U.S. District Court
Eastern District of Virginia - (Alexandria)
CRIMINAL DOCKET FOR CASE #: 1:13-sw-00522-CMH-1

Case title: USA v. In Re: Information Associated with [Redacted]

Date Filed: 07/16/2013
Date Terminated: 03/24/2015

Assigned to: District Judge Claude M. Hilton

Appeals court case number: 13-4625

Defendant (1)

In Re: Information Associated with [Redacted]
TERMINATED: 03/24/2015

Pending Counts	**Disposition**
None	

Highest Offense Level (Opening)

None

Terminated Counts	**Disposition**
None	

Highest Offense Level (Terminated)

None

Complaints	**Disposition**
None	

Interested Party

Ladar Levinson
TERMINATED: 03/24/2015

represented by **Jesse R. Binnall**
Harvev & Binnall PLLC

doing business as
Lavabit LLC
TERMINATED: 03/24/2015

717 King Street
Suite 300
Alexandria, VA 22314
703-888-1943
Fax: 703-888-1930
Email:
jbinnall@harveybinnall.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED
Designation: Retained

Plaintiff

USA represented by **James L. Trump**
United States Attorney's Office
2100 Jamieson Ave
Alexandria, VA 22314
(703)299-3700
Email: jim.trump@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Michael Ben'Ary
US Attorney's Office
(Alexandria-NA)
2100 Jamieson Avenue
Alexandria, VA 22314
NA
703-299-3700
Email:
michael.ben'ary2@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Tracy Doherty McCormick
US Attorney's Office
(Alexandria-NA)
2100 Jamieson Avenue
Alexandria, VA 22314
NA
703 299-3715
Email:
tracy.d.mccormick@usdoj.gov
ATTORNEY TO BE NOTICED
Designation: US Attorney

Date Filed	#	Docket Text
02/24/2016	36	ORDER granting 35 Motion to Unseal Document as to In Re: Information Associated with [Redacted] (1). ORDERED that the above-captioned cases are unsealed to allow the Clerk's Office to file on the public docket and make electronically available through CM/ECF the following pleadings, transcripts, and order as redacted in accordance with the Attachments to this Order. Signed by District Judge Claude M. Hilton on 2/24/2016. (Attachments: # 1 Attachment 1, # 2 Attachment 2, # 3 Attachment 3, # 4 Attachment 4, # 5 Attachment 5, # 6 Attachment 6, # 7 Attachment 7, # 8 Attachment 8, # 9 Attachment 9, # 10 Attachment 10, # 11 Attachment 11, # 12 Attachment 12, # 13 Attachment 13, # 14 Attachment 14, # 15 Attachment 15, # 16 Attachment 16, # 17 Attachment 17, # 18 Attachment 18, # 19 Attachment 19 Part 1, # 20 Attachment 19 Part 2, # 21 Attachment 19 Part 3, # 22 Attachment 19 Part 4, # 23 Attachment 19 Part 5, # 24 Attachment 19 Part 6, # 25 Attachment 19 Part 7, # 26 Attachment 19 Part 8, # 27 Attachment 19 Part 9, # 28 Attachment 19 Part 10, # 29 Attachment 20 Part 1, # 30 Attachment 20 Part 2, # 31 Attachment 20 Part 3, # 32 Attachment 21, # 33 Attachment 22, # 34 Attachment 23, # 35 Attachment 24, # 36 Attachment 25, # 37 Attachment 26, # 38 Attachment 27, # 39 Attachment 28, # 40 Attachment 29) (rban,) (Additional attachment(s) added on 3/4/2016: # 41 Redacted Docket Sheet) (rban,). (Entered: 03/04/2016)
03/04/2016		Case unsealed as to In Re: Information Associated with [Redacted] (rban,) (Entered: 03/04/2016)

Document Selection Menu

Select the document you wish to view.

Document Number: 36		4 pages	0.5 mb

Attachment	**Description**		
1	Attachment 1	12 pages	1.7 mb
2	Attachment 2	5 pages	0.5 mb
3	Attachment 3	5 pages	0.7 mb
4	Attachment 4	1 page	181 kb
5	Attachment 5	2 pages	291 kb
6	Attachment 6	1 page	173 kb
7	Attachment 7	2 pages	209 kb
8	Attachment 8	12 pages	1.8 mb
9	Attachment 9	10 pages	1.4 mb
10	Attachment 10	2 pages	214 kb
11	Attachment 11	1 page	95 kb
12	Attachment 12	12 pages	2.3 mb
13	Attachment 13	2 pages	219 kb
14	Attachment 14	2 pages	206 kb
15	Attachment 15	1 page	192 kb
16	Attachment 16	15 pages	2.1 mb
17	Attachment 17	2 pages	144 kb
18	Attachment 18	2 pages	145 kb
19	Attachment 19 Part 1	17 pages	8.6 mb
20	Attachment 19 Part 2	20 pages	9.1 mb
21	Attachment 19 Part 3	21 pages	2.2 mb
22	Attachment 19 Part 4	19 pages	9.2 mb
23	Attachment 19 Part 5	18 pages	9.1 mb
24	Attachment 19 Part 6	18 pages	9.3 mb
25	Attachment 19 Part 7	18 pages	9.4 mb

26	Attachment 19 Part 8	19 pages	9.4 mb
27	Attachment 19 Part 9	17 pages	9.4 mb
28	Attachment 19 Part 10	15 pages	7.1 mb
29	Attachment 20 Part 1	82 pages	9.4 mb
30	Attachment 20 Part 2	67 pages	9.4 mb
31	Attachment 20 Part 3	15 pages	1.8 mb
32	Attachment 21	2 pages	266 kb
33	Attachment 22	41 pages	6.4 mb
34	Attachment 23	4 pages	0.6 mb
35	Attachment 24	2 pages	188 kb
36	Attachment 25	26 pages	4.0 mb
37	Attachment 26	1 page	134 kb
38	Attachment 27	6 pages	0.8 mb
39	Attachment 28	2 pages	209 kb
40	Attachment 29	27 pages	3.8 mb
41	Redacted Docket Sheet	5 pages	1.0 mb

Note: You must view each document individually because the combined PDF would be over the 40 MB size limit.

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	)	No. 1:13EC297
IN THE MATTER OF THE SEARCH AND SEIZURE OF INFORMATION ASSOCIATED WITH [**REDACTED**] THAT IS STORED AT PREMISES CONTROLLED BY LAVABIT LLC	)	No. 1:13SW522
In re Grand Jury	)	No. 13-1

ORDER

WHEREAS, on January 7, 2016, the Court denied the Motion to Unseal Records and Vacate Non-Disclosure Orders respecting case numbers 1:13EC297, 1:13SW522, and No. 13-1 and ordered the United States to file on the public docket copies of all the previously filed pleadings, transcripts, and orders with redactions for only the identity of the subscriber and the subscriber's email address;

WHEREAS, on February 24, 2016, the United States moved to publicly file *ex parte* documents redacted of sensitive, nonpublic facts the disclosure of which could damage the ongoing investigation;

WHEREAS, on February 24, 2016, the United States moved to redact publicly filed documents of (a) information specific to the grand jury target that would disclose, in effect, the target's identity or would be protected from disclosure under Fed.R.Crim.P. 6(e), such as the

criminal statutes under investigation by the grand jury; and (b) information, such as the home address of Mr. Levison that should be redacted pursuant to Fed.R.Crim.P. 49.1 and EDVA Local Rule 49;

The court hereby finds that the government has a compelling interest in keeping under seal certain facts, the disclosure of which could damage the ongoing investigation or is protected by Fed.R.Crim.P. 6(e) and 49.1; the government's interest in keeping the redacted material sealed outweighs any public interest in disclosure; and having considered alternatives to the proposed redactions none will adequately protect those interests; it is hereby

ORDERED that the above-captioned cases are unsealed to allow the Clerk's office to file on the public docket and make electronically available through the CM/ECF system the following pleadings, transcripts, and orders as redacted in accordance with the Attachments to this Order:

I. **Case Number 1:13EC297**

1. Redacted Docket Sheet 1:13EC297
2. Redacted Motion for Order to Show Cause as to In Re: Pen Register (Dkt. #1)
3. Redacted ORDER Granting Motion for Order to Show Cause (Dkt. #2)
4. Redacted Summons Issued in case as to In Re: Pen Register (Dkt.. #3)
5. Redacted Supplement re Motion for Order to Show Cause (Dkt. #4)
6. Redacted Minute Entry for proceedings (Dkt. #5)
7. Redacted Order Denying Motion to Unseal (Dkt. #6)
8. Redacted Motion to Seal the grand jury subpoena (Dkt. #7)
9. Redacted Order Granting Motion to Seal the grand jury subpoena (Dkt. #8)
10. Redacted Minute Entry for Proceedings (Dkt. #9)
11. Redacted Sealed Transcript of Proceedings (Dkt. #10)
12. Redacted Under Seal Ex Parte Motion (Dkt. #11)
13. Redacted Sealed Order re UNDER SEAL EX PARTE MOTION (Dkt. #12)
14. Redacted version of Sealed Order (Dkt. #13)
15. Redacted Motion to Unseal Case (Dkt. #14)
16. Redacted Order to Respond to Motion to Unseal Case (Dkt. #15)

17. Redacted Response by US to In Re: Pen Register (Dkt. #16)
18. Redacted Protective Order as to In Re: Pen Register (Dkt. #17)

II. **Case Number 1:13SW522**

1. Redacted Docket Sheet 1:13SW522
2. Redacted Search Warrant Application and Affidavit (Dkt. #1)
3. Redacted Search Warrant Issued (Dkt. #2)
4. Redacted Motion to Seal Search Warrant (Dkt. #3)
5. Redacted Order to Seal (Dkt. #4)
6. Redacted Application for Non-Disclosure (Dkt. #5)
7. Redacted Nondisclosure Order (Dkt. #6)
8. Redacted Waiver of Personal Appearance (Dkt. #7)
9. Redacted Motion to Unseal Court Records (Dkt. #8)
10. Redacted Motion to Quash Subpoena (Dkt. #9)
11. Redacted Order denying Motion to Unseal and Motion to Quash (Dkt. #10)
12. Redacted Minute Entry (Dkt. #11)
13. Redacted Motion for Sanctions (Dkt. #12)
14. Redacted Order Granting Motion for Sanctions (Dkt. #13)
15. Redacted Notice of Appeal (Dkt. #14)
16. Redacted Transmission of Notice of Appeal (Dkt. #15)
17. Redacted Transcript of Proceedings (Dkt. #16)
18. Redacted USCA Case Number 13-4626 (Dkt. #17)
19. Redacted Order of USCA Consolidating Case No. 13-4625 and 4626 (Dkt. #18)
20. Redacted Under Seal Ex Parte Motion (Dkt. #19)
21. Redacted Sealed Order re Under Seal Ex Parte Motion (Dkt. #20)
22. Redacted version of Sealed Order (Dkt. #21)
23. Redacted Published Opinion of USCA (Dkt. #22)
24. Redacted Judgment of USCA (Dkt. #23)
25. Redacted USCA Mandate re Notice of Appeal (Dkt. #24)
26. Redacted Motion to Unseal Case (Dkt. #25)
27. Redacted Order to Respond to Motion to Unseal Case (Dkt. #26)
28. Redacted Response by US (Dkt. #27)
29. Redacted Protective Order (Dkt. #28)
30. Redacted Response of the United States in Opposition to Motion to Quash Subpoena and Unseal Court Records (Filed July 31, 2013) (Dkt. #TBD)

It is further ORDERED that the originally filed, unredacted pleadings, transcripts, and orders in matters 1:13EC297, 1:13SW522, and No. 13-1 remain under seal, and that no part of

them may be disclosed without Court order except to the extent provided above and in the Court's January 7, 2016 Order.

