that will help this or what?

25   MR. TRUMP: I don't believe so, Your Honor, because

1 you've already articulated the reason why is that anything done

2 by Mr. Levison in terms of writing code or whatever, we have to

3 trust Mr. Levison that we have gotten the information that we

4 were entitled to get since June 28th. He's had every

5 opportunity to propose solutions to come up with ways to address

6 his concerns and he simply hasn't.

7   We can assure the Court that the way that this would

8 operate, while the metadata stream would be captured by a

9 device, the device does not download, does not store, no one

10 looks at it. It filters everything, and at the back end of the

11 filter, we get what we're required to get under the order.

12   So there's no agents looking through the 400,000 other

13 bits of information, customers, whatever. No one looks at that,

14 no one stores it, no one has access to it. All we're going to

15 look at and all we're going to keep is what is called for under

16 the pen register order, and that's all we're asking this Court

17 to do.

18   THE COURT: All right. Well, I think that's

19 reasonable. So what is this before me for this morning other

20 than this motion to quash and unseal which I've ruled on?

21   MR. TRUMP: The only thing is to order the production

22 of the encryption keys, which just --

23   THE COURT: Hasn't that already been done? There's a

24 subpoena for that.

25   MR. TRUMP: There's a search warrant for it, the motion

1   to quash.

2   THE COURT: Search warrant.

3   MR. TRUMP: Excuse me?

4   THE COURT: I said subpoena, but I meant search

5   warrant.

6   MR. TRUMP: We issued both, Your Honor, but Your Honor

7   authorized the seizure of that information. And we would ask

8   the Court to enforce that by directing Mr. Levison to turn over

9   the encryption keys.

10   If counsel represents that that will occur, we can not

11 waste any more of the Court's time. If he represents that

12 Mr. Levison will not turn over the encryption keys, then we have

13 to discuss what remedial action this Court can take to require

14 compliance with that order.

15   THE COURT: Well, I will order the production of

16 those -- of those keys.

17   Is that simply Mr. Levison or is that the corporation

18 as well?

19   MR. TRUMP: That's one and the same, Your Honor.

20   Just so the record is clear. We understand from

21 Mr. Levison that the encryption keys were purchased

22 commercially. They're not somehow custom crafted by

23 Mr. Levison. He buys them from a vendor and then they're

24 installed.

25   THE COURT: Well, I will order that. If you will

1 present an order to me, I'll enter it later on.

2   MR. TRUMP: Thank you.

3   MR. BINNALL: Thank you, Your Honor.

4   As far as time frame goes, my client did ask me if the

5 Court did order this if the Court could give him approximately

6 five days in order to actually physically get the encryption

7 keys here. And so it will be -- or just some sort of reasonable

8 time frame to get the encryption keys here and in the

9 government's hands. He did ask me to ask exactly the manner

10 that those are to be turned over.

11   MR. TRUMP: Your Honor, we understand that this can be

12 done almost instantaneously, as soon as Mr. Levison makes

13 contact with an agent in Dallas, and we would ask that he be

14 given 24 hours or less to comply. This has been going on for a

15 month.

16   THE COURT: Yeah, I don't think 24 -- 24 hours would be

17 reasonable. Doesn't have to do it in the next few minutes, but

18 I would think something like this, it's not anything he has to

19 amass or get together. It's just a matter of sending something.

20   So I think 24 hours would be reasonable.

21   MR. BINNALL: Yes. Thank you, Your Honor.

22   THE COURT: All right. And you'll present me an order?

23   MR. TRUMP: We will, Your Honor. Thank you.

24   THE COURT: All right. Thank you-all, and we'll

25 adjourn until -- or stand in recess till 3 o'clock. Well,

1   recess till 9 o'clock tomorrow morning.

2   * * *
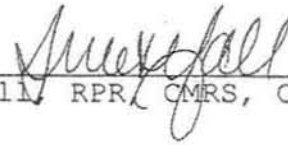
3   (Proceedings concluded at 10:25 a.m.)

4

5

6

7   _____

8

9   CERTIFICATION

10

11   I certify, this 19th day of August 2013, that the

12   foregoing is a correct transcript from the record of proceedings

13   in the above-entitled matter to the best of my ability.

14

15   /s/

16   Tracy Westfall, RPR, CMRS, CCR

17
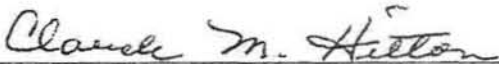
18

19

20

21

22

23

24

25

EXHIBIT 19

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE USE OF A PEN REGISTER/TRAP AND TRACE DEVICE ON AN ELECTRONIC MAIL ACCOUNT	)))))))	**UNDER SEAL** No. 1:13EC297
IN THE MATTER OF THE SEARCH AND SEIZURE OF INFORMATION ASSOCIATED WITH ▮▮▮▮▮▮▮▮▮▮▮▮▮ THAT IS STORED AT PREMISES CONTROLLED BY LAVABIT LLC	)))))))	No. 1:13SW522
In re Grand Jury	)	No. 13-1

ORDER DENYING MOTIONS

This matter comes before the Court on the motions of Lavabit LLC and Ladar Levinson,

its owner and operator, to (1) quash the grand jury subpoena and search and seizure warrant

compelling Lavabit LLC to provide the government with encryption keys to facilitate the

installation and use of a pen register and trap and trace device, and (2) unseal court records and

remove a non-disclosure order relating to these proceedings. For the reasons stated from the

bench, and as set forth in the government's response to the motions, it is hereby

ORDERED that the motion to quash and motion to unseal are DENIED;

It is further ORDERED that, by 5 p.m. CDT on August 2, 2013, Lavabit LLC and Ladar

Levison shall provide the government with the encryption keys and any other "information,

facilities, and technical assistance necessary to accomplish the installation and use of the pen/trap

device" as required by the July 16, 2013 seizure warrant and the June 28, 2013 pen register order.

It is further ORDERED that this Order shall remain under seal until further order of this

Court.

Claude M. Hilton
CLAUDE M. HILTON
UNITED STATES DISTRICT JUDGE

Alexandria, Virginia
August _/_ , 2013

EXHIBIT 20

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE)	**UNDER SEAL**
APPLICATION OF THE UNITED)	
STATES OF AMERICA FOR AN ORDER)	No. 1:13EC297
AUTHORIZING THE USE OF A PEN)	
REGISTER/TRAP AND TRACE DEVICE)	
ON AN ELECTRONIC MAIL ACCOUNT)	
)	
IN THE MATTER OF THE SEARCH AND)	
SEIZURE OF INFORMATION)	
ASSOCIATED WITH)	No. 1:13SW522
████████████████THAT IS)	
STORED AT PREMISES CONTROLLED)	
BY LAVABIT LLC)	
)	
In re Grand Jury)	No. 13-1
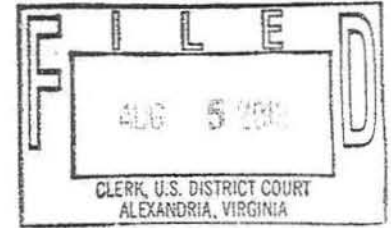
MOTION FOR SANCTIONS

The United States, through the undersigned counsel, pursuant to Title 18, United States

Code, Section 401, hereby moves for the issuance of an order imposing sanctions on Lavabit

LLC and Ladar Levison, its owner and operator, for Lavabit's failure to comply with this Court's

order entered August 1, 2013. In support of this motion, the United States represents:

1.   At the hearing on August 1, 2013, this Court directed Lavabit to provide the

government with the encryption keys necessary for the operation of a pen register/trap and trace

order entered June 28, 2013. Lavabit was ordered to provide those keys by 5 p.m. on August 2,

2013. *See* Order Denying Motions entered August 2, 2013.