It is so ORDERED.

ENTERED this 24th day of February 2016, at Alexandria, Virginia.

Claude M. Hilton
Senior United States District Judge

AO 106 (Rev. 06/09) Application for a Search Warrant

UNDER SEAL

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

FILED
JUL 16 2013
CLERK, U.S. DISTRICT COURT
ALEXANDRIA

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 [redacted]
THAT IS STORED AT PREMISES CONTROLLED BY LAVABIT, LLC

Case No. 1:13SW522

REDACTED

APPLICATION FOR A SEARCH WARRANT

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

located in the Northern District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B

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

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

The search is related to a violation of:

Code Section	*Offense Description*
[redacted]	[redacted]

The application is based on th[redacted]
See Attached Affidavit

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

Reviewed by AUSA/SAUSA:

AUSA Michael Ben'Ary

Applicant's signature

Matthew Braverman, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: July 16, 2013

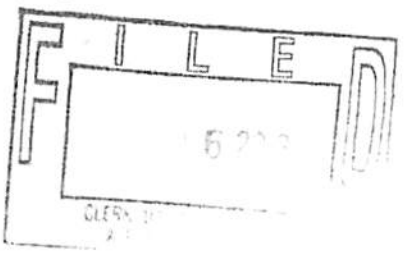
Judge's signature

City and state: Alexandria, Virginia

The Honorable Claude M. Hilton, U.S. District Judge

Printed name and title

UNDER SEAL



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

IN THE MATTER OF THE SEARCH AND SEIZURE OF INFORMATION ASSOCIATED WITH [redacted] THAT IS STORED AT PREMISES CONTROLLED BY Lavabit, LLC	Case No. 1:13SW522 **Filed Under Seal**

REDACTED

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Matthew Braverman , being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for electronically stored information associated with a certain accounts that is stored at premises controlled by Lavabit, LLC, an e-mail provider headquartered at [redacted] Dallas, Texas, 75204. The information to be seized is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Lavabit, LLC to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since 2007. From 2007 until present, I have been assigned to investigate a variety of complex cyber-intrusion investigations. As such, I am familiar with email, email service providers generally, and the use of various techniques to encrypt electronic data.

REDACTED

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ [redacted] have been committed by [redacted] There is also probable cause to search for the information described in Attachment A, and to seize evidence, instrumentalities, contraband or fruits of these crimes, as further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. See 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. [redacted]

7. [redacted]

8. [redacted]

REDACTED

9. [redacted]

10. [redacted]

11. [redacted]

12. [redacted]

13. [redacted]

REDACTED

14. [redacted]

15. [redacted]

16. [redacted]

17. [redacted]

REDACTED

[redacted]

18. [redacted]

[redacted]

19. [redacted]

[redacted]

20. [redacted]

[redacted]

21. [redacted]

[redacted]

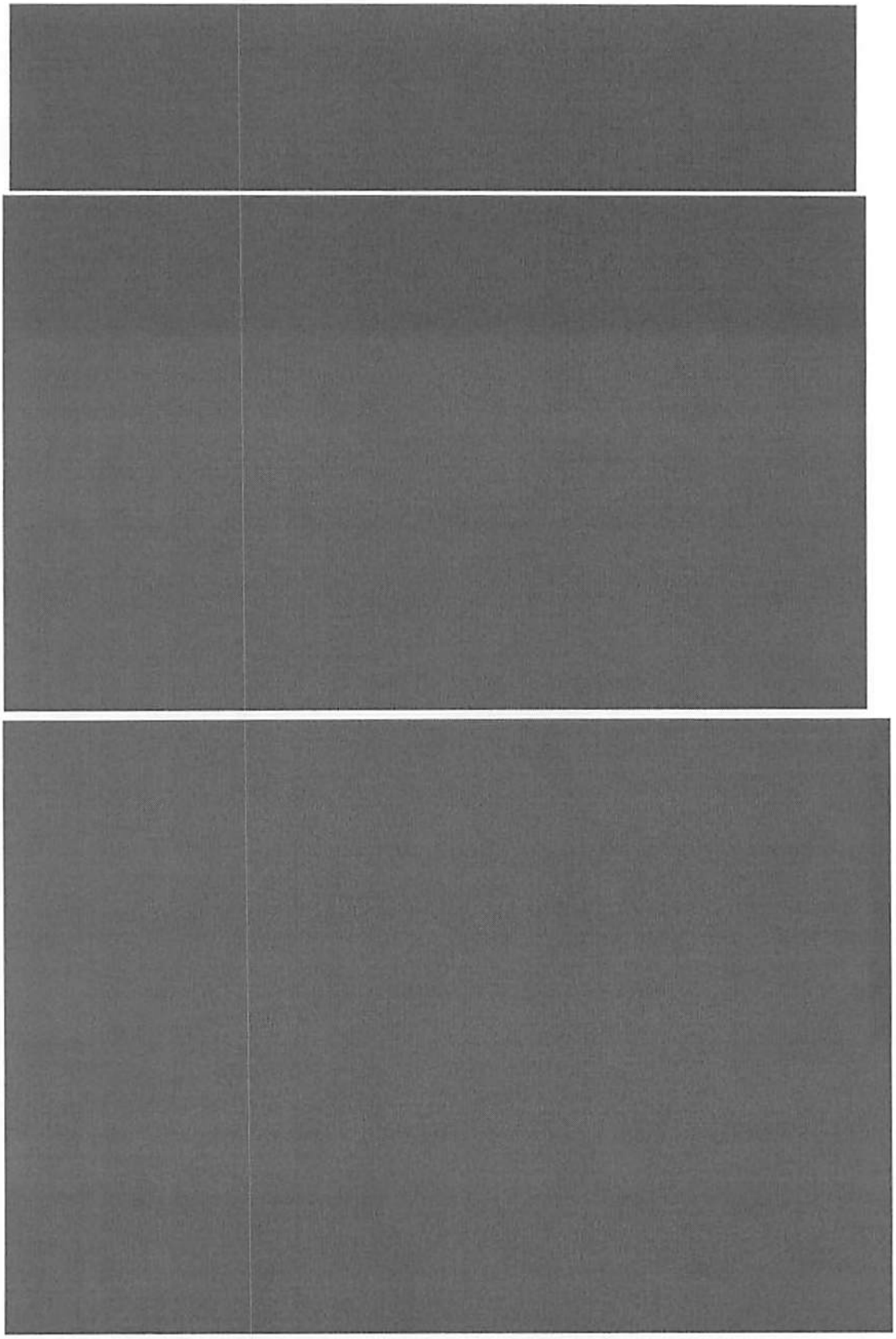
22. [redacted]

[redacted]

VI:

[redacted]

REDACTED



REDACTED

[redacted]

23. 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 [redacted] which is an e-mail account controlled by Lavabit, LLC ("Lavabit").

24. At approximately 4:15 p.m., two FBI Special Agents served that Order on Mr. Ladar Levison, the proprietor of Lavabit, at his home in Texas. The Special Agents identified themselves and advised Mr. Levison of this Court's order. A Special Agent advised Mr. Levison that the court order would request continual transactional records, to include connecting, sending, and receiving IP-Addresses. Mr. Levison advised that the account was a premium account and that in fact the user utilized the encryption. Mr. Levison stated most premium account owners don't utilize the encryption, however, this user was "pretty smart" and did utilize the encryption option. Mr. Levison stated that since the user uses encryption, Mr. Levison would not be able to get the requested information.

25. The Special Agent told Mr. Levison that an FBI Computer Scientist advised that if the FBI obtained got the SSL keys from his server, the FBI then could capture the user's connections, and password in the clear. Mr. Levison agreed that was true. Mr. Levison stated that to pull out the information he would have to log into the user's account himself and extract the requested data. Mr. Levison stated that in effect the FBI would be requesting him to "defeat his own system." Mr. Levison stated he was uncomfortable with this.

REDACTED

26. On July 10, 2013, the United States Attorney's Office arranged a conference call between the United States Attorney's Office, the Department of Justice, the FBI, Mr. Levison, and Mr. Levison's attorney (who has since informed the United States that she no longer represents Mr. Levison). During this conference call, the parties discussed the implementation of the PR/TT device in light of the encryption in place on the target email account. FBI explained, and Mr. Levison appeared to agree, that the "facilities, information and technical assistance" needed to install the PR/TT consisted of (1) access to Lavabit's server to install the PR/TT device, and; (2) encryption keys.

27. On July 13, 2013, Mr. Levison sent an email to AUSA Peterson 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.

28. Based on the above-cited message, it is clear that Mr. Levison is capable of providing the means for the FBI to install the PR/TT, as ordered by this Court, including encryption and SSL keys necessary for the FBI to collect the data in unencrypted form.

REDACTED

29. SSL stands for Secure Socket Layer. It is a protocol used in Internet communications that permits the sender and receiver of communications to encrypt them. Like most encryption methods, SSL relies on the use of keys—essentially, very long numbers that are used in a mathematical algorithm to encrypt or decrypt data.

30. Lavabit's website, at http://lavabit.com/philosophy.html, includes the following question and answer: "Do you support encryption? // Yes, we support encryption and encourage our users to enable encryption in their e-mail client. We support POP3 over SSL on port 995 and SMTP over SSL on port 465. We also support using the STARTTLS command. Our SSL certificate has been granted by the Comodo Group."

31. Lavabit's privacy policy, at http://lavabit.com/privacy_policy.html, states: "For premium users who have elected to use our 'secure' service, incoming e-mail is stored using an asymmetric encryption process that guarantees that it can't be accessed by anyone except the holder of the account password. For these accounts, only the encrypted version of the message is ever saved to disk."

32. The privacy policy also states: "It is also important to know what information Lavabit does NOT store. We do not keep a record of the IP addresses used to access our services (except in the web server logs), and we do not keep a record of what information was accessed during a particular session."