2.   At approximately 1:30 p.m. CDT on August 2, 2013, Mr. Levison gave the FBI a

printout of what he represented to be the encryption keys needed to operate the pen register. This

printout, in what appears to be 4-point type, consists of 11 pages of largely illegible characters. *See* Attachment A. (The attachment was created by scanning the document provided by Mr. Levison; the original document was described by the Dallas FBI agents as slightly clearer than the scanned copy but nevertheless illegible.) Moreover, each of the five encryption keys contains 512 individual characters – or a total of 2560 characters. To make use of these keys, the FBI would have to manually input all 2560 characters, and one incorrect keystroke in this laborious process would render the FBI collection system incapable of collecting decrypted data.

3.   At approximately 3:30 p.m. EDT (2:30 p.m. CDT), the undersigned AUSA contacted counsel for Lavabit LLC and Mr. Levison and informed him that the hard copy format for receipt of the encryption keys was unworkable and that the government would need the keys produced in electronic format. Counsel responded by email at 6:50 p.m. EDT stating that Mr. Levison "thinks" he can have an electronic version of the keys produced by Monday, August 5, 2013.

4.   On August 4, 2013, the undersigned AUSA sent an e-mail to counsel for Lavabit LLC and Mr. Levison stating that we expect to receive an electronic version of the encryption keys by 10:00 a.m. CDT on Monday, August 5, 2013. The e-mail indicated that we expect the keys to be produced in PEM format, an industry standard file format for digitally representing SSL keys. *See* Attachment B. The e-mail further stated that the preferred medium for receipt of these keys would be a CD hand-delivered to the Dallas office of the FBI (with which Mr. Levison is familiar). The undersigned AUSA informed counsel for Lavabit LLC and Mr. Levison that the government would seek an order imposing sanctions if we did not receive the encryption keys in electronic format by Monday morning.

5. The government did not receive the electronic keys as requested. The undersigned AUSA spoke with counsel for Lavabit and Mr. Levison at approximately 10:00 a.m. this morning, and he stated that Mr. Levison might be able to produce the keys in electronic format by 5 p.m. on August 5, 2013. The undersigned AUSA told counsel that was not acceptable given that it should take Mr. Levison 5 to 10 minutes to put the keys onto a CD in PEM format. The undersigned AUSA told counsel that if there was some reason why it cannot be accomplished sooner, to let him know by 11:00 a.m. this morning. The government has not received an answer from counsel.

6. The government therefore moves the Court to impose sanctions on Lavabit LLC and Mr. Levison in the amount of $5000 per day beginning at noon (EDT) on August 5, 2013, and continuing each day in the same amount until Lavabit LLC and Mr. Levison comply with this Court's orders.

7. As noted, Attachment A to this motion is a copy of the printout provided by Mr. Levison on August 2, 2013. Attachment B is a more detailed explanation of how these encryption keys can be given to the FBI in an electronic format. Attachment C to this motion is a proposed order.

8.   A copy of this motion, filed under seal, was delivered by email to counsel for Lavabit LLC on August 5, 2013.

Respectfully submitted,

Neil H. MacBride
United States Attorney

By:

United States Attorney's Office
Justin W. Williams U.S. Attorney's Building
2100 Jamieson Avenue
Alexandria, Virginia 22314
Phone: 703-299-3700

Attachment A

ATTACHMENT B

Lavabit uses 2048-bit Secure Socket Layer (SSL) certificates purchased from GoDaddy to encrypt communication between users and its server. SSL encryption employs public-key cryptography, in which both the sender and receiver each have two mathematically linked keys: a "public" key and a "private" key. "Public" keys are published, but "private" keys are not. In this circumstance, a Lavabit customer uses Lavabit's published public key to initiate an encrypted email session with Lavabit over the internet. Lavabit's servers then decrypt this traffic using their private key. The only way to decrypt this traffic is through the usage of this private key. A SSL certificate is another name for a published public key.