BACKGROUND CONCERNING E-MAIL

33. In my training and experience, I have learned that Lavabit, LLC provides a variety of on-line services, including electronic mail ("e-mail") access, to the public. Lavabit LLC allows subscribers to obtain e-mail accounts at the domain name lavabit.com, like the e-mail account[s] listed in Attachment A. Subscribers obtain an account by registering with

REDACTED

Lavabit, LLC. During the registration process, Lavabit, LLC asks subscribers to provide basic personal information. Therefore, the computers of Lavabit, LLC are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Lavabit, LLC subscribers) and information concerning subscribers and their use of Lavabit, LLC services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

34. In my training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

35. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins

REDACTED

to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

36. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

CONCLUSION

37. Based on the forgoing, I request that the Court issue the proposed search warrant. Because of the urgency of this matter, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Matthew Braverman
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on July 16, 2013

Honorable Claude M. Hilton
UNITED STATES JUDGE

AO 93 (Rev. 12/09) Search and Seizure Warrant

UNDER SEAL

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

REDACTED

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 [redacted]
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

REDACTED

ATTACHMENT A

Property to Be Searched

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

REDACTED

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 [redacted], including encryption keys and SSL keys;

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

REDACTED

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. §§ [redacted] those violations involving [redacted] 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 [redacted] including encryption keys and SSL keys;

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

REDACTED

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.

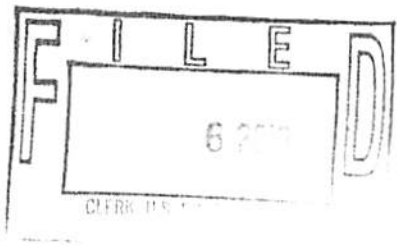
_____ _____

Date Signature

UNDER SEAL

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF VIRGINIA



Alexandria Division

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH [redacted] THAT IS STORED AT PREMISES CONTROLLED BY LAVABIT, LLC	)	UNDER SEAL (Local Rule 49(B)) No. 1:13sw522

REDACTED

GOVERNMENT'S MOTION TO SEAL SEARCH WARRANT
PURSUANT TO LOCAL RULE 49(B)

Upon the return of its executed search warrant,[1] the United States, by and through undersigned counsel, pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, now asks for an Order to Seal the **application in support of a search warrant, the search warrant** and the **affidavit in support of the search warrant**, together with this Motion to Seal and proposed Order, until the United States makes a motion to unseal the application, search warrant and affidavit.

I. REASONS FOR SEALING (See Local Rule 49(B)(1))

1. At the present time, Agents with the Federal Bureau of Investigation are conducting an investigation into [redacted] in violation of Title 18, United States Code, Sections [redacted]

[1] Pursuant to Local Rule 49(B), "[n]o separate motion to seal is necessary to seal a search warrant *from the time of issuance to the time the executed warrant is returned.*" (Emphasis added.) This is because, as Rule 49(B) additionally mandates, "[u]ntil an executed search warrant is returned, search warrants and related papers are not filed with the Clerk."

REDACTED

2. Premature disclosure of the specific details of this ongoing investigation (as reflected in the affidavit in support of search warrant) and this warrant could jeopardize this continuing criminal investigation, including the ability of the United States to locate and arrest additional persons, and may lead to the destruction of additional evidence in other locations. Thus, a sealing order is necessary to avoid hindering the ongoing investigation in this matter.

3. The United States has considered alternatives less drastic than sealing, including, for example, the possibility of redactions, and has determined that none would suffice to protect this investigation.

II. THE GOVERNING LAW (See Local Rule 49(B)(2))

4. It is generally recognized that the public has a common law right of access, but not a First Amendment right of access, to judicial documents, including documents associated with *ex parte* proceedings such as search warrant affidavits. Media General Operations, Inc. v. Buchanan, 417 F.3d 424, 429 (4th Cir. 2005); In re Washington Post Company v. Hughes, 923 F.2d 324, 326 (4th Cir. 1991). "But the right of access is qualified, and a judicial officer may deny access to search warrant documents if sealing is 'essential to preserve higher values' and 'narrowly tailored to serve that interest.'" Media General Operations, 417 F.3d at 429 (citations omitted); see also 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"). Sealing search warrants and their accompanying affidavits and application is within the discretionary powers of a judicial officer where, among other things, an "'affidavit contain[s] sensitive details of an ongoing investigation' and it is 'clear and apparent from the affidavits that any disclosure of the information there would

REDACTED

hamper' th[e] ongoing investigation." Media General Operations 417 F.3d at 430 (citations omitted); see also In re Search Warrant for Matter of Eye Care Physicians of America, 100 F.3d 514, 518 (7th Cir. 1996).

5. Before a district court generally may seal judicial records or documents, it must (a) provide public notice of the request to seal and allow interested parties a reasonable opportunity to object, (b) consider less drastic alternatives to sealing the documents, and (c) provide specific reasons and factual findings supporting its decision to seal the documents and for rejecting the alternatives. Ashcraft v. Conoco. Inc., 218 F.3d 288, 302 (4th Cir. 2000).

6. However, regarding the notice requirement in the specific context of a search warrant, the Fourth Circuit has cautioned that "the opportunity to object" cannot "arise prior to the entry of a sealing order when a search warrant has not been executed." Media General Operations, 417 F.3d at 429. "A rule to the contrary would endanger the lives of officers and agents and allow the subjects of the investigation to destroy or remove evidence before the execution of the search warrant." Id.; see also Franks v. Delaware, 438 U.S. 154, 169 (1978). Accordingly, in the context of search warrants, "the notice requirement is fulfilled by docketing 'the order sealing the documents,' which gives interested parties the opportunity to object after the execution of the search warrants." Media General Operations, 417 F.3d at 430 (quoting Baltimore Sun Co. v. Goetz, 886 F.2d 60, 65 (4th Cir. 1989)); see also Local Rule 49(B) ("Until an executed search warrant is returned, search warrants and related papers are not filed with the Clerk.").

7. As to the requirement of a court's consideration of alternatives, the Fourth Circuit counsels that, "[i]f a judicial officer determines that full public access is not appropriate, she

REDACTED

'must consider alternatives to sealing the documents,' which may include giving the public access to some of the documents or releasing a redacted version of the documents that are the subject to the government's motion to seal." Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 66).

8. Finally, regarding the requirement of specific findings, the Fourth Circuit's precedents state that, "'in entering a sealing order, a 'judicial officer may explicitly adopt the facts that the government presents to justify sealing when the evidence appears creditable,'" Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 65), so long as the ultimate "decision to seal the papers " is "made by the judicial officer," Goetz, 886 F.2d at 65. "Moreover, if appropriate, the government's submission and the [judicial] officer's reason for sealing the documents can be filed under seal." Goetz, 886 F.2d at 65; see also In re Washington Post Co., 807 F.2d 383, 391 (4th Cir. 1986) ("if the court concludes that a denial of public access is warranted, the court may file its statement of the reasons for its decision under seal").

III. PERIOD OF TIME GOVERNMENT SEEKS TO HAVE MATTER REMAIN UNDER SEAL (See Local Rule 49(B)(3))

9. Pursuant to Local Rule 49(B)(3), the application, search warrant and the affidavit will remain sealed until the need to maintain the confidentiality of the search warrant application and the related investigation expires, after which time the United States will move to unseal the application, search warrant and affidavit.

REDACTED

WHEREFORE, the United States respectfully requests that the application for search warrant, the search warrant, and affidavit in support of the search warrant, together with this Motion to Seal and proposed Order be sealed until further Order by the Court.

Respectfully submitted,

Neil H. MacBride
United States Attorney

By: _____
Michael Ben'Ary
Assistant United States Attorney

UNDER SEAL

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

FILED
6 2013
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

IN THE MATTER OF THE SEARCH OF	)	UNDER SEAL
	)	(Local Rule 49(B))
INFORMATION ASSOCIATED WITH [redacted]	)	No. 1:13sw522
	)	
THAT IS STORED AT PREMISES	)	
CONTROLLED BY LAVABIT, LLC	)	

REDACTED

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.

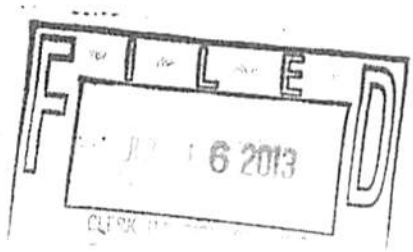
Claude M. Hilton
The Honorable Claude M. Hilton
United States District Judge

Date: July 16, 2013
Alexandria, Virginia

REDACTED

UNDER SEAL

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**

APPLICATION FOR ORDER COMMANDING LAVABIT NOT TO NOTIFY ANY PERSON OF THE EXISTENCE OF SEARCH WARRANT

The United States requests that the Court order Lavabit 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.

Lavabit is a provider of an electronic communication service, as defined in 18 U.S.C. § 2510(15), and/or a remote computer service, as defined in 18 U.S.C. § 2711(2). Pursuant to 18 U.S.C. § 2703, the United States obtained the attached search warrant, which requires Lavabit to disclose certain records and information to the United States. This Court has authority under 18 U.S.C. § 2705(b) to issue "an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order." *Id.*

In this case, such an order would be appropriate because the attached search warrant relates to an ongoing criminal investigation, and its disclosure may alert the targets to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the attached 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. *See* 18 U.S.C. § 2705(b)(2), (3), (5). Some of the evidence in this investigation is stored electronically. If alerted to the

REDACTED

investigation, the subjects under investigation could destroy that evidence, including information saved to their personal computers.

WHEREFORE, the United States respectfully requests that the Court grant the attached Order directing Lavabit not to disclose the existence or content of the attached search warrant, except that Lavabit may disclose the attached search warrant to an attorney for Lavabit for the purpose of receiving legal advice.

The United States further requests that the Court order that this application and any resulting order be sealed until further order of the Court. As explained above, these documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Executed on July 16, 2013.

Michael Ben'Ary
Assistant United States Attorney

REDACTED

UNDER SEAL

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

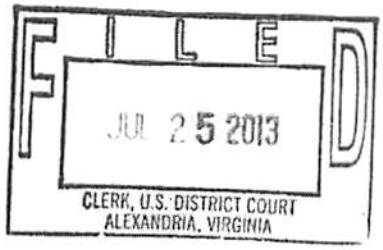
Claude M. Hilton
The Honorable Claude M. Hilton
United States District Judge

REDACTED

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 [redacted] THAT IS STORED AND CONTROLLED AT PREMISES CONTROLLED BY LAVABIT LLC	No. 1:13SW522
In re Grand Jury	No. 13-1

REQUEST FOR WAIVER OF PERSONAL APPEARANCE

Ladar Levinson requests to waive his personal appearance for the hearing to be held in this Court on Thursday, August 1, 2013. The Government does not object to this request for waiver of personal appearance.

LAVABIT LLC
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

REDACTED

Certificate of Service

I certify that on July 25, 2013, this Request for Waiver of Personal Appearance was hand delivered to the person at the addresses listed below:

James L. Trump
Senior Litigation Counsel
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314
jim.trump@usdoj.gov

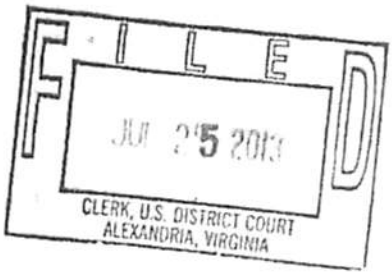
Jesse R. Binnall

REDACTED

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 [redacted] 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

REDACTED

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 [redacted], 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

REDACTED

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.

REDACTED

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 of [redacted]. However, Mr.

REDACTED

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

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 [redacted]. 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.

REDACTED

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.

REDACTED

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

REDACTED

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 [redacted] by [redacted] 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.

REDACTED

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

REDACTED

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:

James L. Trump
Senior Litigation Counsel
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314
jim.trump@usdoj.gov

Jesse R. Binnall

REDACTED

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 [redacted] THAT IS STORED AND CONTROLLED AT PREMISES CONTROLLED BY LAVABIT LLC	No. 1:13SW522
In re Grand Jury	No. 13-1

FILED
5 2013
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

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

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 [redacted] ("Lavabit Subpoena and Warrant").

ARGUMENT

If the Government gains access to Lavabit's Master Key, it will have unlimited access to not only [redacted] ("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.

REDACTED

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.

REDACTED

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.

REDACTED

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.

REDACTED

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

REDACTED

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

REDACTED

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

REDACTED

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:

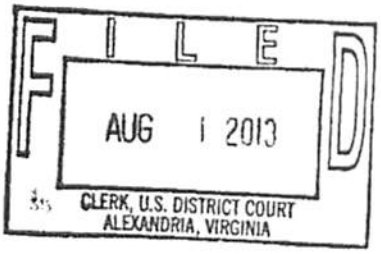
James L. Trump
Senior Litigation Counsel
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314
jim.trump@usdoj.gov

Jesse R. Binnall

REDACTED

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 [redacted] 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

REDACTED

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 1, 2013

Date: 8/1/13 Judge: Hilton Reporter: Westfall
Time: 10:00 – 10:20 Interpreter: _____
Language: _____

****UNDER SEAL HEARING****

Case Numbers: 1:13EC00297, 1:13SW522, GJ 13-1

REDACTED

Counsel for Government:	Respondent:
James Trump Brandon Van Grack Michael Ben'Ary Josh Goldfoot Ben Fitzpatrick	Jesse Binnall for Ladar Levison (Levison's appearance waived)

Appearances of Counsel for (✓) Government (✓) Respondent

Lavabit's Motion to Quash – Denied, Mr. Levison Ordered to turn over the encryption keys. Respondent's request for 5 days to do so – Denied, Respondant given 24 hours.

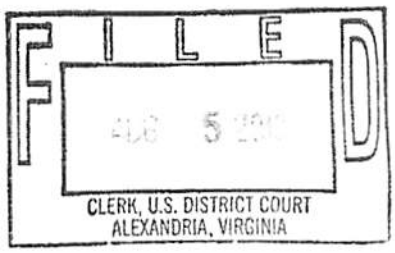
Lavabit's Motion to Unseal – Denied.

REDACTED

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 [redacted] THAT IS STORED AT PREMISES CONTROLLED BY LAVABIT LLC	)	No. 1:13SW522
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

REDACTED

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.

REDACTED

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.

REDACTED

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: _____

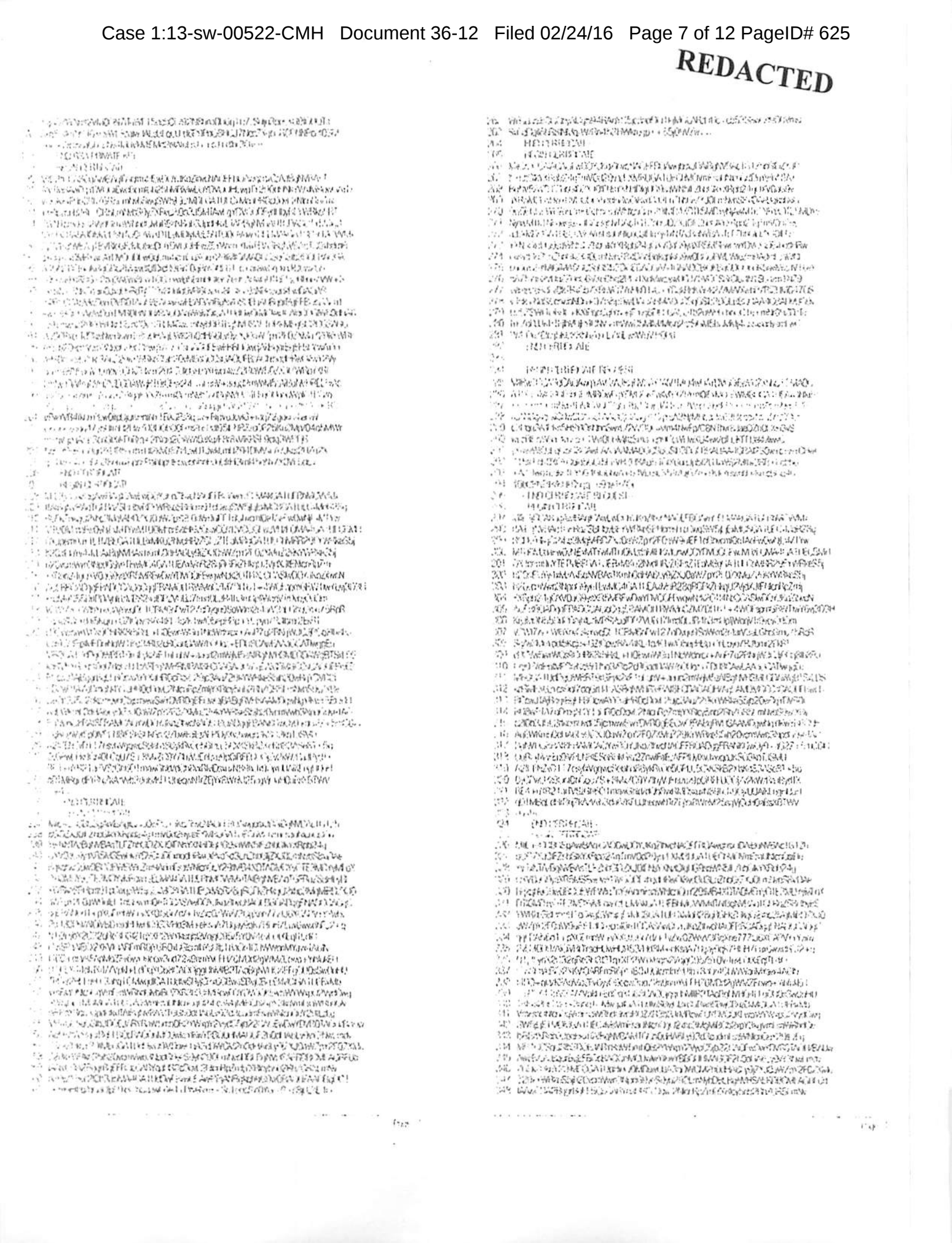
James L. Trump
United States Attorney's Office
Justin W. Williams U.S. Attorney's Building
2100 Jamieson Avenue
Alexandria, Virginia 22314
Phone: 703-299-3700

REDACTED

Attachment A

REDACTED

REDACTED



REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

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.

REDACTED

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

Alexandria Division

FILED
AUG 5 2013
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

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 [redacted] 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

REDACTED

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

REDACTED

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 IN THE MATTER OF THE SEARCH AND SEIZURE OF INFORMATION ASSOCIATED WITH [redacted] THAT IS STORED AND CONTROLLED AT PREMISES CONTROLLED BY LAVABIT LLC	**FILED UNDER SEAL** 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

REDACTED

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:

James L. Trump
Senior Litigation Counsel
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314
jim.trump@usdoj.gov

Jesse R. Binnall

REDACTED

APPEAL TRANSMITTAL SHEET (non-death penalty)

Transmittal to 4CCA of notice of appeal filed: 08/15/13

✓ First NOA in Case
___ Subsequent NOA-same party
___ Subsequent NOA-new party
___ Subsequent NOA-cross appeal
___ Paper ROA ___ Paper Supp.
Vols: _____
Other: _____

District: VAED

Division: EDVA

Caption: USA

v

In Re: Information Associated with Ed_Snowden@lavabit.com

District Case No.: 1:13sw522

4CCA No(s). for any prior NOA:

4CCA Case Manager:

Exceptional Circumstances: ___ Bail ___ Interlocutory ___ Recalcitrant Witness ___ Other _____

Confinement-Criminal Case:
___ Death row-use DP Transmittal
___ Recalcitrant witness
___ In custody
___ On bond
___ On probation

Defendant Address-Criminal Case:

District Judge: Claude M. Hilton

Court Reporter (list all): Tracy Westfall

Coordinator: Richard Banke

Fee Status:
___ No fee required (USA appeal) ___ Appeal fees paid in full ✓ Fee not paid

Criminal Cases:
___ District court granted & did not revoke CJA status (continues on appeal)
___ District court granted CJA & later revoked status (must pay fee or apply to 4CCA)
___ District court never granted CJA status (must pay fee or apply to 4CCA)

Civil, Habeas & 2255 Cases:
___ Court granted & did not revoke IFP status (continues on appeal)
___ Court granted IFP & later revoked status (must pay fee or apply to 4CCA)
___ Court never granted IFP status (must pay fee or apply to 4CCA)

PLRA Cases:
___ Proceeded PLRA in district court, no 3-strike determination (must apply to 4CCA)
___ Proceeded PLRA in district court, determined to be 3-striker (must apply to 4CCA)

Sealed Status (check all that apply):
____ Portions of record under seal
✓ Entire record under seal
____ Party names under seal
____ Docket under seal

Record Status for Pro Se Appeals (check any applicable):
___ Assembled electronic record transmitted
___ Additional sealed record emailed to 4cca-filing
___ Paper record or supplement shipped to 4CCA
___ No in-court hearings held
___ In-court hearings held – all transcript on file
___ In-court hearings held – all transcript not on file
___ Other:

Record Status for Counseled Appeals (check any applicable):
✓ Assembled electronic record available if requested
___ Additional sealed record available if requested
___ Paper record or supplement available if requested
___ No in-court hearings held
___ In-court hearings held – all transcript on file
✓ In-court hearings held – all transcript not on file
___ Other:

Deputy Clerk: Kathy Roberts Phone: 703-2992102 Date: 08/16/13

01/2012

REDACTED

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 [redacted] 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.

COPY

TRANSCRIPT OF HEARING

BEFORE THE HONORABLE CLAUDE M. HILTON

UNITED STATES DISTRICT JUDGE

APPEARANCES:

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.

P R O C E E D I N G S

THE CLERK: *In re:* Case Nos. 1:13 EC 297, 1:13 SW 522, and Grand Jury No. 13-1.

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

THE COURT: Good morning.

MR. BINNALL: Good morning, Your Honor. Jesse Binnall on behalf of Lavabit and Mr. Levison.

THE COURT: All right.

MR. BINNALL: May it please the Court. We're before the Court today on two separate motions, a motion to quash the requirement of Lavabit to produce its encryption keys and the motion to unseal and lift the nondisclosure requirements of Mr. Levison.

Your Honor, the motion to quash in this arises because the privacy of users is at -- of Lavabit's users are at stake. We're not simply speaking of the target of this investigation. We're talking about over 400,000 individuals and entities that are users of Lavabit who use this service because they believe their communications are secure.

By handing over the keys, the encryption keys in this case, they necessarily become less secure. In this case it is true that the face of the warrant itself does limit the documents or -- and communications to be viewed and the specific metadata to be viewed to the target of the case, [redacted]

However, there is a lack of any sort of check or balance in order to ensure that the -- that the encrypted data of other Lavabit users remain secure. The encryption in this case doesn't protect only content. It protects login data and the other -- some of the other metadata involved in this case.