To obtain a SSL certificate from GoDaddy, a user needs to first generate a 2048-bit private key on his/her computer. Depending on the operating system and web server used, there are multiple ways to generate a private key. One of the more popular methods is to use a freely available command-line tool called OpenSSL. This generation also creates a certificate signing request file. The user sends this file to the SSL generation authority (e.g. GoDaddy) and GoDaddy then sends back the SSL certificate. The private key is not sent to GoDaddy and should be retained by the user. This private key is stored on the user's web server to permit decryption of internet traffic, as described above. The FBI's collection system that will be installed to implement the PR/TT also requires the private key to be stored to decrypt Lavabit email and internet traffic. This decrypted traffic will then be filtered for the target email address specified in the PR/TT order.

Depending on how exactly the private key was first generated by the user, it itself may be encrypted and protected by a password supplied by the user. This additional level of security is useful if, for example, a backup copy of the private key is stored on a CD. If that CD was lost or stolen, the private key would not be compromised because a password would be required to access it. However, the user that generated the private key would have supplied it at generation time and would thus have knowledge of it. The OpenSSL tool described above is capable of decrypting encrypted private keys and converting the keys to a non-encrypted format with a simple, well-documented command. The FBI's collection system and most web servers requires the key to be stored in a non-encrypted format.

A 2048-bit key is composed of 512 characters. The standard practice of exchanging private SSL keys between entities is to use some electronic medium (e.g., CD or secure internet exchange). SSL keys are rarely, if ever, exchanged verbally or through print medium due to their long length and possibility of human error. Mr. Levison has previously stated that Lavabit actually uses five separate public/private key pairs, one for each type of mail protocol used by Lavabit.

PEM format is an industry-standard file format for digitally representing SSL keys. PEM files can easily be created using the OpenSSL tool described above. The preferred medium for receiving these keys would be on a CD.

EXHIBIT 21

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division
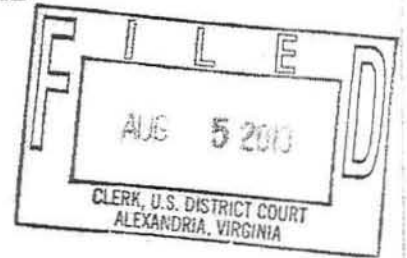
IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE USE OF A PEN REGISTER/TRAP AND TRACE DEVICE ON AN ELECTRONIC MAIL ACCOUNT	) **UNDER SEAL**)) No. 1:13EC297)))))
IN THE MATTER OF THE SEARCH AND SEIZURE OF INFORMATION ASSOCIATED WITH ████████████ THAT IS STORED AT PREMISES CONTROLLED BY LAVABIT LLC	)))) No. 1:13SW522))))
In re Grand Jury	) No. 13-1

ORDER

This matter comes before the Court on the motion of the government for sanctions for
failure to comply with this Court's order entered August 2, 2013. For the reasons stated in the
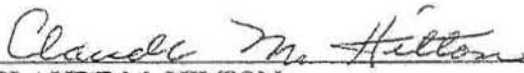government's motion, and pursuant to Title 18, United States Code, Section 401, it is hereby

ORDERED that the motion for sanctions is granted;

It is further ORDERED that, if the encryption keys necessary to implement the pen
register and trap and trace device are not provided to the FBI in PEM or equivalent electronic
format by noon (CDT) on August 5, 2013, a fine of five thousand dollars ($5,000.00) shall be
imposed on Lavabit LLC and Mr. Levison;

It is further ORDERED that, if the encryption keys necessary to implement the pen
register and trap and trace device are not provided to the FBI in PEM or equivalent electronic

format by noon (CDT) each day thereafter beginning August 6, 2013, a fine of five thousand dollars ($5,000.00) shall be imposed on Lavabit LLC and Mr. Levison for each day of non-compliance; and

It is further ORDERED that the government's motion for sanctions and this Order shall remain under seal until further order of this Court.