We believe that this is not the least restrictive means in order to provide the government the data that they are looking for. Specifically --

THE COURT: You have two different encryption codes, one for the logins and the messages that are transmitted. You have another code that encrypts the content of the messages, right?

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

From my understanding of the way that this works is that there is one SSL key. That SSL key is what is issue in this case, and that SSL key specifically protects the communication, the over -- the breadth of the communication itself from the user's actual computer to the server to make sure that the user is communicating with exactly who the user intends to be communicating with, the server.

And that's one of the things that SSL does. It ensures that you're talking to the right person via e-mail and there's not a so-called man in the middle who's there to take that message away.

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

message and interpret the message as well?

MR. BINNALL: My understanding is that it does, Your Honor, but because that's not my technical expertise, I'm not going to represent to the Court anything on that one way or another. But my understanding is there is one general key here that is at issue.

THE COURT: Well, why would you set up such? I mean, a telephone, you've got telephone numbers and --

MR. BINNALL: Correct.

THE COURT: -- those can be traced very easily without any look at the content of the message that's there. You-all could have set up something the same way.

MR. BINNALL: We could have, Your Honor. Actually, if you're to --

THE COURT: So if anybody's -- you're blaming the government for something that's overbroad, but it seems to me that your client is the one that set up the system that's designed not to protect that information, because you know that there needs to be access to calls that go back and forth to one person or another. And to say you can't do that just because you've set up a system that everybody has to -- has to be unencrypted, if there's such a word, that doesn't seem to me to be a very persuasive argument.

MR. BINNALL: I understand the Court's point, and this is the way that I understand why it's done that way.

There's different security aspects involved for people who want to protect their privacy, and there certainly is the actual content of the message themselves. That's certainly what I would concede is the highest security interest.

But there's also the security interest to make sure that they're communicating with who you want to be communicating with. That is equally of a concern for privacy issues because that is, at the end of the day, one of the things that secures the content of the message.

In this case it is true that most Internet service providers do log, is what they call it, a lot of the metadata that the government wants in this case without that necessarily being encrypted, things such as who something is going to, who it's going from, the time it's being sent, the IP address from which it is being sent.

Lavabit code is not something that you buy off the shelf. It is code that was custom made. It was custom made in order to secure privacy to the largest extent possible and to be the most secure way possible for multiple people to communicate, and so it has chosen specifically not to log that information.

Now, that is actually information that my client has offered to start logging with the particular user in this case. It is, however, something that is quite burdensome on him. It is something that would be custom code that would take between 20 to 40 hours for him to be able to produce. We believe that

is a better alternative than turning over the encryption key which can be used to get the data for all Lavabit users.

I hope that addresses the Court's concern kind of with regard to the metadata and why it is not more -- why Lavabit hasn't created an encryption system that may honestly be more within the mainstream, but this is a provider that specifically was started in order to have to protect privacy interests more than the average Internet service provider.

THE COURT: I can understand why the system was set up, but I think the government is -- government's clearly entitled to the information that they're seeking, and just because you-all have set up a system that makes that difficult, that doesn't in any way lessen the government's right to receive that information just as they would from any telephone company or any other e-mail source that could provide it easily. Whether it's -- in other words, the difficulty or the ease in obtaining the information doesn't have anything to do with whether or not the government's lawfully entitled to the information.

MR. BINNALL: It is -- and we don't disagree that the government is entitled to the information. We actually --

THE COURT: Well, how are we going to get it? I'm going to have to deny your motion to quash. It's just not overbroad. The government's asking for a very narrow, specific bit of information, and it's information that they're entitled to.

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

MR. BINNALL: Your Honor, what I would still say is the best method for them to get it is, first of all, there be some way for there to be some sort of accountability other than just relying on the government to say we're not going to go outside the scope of the warrant.

This is nothing that is, of course, personal against the government and the, you know, very professional law enforcement officers involved in this case. But quite simply, the way the Constitution is set up, it's set up in a way to ensure that there's some sort of checks and balances and accountability.

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

MR. BINNALL: Well --

THE COURT: Suggest something to me.

MR. BINNALL: I think that the least restrictive means possible here is that the government essentially pay the reasonable expenses, meaning in this case my client's extensive labor costs to be capped at a reasonable amount.

THE COURT: Has the government ever done that in one of these pen register cases?

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

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

MR. BINNALL: And Your Honor's certainly seen more of these than I have.

THE COURT: So would it be reasonable to start now with your client?

MR. BINNALL: I think everyone would agree that this is an unusual case. And that this case, in order to protect the privacy of 400,000-plus other users, some sort of relatively small manner in which to create a log system for this one user to give the government the metadata that they're looking for is the least restrictive mean here, and we can do that in a way that doesn't compromise the security keys.

This is actually a way that my client --

THE COURT: You want to do it in a way that the government has to trust you --

MR. BINNALL: Yes, Your Honor.

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

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

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

MR. BINNALL: Your Honor, because that's what the basis of Fourth Amendment law says is more acceptable, is that the government is the entity that you really need the checks and balances on.

Now, my --

THE COURT: I don't know that the Fourth Amendment says that. This is a criminal investigation.

MR. BINNALL: That is absolutely correct.

THE COURT: A criminal investigation, and I don't know that the Fourth Amendment says that the person being investigated here is entitled to more leeway and more rights than the government is. I don't know.

MR. BINNALL: There certainly is a balance of power there. I, of course, am not here to represent the interest of [redacted] I'm here specifically looking over my client who has sensitive data --

THE COURT: I understand. I'm trying to think of working out something. I'm not sure you're suggesting anything to me other than either you do it and the government has to trust you to give them whatever you want to give them or you have to trust the government that they're not going to go into your other files.

Is there some other route?

MR. BINNALL: I would suggest that the government -- I'm sorry -- that the Court can craft an order to say that we can -- that we should work in concert with each other in order to come up with this coding system that gives the government all of the metadata that we can give them through this logging procedure that we can install in the code, and then using that as a least restrictive means to see if that can get the government the information that they're looking for on the specific account.

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

MR. BINNALL: I mean, 20, 40 hours. So I would suggest that would probably be a week to a week and a half, Your Honor, although I would be willing to talk to my client to see if we can get that expedited.

THE COURT: To install it?

MR. BINNALL: Well, to write the code.

THE COURT: You don't have a code right at the moment. You would have to write something?

MR. BINNALL: That's correct. And the portion of the government's brief that talks about the money that he was looking for is that reasonable expense for him basically to do nothing for that period of time but write code to install in order to take the data from [redacted] and put it in a way that the government will see the logged metadata involved.

THE COURT: All right. I think I understand your position. I don't think you need to argue this motion to unseal. This is a grand jury matter and part of an ongoing criminal investigation, and any motion to unseal will be denied.

MR. BINNALL: If I could have the Court's attention just on one issue of the nondisclosure provision of this. And I understand the Court's position on this, but there is other privileged communications if the Court would be so generous as to allow me very briefly to address that issue?

There's other First Amendment considerations at issue with not necessarily just the sealing of this, but what

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

The First Amendment, of course, doesn't just cover speech and assembly, but the right to petition for a redress of grievances. We're talking about a statute here, and, honestly, a statute that is very much in the public eye and involving issues that are currently pending before Congress.

I think the way that the order currently is written, besides being --

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

MR. BINNALL: I'm talking about the sealing order and the order that prohibits Mr. Levison from disclosing any information.

Now, we don't want to disclose -- we have no intention of disclosing the target, but we would like to be able to, for instance, talk to members of the legislature and their staffs about rewriting this in a way that's --

THE COURT: No. This is an ongoing criminal investigation, and there's no leeway to disclose any information about it.

MR. BINNALL: And so at that point it will remain with only Mr. Levison and his lawyers, and we'll keep it at that.

THE COURT: Let me hear from Mr. Trump.

Is there some way we can work this out or something that I can do with an order that will help this or what?

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

you've already articulated the reason why is that anything done by Mr. Levison in terms of writing code or whatever, we have to trust Mr. Levison that we have gotten the information that we were entitled to get since June 28th. He's had every opportunity to propose solutions to come up with ways to address his concerns and he simply hasn't.

We can assure the Court that the way that this would operate, while the metadata stream would be captured by a device, the device does not download, does not store, no one looks at it. It filters everything, and at the back end of the filter, we get what we're required to get under the order.

So there's no agents looking through the 400,000 other bits of information, customers, whatever. No one looks at that, no one stores it, no one has access to it. All we're going to look at and all we're going to keep is what is called for under the pen register order, and that's all we're asking this Court to do.

THE COURT: All right. Well, I think that's reasonable. So what is this before me for this morning other than this motion to quash and unseal which I've ruled on?

MR. TRUMP: The only thing is to order the production of the encryption keys, which just --

THE COURT: Hasn't that already been done? There's a subpoena for that.

MR. TRUMP: There's a search warrant for it, the motion

to quash.

THE COURT: Search warrant.

MR. TRUMP: Excuse me?

THE COURT: I said subpoena, but I meant search warrant.

MR. TRUMP: We issued both, Your Honor, but Your Honor authorized the seizure of that information. And we would ask the Court to enforce that by directing Mr. Levison to turn over the encryption keys.

If counsel represents that that will occur, we can not waste any more of the Court's time. If he represents that Mr. Levison will not turn over the encryption keys, then we have to discuss what remedial action this Court can take to require compliance with that order.

THE COURT: Well, I will order the production of those -- of those keys.

Is that simply Mr. Levison or is that the corporation as well?

MR. TRUMP: That's one and the same, Your Honor.

Just so the record is clear. We understand from Mr. Levison that the encryption keys were purchased commercially. They're not somehow custom crafted by Mr. Levison. He buys them from a vendor and then they're installed.

THE COURT: Well, I will order that. If you will

present an order to me, I'll enter it later on.

MR. TRUMP: Thank you.

MR. BINNALL: Thank you, Your Honor.

As far as time frame goes, my client did ask me if the Court did order this if the Court could give him approximately five days in order to actually physically get the encryption keys here. And so it will be -- or just some sort of reasonable time frame to get the encryption keys here and in the government's hands. He did ask me to ask exactly the manner that those are to be turned over.

MR. TRUMP: Your Honor, we understand that this can be done almost instantaneously, as soon as Mr. Levison makes contact with an agent in Dallas, and we would ask that he be given 24 hours or less to comply. This has been going on for a month.

THE COURT: Yeah, I don't think 24 -- 24 hours would be reasonable. Doesn't have to do it in the next few minutes, but I would think something like this, it's not anything he has to amass or get together. It's just a matter of sending something.

So I think 24 hours would be reasonable.

MR. BINNALL: Yes. Thank you, Your Honor.

THE COURT: All right. And you'll present me an order?

MR. TRUMP: We will, Your Honor. Thank you.

THE COURT: All right. Thank you-all, and we'll adjourn until -- or stand in recess till 3 o'clock. Well,

recess till 9 o'clock tomorrow morning.

* * *

(Proceedings concluded at 10:25 a.m.)

CERTIFICATION

I certify, this 19th day of August 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

Tracy Westfall, RPR, CMRS, CCR

FILED: August 29, 2013

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

REDACTED

No. 13-4625
(1:13-sw-00522-CMH-1)

In re: UNDER SEAL

UNITED STATES OF AMERICA

Plaintiff - Appellee

v.

UNDER SEAL

Party-in-Interest - Appellant

This case has been opened on appeal.

Originating Court	United States District Court for the Eastern District of Virginia at Alexandria
Originating Case Number	1:13-sw-00522-CMH-1
Date notice of appeal filed in originating court:	08/16/2013
Appellant (s)	Under Seal
Appellate Case Number	13-4625

Case Manager	RJ Warren 804-916-2702

REDACTED

FILED: August 29, 2013

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

REDACTED

No. 13-4625 (L)
(1:13-sw-00522-CMH-1)
(1:13-dm-00022-CMH-1)

In re: UNDER SEAL

UNITED STATES OF AMERICA

Plaintiff - Appellee

v.

UNDER SEAL

Party-in-Interest - Appellant

No. 13-4626
(1:13-dm-00022-CMH-1)
(1:13-sw-00522-CMH-1)

In re: GRAND JURY PROCEEDINGS

UNITED STATES OF AMERICA

Plaintiff - Appellee

v.

REDACTED

UNDER SEAL

Party-in-Interest - Appellant

ORDER

The court consolidates Case No. 13-4625 and Case No. 13-4626. Entry of appearance forms and disclosure statements filed by counsel and parties to the lead case are deemed filed in the secondary case.

For the Court--By Direction

/s/ Patricia S. Connor, Clerk

FILED
SEP 20 2013
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

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 [redacted] THAT IS STORED AND CONTROLLED AT PREMISES CONTROLLED BY LAVABIT LLC	NO. 1:13 SW 522
IN RE GRAND JURY SUBPOENA	NO. 13-1

REDACTED

EX PARTE AND UNDER SEAL

MOTION OF THE UNITED STATES TO UNSEAL CERTAIN DOCUMENTS RELATED TO LITIGATION WITH LAVABIT, LLC, AND SEALED STATEMENT OF REASONS THAT OTHER INFORMATION SHOULD REMAIN UNDER SEAL

The United States, by and through its undersigned attorneys, hereby requests that the Court partially unseal certain pleadings and orders that were filed in the above-captioned matters. The government originally requested the Court seal these documents because their public release would damage an ongoing criminal investigation. Since that time, Lavabit, LLC, and its proprietor, Ladar Levison, shut down its e-mail service. In addition, Mr. Levison made numerous public statements that his decision to shut down was in response to government attempts to obtain data related to a user or users of his service (a statement which, as discussed further below, Lavabit had previously represented it was prohibited from making due to the Court's sealing orders). The shutdown, and the attendant publicity generated by Mr. Levison

REDACTED

and his counsel's numerous media appearances, ended the government's ability to obtain evidence from any e-mail account hosted by Lavabit, LLC and alerted the target of the government's ongoing investigative actions. Thus, a substantial amount of the damage the government cited in its earlier sealing requests has been done. As such, the government hereby requests the Court partially unseal certain pleadings, as explained in more detail below.

BACKGROUND

The United States is conducting a criminal investigation of [redacted] for violations of numerous criminal statutes. On [redacted], a criminal complaint was filing charging [redacted] with violations of 18 U.S.C. [redacted] remains a fugitive. As part of the investigation, the United States discovered a number of e-mail accounts believed to be used by [redacted] that were hosted at the domain lavabit.com. That domain belongs to Lavabit, LLC, which, prior to August 8, 2013, offered e-mail services to the general public.

As part of the investigation into [redacted] the United States began to investigate the e-mail accounts believed to belong to him that were provided by Lavabit. On June 8, 2013, a grand jury subpoena was issued to Lavabit requesting billing and subscriber information for one Lavabit e-mail account [redacted]. Lavabit provided the information requested in the subpoena, via e-mail, on June 8. 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 the same Lavabit e-mail account. The Application and Order were sealed, and Mr. Levison was directed not to disclose the Order to any other person other than his attorney. Mr. Levison received the Order on June 11, 2013. He responded, by mail, on June 27,

REDACTED

2013. Mr. Levison provided very little of the information sought by the June 10, 2013 Order. For example, Mr. Levison provided no transactional records for the account.

On June 28, 2013, the United States obtained a pen register/trap and trace order for this Lavabit e-mail account (Dkt. No. 1:13 EC 297). The pen register application and Order were sealed. That same day, agents of the Federal Bureau of Investigation met with Mr. Levison to discuss the grand jury subpoena, the June 27, 2013 § 2703(d) Order, and pen register Order. Mr. Levison told the agents he would not comply with the pen register order and that he wanted to speak with an attorney. Later that same day, the United States obtained an Order from Magistrate Judge Theresa C. Buchanan directing Lavabit to comply with the pen register Order forthwith. Lavabit still did not comply with the pen register order.

On July 9, 2013, the United States requested that this Court enter an Order to Show Cause why Lavabit and Mr. Levison should not be held in contempt for failing to comply with the pen register order. A hearing on the United States motion was held on July 16, 2013.

On July 11, 2013, the United States issued a grand jury subpoena requiring Mr. Levison to appear before the grand jury on July 16, 2013. Mr. Levison was directed to bring copies of Lavabit's encryption keys, and any other information necessary to accomplish the installation and use of a pen register/trap and trace device pursuant to the June 28, 2013 pen register Order.

On July 16, 2013, prior to the hearing on the United States' request for an Order to Show Cause, this Court authorized a search warrant, issued pursuant to 18 U.S.C. § 2703, commanding Lavabit to produce any information necessary to decrypt communications sent to and from the Lavabit e-mail account listed in the pen register Order (Dkt. No. 1:13 SW 522). The search warrant, application, and affidavit in support were sealed, and Lavabit was ordered not to disclose the search warrant.

REDACTED

At the July 16, 2013, hearing, Mr. Levison appeared *pro se*. Mr. Levison agreed to allow the United States to install a pen register/trap and trace device on his system. He did not provide any decryption assistance, nor did he provide copies of Lavabit's encryption keys. The United States withdrew the grand jury subpoena and Mr. Levison did not appear before the grand jury. After the hearing, this Court placed the grand jury subpoena that Mr. Levison had received under seal.

On July 25, 2013, Lavabit and Mr. Levison, through counsel, moved to quash the withdrawn subpoena and search warrant 1:13 SW 522. He also moved to unseal four categories of documents, which Mr. Levison described as "records concerning the United States government's attempt to obtain certain encryption keys": (1) all orders and documents filed in this matter[1] before the Court's issuance of the July 16, 2013 Sealing Order; (2) all orders and documents filed in this matter after the issuance of the July 16, 2013 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 connection with such orders or requests for such orders. As a basis for unsealing, Mr. Levison argued that the sealing order "unjustly restrained [him] from contacting Lavabit subscribers who could be subjected to government surveillance. . . ." Mot. for Unsealing of Sealed Court Records and Removal of Non-Disclosure Order and Mem. of Law in Supp. of Mot. 1-2, 5 ("Lavabit Mot. to Unseal").

On August 1, 2013, this Court held a hearing on Lavabit's motions. The motions were denied by written Order. The Court also ordered Mr. Levison and Lavabit to provide Lavabit's

[1] Mr. Levison's pleading did not define the "matter" at issue. However, the document was filed with a caption that included docket numbers 1:13 EC 297, 1:13 SW 522, and Grand Jury No. 13-1.

REDACTED

encryption keys and any other information necessary to accomplish the use of the pen register/trap and trace device to the government no later than 5 p.m. on August 2, 2013.

Mr. Levison did not provide the keys in a usable format by the Court's deadline.[2] On August 5, 2013, the United States moved for sanctions against Mr. Levison and Lavabit. That same day, the Court ordered that if Lavabit and Mr. Levison did not comply with the Court's directive by noon on August 5, 2013, the Court would impose a fine of $5,000 each day until Lavabit complied.

On August 7, Mr. Levison provided a usable version of Lavabit's encryption keys to the United States. On August 8, 2013, Mr. Levison ceased operating Lavabit, LLC. He posted a message to the website "lavabit.com" which stated, in part: "I have been forced to make a difficult decision: to become complicit in crimes against the American people or walk away from nearly ten years of hard work by shutting down Lavabit. After significant soul searching, I have decided to suspend operations." Mr. Levison's statement on the website concluded with a request for donations.

Mr. Levison's decision to shut down Lavabit drew significant media attention, and Mr. Levison and his attorney subsequently gave numerous media interviews relating to his decision. A list of some of those interviews is attached to this pleading as Exhibit 24. Within a day of Mr. Levison's public announcement, The Guardian published a statement, purported to be from [redacted] lauding Lavabit's decision. [redacted]

[2] Mr. Levison had provided an illegible, printed version of the encryption keys, which was useless.

REDACTED

[redacted]

On August 15, 2013, Lavabit filed two notices of appeal. Both notices of appeal indicated that Lavabit and Mr. Levison would appeal the Court's August 1 and August 5 Orders. One notice of appeal was captioned with docket numbers 1:13 EC 297 and 1:13 SW 522. The other notice of appeal was captioned with Grand Jury No. 13-1. The Fourth Circuit has consolidated the appeals.

At present, the United States seeks to partially unseal the following documents:

Document	Case Number	Exhibit No.
18 U.S.C. § 2703(d) Order	1:13 EC 254	1
Pen Register Order	1:13 EC 297	2
Motion for Entry of an Order to Compel	1:13 EC 297	3
Order Compelling Compliance Forthwith	1:13 EC 297	4
Motion of the United States for an Order to Show Cause	1:13 EC 297	5
Order to Show Cause	1:13 EC 297	6
Summons	1:13 EC 297	7
Grand Jury Subpoena dated July 11, 2013	13-1; 13 GJ 2527; 13-2451	8
Search Warrant	1:13 SW 522	9
Order to Seal	1:13 SW 522	10
18 U.S.C. § 2705(b) Order	1:13 SW 522	11
USA Supplement to Motion for Order to Show Cause	1:13 EC 297	12
Hearing Transcript		13

REDACTED

Order Denying Motion to Unseal	1:13 EC 297	14
Motion to Quash Subpoena and Search Warrant and Memorandum of Law in Support of Motion	1:13 EC 297; 1:13 SW 522; No. 13-1	15
Motion for Unsealing of Sealed Court Records and Removal of Non-Disclosure Order and Memorandum of Law in Support of Motion	1:13 EC 297; 1:13 SW 522; No. 13-1	16
Response of the United States in Opposition to Lavabit's Motion to Quash Subpoena and Motion For Unsealing of Sealed Court Records	1:13 EC 297; 1:13 SW 522; No. 13-1	17
Hearing Transcript		18
Order Denying Motions	1:13 EC 297; 1:13 SW 522; No. 13-1	19
Motion for Sanctions	1:13 EC 297; 1:13 SW 522; No. 13-1	20
Order [Imposing Sanctions]	1:13 EC 297; 1:13 SW 522; No. 13-1	21
Notices of Appeal	1:13 EC 297; 1:13 SW 522; No. 13-1	22
Notice of Appeal (Amended)	1:13 SW 522	23

Redacted versions of each document are attached to this pleading as exhibits 1-23.