Claude M. Hilton
CLAUDE M. HILTON
UNITED STATES DISTRICT JUDGE

Alexandria, Virginia
August 5 , 2013

EXHIBIT 22

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

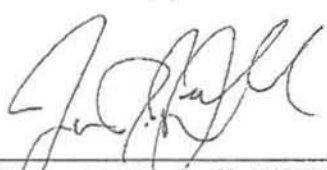|	
IN THE MATTER OF THE APPLICATION OF THE UNITED STATES AUTHORIZING THE USE OF A PEN REGISTER/TRAP AND TRACE DEVICE ON AN ELECTRONIC MAIL ACCOUNT	**FILED UNDER SEAL** No. 1:13EC297
IN THE MATTER OF THE SEARCH AND SEIZURE OF INFORMATION ASSOCIATED WITH ███████████ THAT IS STORED AND CONTROLLED AT PREMISES CONTROLLED BY LAVABIT LLC	No. 1:13SW522

NOTICE OF APPEAL

Notice is hereby given that Lavabit LLC ("Lavabit") and Mr. Ladar Levison

("Mr. Levison") in the above named case, hereby appeal to the United States

Court of Appeals for the Fourth Circuit from the Orders of this Court entered

on August 1, 2013 and August 5, 2013.

LAVABIT LLC
LADAR LEVISON
By Counsel

_____
Jesse R. Binnall, VSB# 79292
Bronley & Binnall, PLLC
10387 Main Street, Suite 201
Fairfax, Virginia 22030
(703) 229-0335 - Telephone
(703) 537-0780 - Facsimile
jbinnall@bblawonline.com
Counsel for Lavabit LLC

1

<u>Certificate of Service</u>

I certify that on this 15th day of August, 2013, this Notice of Appeal was emailed and mailed to the person at the addresses listed below:

United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314

Jesse R. Binnall

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

In re Grand Jury	**FILED UNDER SEAL** No. 13-1

NOTICE OF APPEAL

Notice is hereby given that Lavabit LLC ("Lavabit") and Mr. Ladar Levison

("Mr. Levison") in the above named case, hereby appeal to the United States

Court of Appeals for the Fourth Circuit from the Orders of this Court entered

on August 1, 2013 and August 5, 2013.

LAVABIT LLC
LADAR LEVISON
By Counsel

Jesse R. Binnall, VSB# 79292
Bronley & Binnall, PLLC
10387 Main Street, Suite 201
Fairfax, Virginia 22030
(703) 229-0335 - Telephone
(703) 537-0780 - Facsimile
jbinnall@bblawonline.com
Counsel for Lavabit LLC

1

Certificate of Service

I certify that on this 15th day of August, 2013, this Notice of Appeal was emailed and mailed to the person at the addresses listed below:

United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314

Jesse R. Binnall

2

EXHIBIT 23

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES AUTHORIZING THE USE OF A PEN REGISTER/TRAP AND TRACE DEVICE ON AN ELECTRONIC MAIL ACCOUNT	**FILED UNDER SEAL**
	No. 1:13SW522
IN THE MATTER OF THE SEARCH AND SEIZURE OF INFORMATION ASSOCIATED WITH ████████████ THAT IS STORED AND CONTROLLED AT PREMISES CONTROLLED BY LAVABIT LLC	

NOTICE OF APPEAL

Notice is hereby given that Lavabit LLC ("Lavabit") and Mr. Ladar Levison

("Mr. Levison") in the above named case, hereby appeal to the United States

Court of Appeals for the Fourth Circuit from the Orders of this Court entered

on August 1, 2013 and August 5, 2013.

**LAVABIT LLC
LADAR LEVISON**
By Counsel

_____
Jesse R. Binnall, VSB# 79292
Bronley & Binnall, PLLC
10387 Main Street, Suite 201
Fairfax, Virginia 22030
(703) 229-0335 - Telephone
(703) 537-0780 - Facsimile
jbinnall@bblawonline.com
Counsel for Lavabit LLC

Certificate of Service

I certify that on this 16th day of August, 2013, this Notice of Appeal was emailed and mailed to the person at the addresses listed below:

United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314

Jesse R. Binnall