ARGUMENT

Lavabit no longer provides e-mail services to the target of the government's investigation. Moreover, Lavabit has notified the target of the government's investigation regarding the government's interest in the target's Lavabit accounts. Lavabit's failure to provide e-mail service means that the target's Lavabit e-mail accounts are no longer viable sources of information or evidence in the government's investigation. Lavabit's notification of the user

means that the damage from user notification, such as the destruction of electronic evidence by the target, has likely already occurred. Thus, some of the reasons for sealing certain sealed pleadings no longer apply. The United States therefore requests that certain documents be partially unsealed.

However, the criminal investigation into [redacted] remains ongoing, and Lavabit's violations of the sealing order have not entirely eliminated the reasons for sealing documents that are at issue in this matter. The justifications for sealing outlined in the government's original motion still apply to certain categories of information, and such information should remain sealed. The United States hereby reasserts (and incorporates by reference) those justifications as to the following categories of information:

1) Investigative Facts, Including Applications for Legal Process and Affidavits in Support of Those Applications. The above-captioned matters, which relate to a pen register, search warrant, and grand jury subpoena, include pleadings outlining the government's ongoing criminal investigation into [redacted] Though the target of the investigation has been charged with certain offenses, the government's investigation into his criminal conduct is ongoing. The government continues to investigate the scope of [redacted] unlawful activity, as well as whether he conspired with others. As such, the documents in this category, which contain recitations of the basis for obtaining the orders sought and their relevance to the investigation, contain "sensitive nonpublic facts," the disclosure of which could damage the ongoing investigation. This is sufficient justification for sealing. *See In re Application of the United States of America for an Order Pursuant to 18 U.S.C. Section 2703(d)*, 707 F.3d 283, 293-94 (4th Cir. 2013); *see also ACLU v. Holder*, 673 F.3d 245, 253 (4th

REDACTED

Cir. 2011) (noting government has compelling interest in protecting the integrity of ongoing investigations).

The United States has also redacted the specific accounts targeted by the government. Though these accounts, due to Mr. Levison's actions, are no longer operational, knowledge of the specific accounts known to the government could alert the target as to what information the government has, or does not have, about his activities. This could allow him to alter or destroy electronic evidence stored in other places. Such action would damage the investigation and thus this information should remain sealed. *See In re Application*, 707 F.3d at 293-94.

2) The Identities of Law Enforcement Personnel Involved in the Ongoing Investigation. The United States has redacted the identities of court and law enforcement personnel. Law enforcement personnel are redacted because, in other investigations [redacted] individuals who did not support the investigation attempted to harass individuals working on the case by publishing their home addresses, work telephone numbers, and work e-mail addresses, and encouraged others to directly contact them. Some individuals also researched court personnel and placed personal information about such personnel on the internet. As such, this information has been redacted to minimize disruption to the investigation and to the operation of the courts. This is a valid justification for sealing. *See, e.g., United States v. Ramey*, 791 F.2d 317, 318-20 (4th Cir. 1986) (noting that a case may be sealed for legitimate prosecutorial needs and that protection of witness identities is a valid justification for sealing an indictment).

3) Information Required to be Sealed by Law. Some information contained in the records should be sealed by operation of law. For instance, some of the facts contained in various applications is derived from the returns of grand jury subpoenas, which should be sealed

REDACTED

pursuant to Federal Rule of Criminal Procedure 6(e). Other documents contain the address of Mr. Levison's personal residence, which is where his business is headquartered. This is personal information which must be redacted pursuant to the E-Government Act of 2002. *See* E.D. Va. Local R. 49.

One document specifically bears mention in this category: the grand jury subpoena issued to Mr. Levison. This subpoena was issued to Mr. Levison but later withdrawn after the government obtained a search warrant for the same information. Mr. Levison never appeared before the grand jury, and the government's interest in the information sought by the subpoena will be revealed by the unsealing of the government's search warrant. Thus, the government does not believe that the grand jury subpoena needs to remain sealed at this time. To the extent the court believes the release of the subpoena would disclose a "matter before the grand jury," the government seeks permission from the Court to disclose the subpoena as part of the record, if necessary, in the Court of Appeals.

REDACTED

CONCLUSION

For the foregoing reasons, the United States requests that the Court sign the proposed order (Exhibit 25) partially unsealing the documents described in this motion, and authorize the release of the redacted versions attached to this pleading as Exhibits 1-23. A redacted version of the proposed order suitable for public release is attached as Exhibit 26.

Respectfully submitted,

Kathleen M. Kahoe
Acting United States Attorney

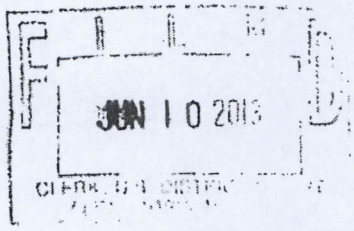
By: _____

Andrew Peterson
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
Alexandria, VA 22314
703-299-3700
Andy.peterson@usdoj.gov

REDACTED

EXHIBIT 1

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. § 2703(d)

MISC. NO. 1:13 EC 254

REDACTED

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

REDACTED

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.

/s/
John F. Anderson
United States Magistrate Judge

June 10, 2013
Date

A TRUE COPY, TESTE:
CLERK, U.S. DISTRICT COURT
BY [redacted]
DEPUTY CLERK

REDACTED

ATTACHMENT A

I. The Account(s)

The Order applies to certain records and information associated with the following email account(s): [redacted].

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).

REDACTED

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

REDACTED

EXHIBIT 2

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

REDACTED

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

ORDER

This matter having come before the Court pursuant to an Application under 18 U.S.C. § 3122, by [redacted], 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 [redacted] that is registered to subscriber [redacted] 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. §§ [redacted] by [redacted].

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

REDACTED

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

REDACTED

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: 9/20/13

REDACTED

EXHIBIT 3

FILED
SEP 20 2013
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

REDACTED

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

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 [redacted]. 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

REDACTED

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

REDACTED

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: [redacted]
Assistant United States Attorney

REDACTED

EXHIBIT 4

FILED
JUN 28 2013
CLERK, U.S. DISTRICT COURT
ALEXANDRIA

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

REDACTED

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

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 [redacted], 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;"

REDACTED

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

/s/
Theresa Carroll Buchanan
United States Magistrate Judge
Hon. Theresa C. Buchanan
United States Magistrate Judge

REDACTED

EXHIBIT 5

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

FILED
JUL - 9 2013
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

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

REDACTED

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 [redacted]

[redacted]

REDACTED

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.

REDACTED

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 [redacted] 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

REDACTED

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: [redacted]

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

REDACTED

PROPOSED
ORDER TO SHOW CAUSE

REDACTED

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

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

REDACTED

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

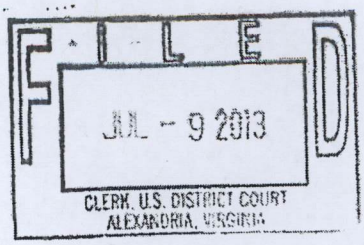
REDACTED

EXHIBIT 6

REDACTED

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

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

REDACTED

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

/s/
Claude M. Hilton
United States District Judge

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

BY [redacted]
DEPUTY CLERK

REDACTED

EXHIBIT 7

AO 83 (Rev. 06/09) Summons in a Criminal Case

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

REDACTED

UNDER SEAL

United States of America
v.

Ladar Levison

Defendant

Case No. 1:13ec297

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

[redacted]
Issuing officer's signature

[redacted] – Deputy Clerk
Printed name and title

I declare under penalty of perjury that I have:

☐ Executed and returned this summons

☐ Returned this summons unexecuted

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

Date:

[redacted]
DEPUTY CLERK

Printed name and title

REDACTED

EXHIBIT 8

REDACTED

AO 110 (Rev. 01/09) Subpoena to Testify Before a Grand Jury

13-1 / 13032527 - 13 - 2351

United States District Court

for the

Eastern District of Virginia

SUBPOENA TO TESTIFY BEFORE THE GRAND JURY

TO: Ladar Norman Levison
[redacted]
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 testify 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

[redacted]

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:

[redacted]

Office of the United States Attorney
Justin W. Williams United States Attorney's Building
2100 Jamieson Avenue
Alexandria, Virginia 22314 (703) 299-3709

REDACTED

AO 110 (Rev. 01/09) Subpoena to Testify Before a Grand Jury (Page 2)

PROOF OF SERVICE

This subpoena for (name of individual or organization) Loder Norman Lewis
was received by me on (date) July 11, 2013.

☒ I personally served the subpoena on the individual at (place) [redacted]
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 individual) _____, 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, 2013

[redacted]

FBI - Dallas
Server's address

Additional information regarding attempted services, etc

REDACTED

EXHIBIT 9

AO 93 (Rev. 12/09) Search and Seizure Warrant

UNDER SEAL

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

REDACTED

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 [redacted]
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

/s/
Claude M. Hilton
United States District Judge

City and state: Alexandria, Virginia

REDACTED

ATTACHMENT A

Property to Be Searched

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

REDACTED

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 [redacted] including encryption keys and SSL keys;

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

REDACTED

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. §§ [redacted] those violations involving [redacted] 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 [redacted] including encryption keys and SSL keys;

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

REDACTED

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

REDACTED

EXHIBIT 10

UNDER SEAL

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

FILED
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

IN THE MATTER OF THE SEARCH OF	)	UNDER SEAL
	)	(Local Rule 49(B))
INFORMATION ASSOCIATED WITH [redacted]	)	No. 1:13sw522
	)	
THAT IS STORED AT PREMISES	)	
CONTROLLED BY LAVABIT, LLC	)	

REDACTED

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.

/s/
Claude M. Hilton
United States District Judge

Date: July 16, 2013
Alexandria, Virginia

REDACTED

EXHIBIT 11

REDACTED

UNDER SEAL

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

/s/
Claude M. Hilton
United States District Judge

REDACTED

EXHIBIT 12

IN THE UNITED STATES DISTRICT COURT FOR T

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

FILED
JUL 16 2013
CLERK, U.S. DISTRICT COURT

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

REDACTED

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.

REDACTED

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 [redacted] 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.

REDACTED

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

REDACTED

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

[redacted]

By [redacted]

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

REDACTED

EXHIBIT 13

REDACTED

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

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

COPY

TRANSCRIPT OF HEARING

BEFORE THE HONORABLE CLAUDE M. HILTON

UNITED STATES DISTRICT JUDGE

APPEARANCES:

For the United States: James Trump, Esq.
Andrew Peterson, Esq.
Brandon Van Grack, Esq.
Michael Ben'Ary, Esq.

For the Respondent: Ladar Levison, Respondent

Court Reporter: Tracy L. Westfall, RPR, CMRS, CCR

Proceedings reported by machine shorthand, transcript produced by computer-aided transcription.

REDACTED

P R O C E E D I N G S

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

MR. TRUMP: Good morning, Judge. Jim Trump on behalf of the United States. With me is Andy Peterson, Brandon Van Grack from the United States Department of Justice, Mr. Ben'Ary behind me, and Matt Braverman, special agent for the FBI.

THE COURT: All right.

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

THE COURT: All right. Mr. Trump.

MR. TRUMP: Your Honor, we submitted our supplemental paper this morning describing the communication we've had with Lavabit, LLC, through Mr. Levison. And I think, very simply, we would like this Court to inquire of Mr. Levison whether he intends to comply with the pen register order which would require him to allow the FBI access to his server to install a device which will extract data, filter that data, and provide that data to the FBI, and to provide the FBI with the encryption keys to the extent there is encrypted information, included among within the body of information called for by the pen register order.

As the Court is aware, and as we will provide with Mr. Levison, we obtained a search warrant this morning from Your Honor for the same encryption keys. Thus, to the extent there's

REDACTED

any question as to whether Mr. Levison would be required to provide these keys, it's now subject both to the pen register order and the search warrant, the seizure warrant.

That's where we stand, Your Honor. If Mr. Levison agrees to comply with the order, we would not seek any sanctions. We would ask that he be directed to forthwith make his servers available so the FBI can install that device and to extract the encryption keys.

If, however, he informs the Court he is not willing to comply with the order, we would ask the Court to impose sanctions. We suggested in our pleading a thousand dollars a day to be paid to the United States government until he complies. If he doesn't comply with that sanction, then we would be back in court seeking additional sanctions or charging additional offenses.

THE COURT: All right. Mr. Levison.

MR. LEVISON: Good morning, Your Honor. I'm not sure what order I should make these in, but I would like to request a couple of things by motion.

I'd like to move that all of the nonsensitive portions of the documents that were provided, i.e., everything except the account in question, be unsealed. I believe it's important for the industry and the people to understand what the government is requesting by demanding that I turn over these encryption keys for the entire service.

THE COURT: All right. What do you say to that, Mr. Trump? Deal with the motions before I --

MR. TRUMP: What Mr. Levison is trying to do, Your Honor, is invite industry to come in and litigate as a surrogate for him the issue of whether the encryption keys are part and parcel of the pen register order. And that's one of the reasons we sought the search warrant, to make it clear, whether through the search warrant or pen register order, he is required to provide these keys.

We know he's been in contact with attorneys who also represent industry groups and others who have litigated issues like this in the WikiLeaks context and others. But we would object to unsealing this matter because it's just Mr. --

THE COURT: And they've done that in connection with the issuance of a pen register?

MR. TRUMP: They have litigated privacy-related issues in the context of process under 2703. I'm not sure -- not a pen register, but with respect to 2703.

But we discussed this issue with Mr. Levison and his counsel by conference call. We indicated that the only data that the government seeks is that which is required by the pen register order. That it's just the basic header to e-mail traffic, sender, recipient, time, duration, that sort of thing.

If Mr. Levison wants to object to providing the keys, he can certainly object to doing that and then we can proceed

REDACTED

from there, but I don't think he's entitled to try to make this a public proceeding to invite others in to litigate those issues on his behalf.

THE COURT: All right. Well, I believe that to be correct. I mean, this is a criminal investigation. A pen register has been ordered and is here at issue, and any motion to unseal that will be denied.

You said you had another motion, I believe?

MR. LEVISON: Yeah. My issue is only with the SSL keys. So if that is litigated separately and that portion of the proceeding is unsealed, I'm comfortable with that.

THE COURT: I don't understand what you're saying, separate proceedings.

MR. LEVISON: Sorry. I have always agreed to the installation of the pen register device. I have only ever objected to turning over the SSL keys because that would compromise all of the secure communications in and out of my network, including my own administrative traffic.

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

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

THE COURT: Did my initial order -- I don't recall at the moment. Did my initial order recall the encrypted devices with the installation of a pen register?

MR. TRUMP: The pen register, as issued, just required all assistance, technical assistance, facilities, and

information, to facilitate the pen register.

This morning the search warrant required --

THE COURT: Yeah, but the search warrant's a different matter now. That's not before me this morning. The only thing that's before me this morning is the pen register.

MR. TRUMP: Correct.

THE COURT: So as I understand it, my initial order ordered nothing but that the pen register be put in place.

MR. TRUMP: And all technical assistance, information, and facilities necessary to implement the pen register. And it's our position that without the encryption keys, the data from the pen register will be meaningless. So to facilitate the actual monitoring required by the pen register, the FBI also requires the encryption keys.

THE COURT: Well, that could be, but I don't know that I need -- I don't know that I need to reach that because I've issued a search warrant for that.

MR. TRUMP: Correct, Your Honor. That the -- to avoid litigating this issue, we asked the Court to enter the seizure warrant.

THE COURT: Well, what I'm saying is if he agrees that the pen register be established, and that the only thing he doesn't want to do in connection with the pen register is to give up the encryption device or code --

MR. LEVISON: I've always maintained that.

REDACTED

THE COURT: -- so we've got no issue here. You're ready to do that?

MR. LEVISON: I've been ready to do that since Agent Howard spoke to me the first time.

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

MR. TRUMP: Well, then we have to inquire of Mr. Levison whether he will produce the encryption keys pursuant to the search warrant that Your Honor just signed.

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

MR. TRUMP: Well, it's the same issue. You could ask him, Your Honor. We can serve him with the warrant and ask him if he's going to comply rather than --

MR. LEVISON: Your Honor, I've also been issued a subpoena demanding those same keys, which I brought with me in the event that we would have to address that subpoena.

THE COURT: I don't know, Mr. Trump. I don't think I want to get involved in asking him. You can talk with him and see whether he's going to produce them or not and let him tell you. But I don't think I ought to go asking what he's going to do and what he's not going to do because I can't take any action about it anyway.

If he does not comply with the subpoena, there are remedies for that one way or another.

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

REDACTED

followed by a compulsion order from Judge Buchanan. The compulsion order required the encryption keys to be produced.

So, yes, part of the show cause order is to require compliance both with the pen register order and the compulsion order issued by Judge Buchanan.

And that order, which was attached to the show cause order, states, "To the extent any information, facilities, or technical assistance are under the control of Lavabit are needed to provide the FBI with the encrypted data, Lavabit shall provide such information, facilities, or technical assistance forthwith."

MR. LEVISON: I would object to that statement. I don't know if I'm wording this correctly, but what was in that order to compel was a statement that was incorrect.

Agent Howard seemed to believe that I had the ability to encrypt the e-mail content stored on our servers, which is not the case. I only have the keys that govern communications into and out of the network, and those keys are used to secure the traffic for all users, not just the user in question.

So the statement in that order compelling me to decrypt stuff and Agent Howard stating that I have the ability to do that is technically false or incorrect. There was never an explicit demand that I turn over these keys.

THE COURT: I don't know what bearing that would have, would it? I mean, I don't have a problem -- Judge Buchanan

UNDER SEAL

REDACTED

issued an order in addition to mine, and I'm not sure I ought to be enforcing Judge Buchanan's order.

My order, if he says that he will produce or allow the installation of the pen register, and in addition I have issued a search warrant for the codes that you want, which I did this morning, that's been entered, it seems that this issue is over as far as I'm concerned except I need to see that he allows the pen register and complies with the subpoena.

MR. TRUMP: Correct.

THE COURT: If he doesn't comply -- if he doesn't comply with the subpoena, then that has -- I have to address that.

MR. TRUMP: Right.

THE COURT: But right now there's nothing for me to address here unless he is not telling me correctly about the pen register.

MR. TRUMP: Well, we can -- Your Honor, if we can talk to Mr. Levison for five minutes, we can ask him whether he will honor the warrant that you just issued.

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

THE COURT: Well, what can I do about it if he doesn't, if he tells you he's not going to? You've got the right to go out and search and get it.

MR. TRUMP: Well, we can't get the information without his assistance. He's the only who knows and has possession of

REDACTED

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

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

THE COURT: Wait just a second.

You're trying to get me ahead. You're trying to get me to deal with a contempt before there's any contempt, and I have a problem with that.

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

THE COURT: I know you are. And I'd love for you-all to get together and do that. I don't want to deal with it either. But I don't think we can sit around and agree that there's going to be a default and I will address it before it occurs.

MR. TRUMP: I'm just trying to figure out whether there's going to be a default. We'll take care of that, Judge.

THE COURT: You can. I think the way we've got to do this -- and I'll listen to you. I'm cutting you off, I know, but I'll listen to you in a minute.

The way we have to do this, the hearing that's before me this morning on this issue of the pen register, that's been resolved, or so he's told me. I don't know whether you want to continue this one week and see if he complies with that, which I guess would be prudent to do, or a few days for him to comply with the pen register. Then we will wait and see what happens with the subpoena.

REDACTED

Because as far as my pen register order is concerned, he says he's going to comply with it. So that issue's over and done with. The next issue will be whether or not he complies with the subpoena. And I don't know and I don't want to presume, and I don't want him to represent to me what he intends to do when he can very well go home and decide he's going to do something different.

When that warrant is served, we'll know what he's going to do. I think we've got -- I don't see another way to do it.

MR. TRUMP: That's fine, Your Honor. We will serve the warrant on him as soon as we conclude this hearing, and we'll find out whether he will provide the keys or not.

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

MR. LEVISON: Well, I mean, I've always maintained that all the government needs to do is contact me and set up an appointment to install that pen register. So I don't know why there has never been any confusion about my willingness to install it. I've only ever objected to the providing of those keys which secure any sensitive information going back and forth.

But my motion, and I'm not sure if it's relevant or not because it deals more with the issue of the subpoena demanding the keys and for what will be the forthcoming search warrant, would be a continuance so that I can retain counsel to address

REDACTED

that particular issue.

THE COURT: Well, I mean, there's nothing before me with that. I've issued the subpoena. Whatever happens with that, that's -- you're trying to get me to do what Mr. Trump wanted to do and to arrange this beforehand.

MR. LEVISON: Well, I don't know if I have to appear before that grand jury right now and give the keys over or face arrest. I'm not a lawyer so I don't understand the procedure.

THE COURT: I don't know either. You need to have -- it would be wise to have a lawyer.

MR. LEVISON: Okay.

THE COURT: I don't know what's going to happen. I don't know. They haven't served the warrant yet. I have no idea. Don't know what's going to happen with it. You'll just have to figure that out, and it be wise to have a lawyer to do it, I would think.

MR. LEVISON: I guess while I'm here in regards to the pen register, would it be possible to request some sort of external audit to ensure that your orders are followed to the letter in terms of the information collected and preserved?

THE COURT: No. The law provides for those things, and any other additional or extra monitoring you might want or think is appropriate will be denied, if that's what you're requesting.

MR. LEVISON: Okay. I mean, it requests that the government return to the Court records --

THE COURT: You need to talk to a lawyer about what the law requires for the issuance of a pen register.

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

THE COURT: The law sets out what is done in that regard. Your lawyer can fill you in if you want to know.

MR. LEVISON: I've always been willing to accept the device. I just have some concern about ensuring that it's used properly.

THE COURT: Should we continue this to some specific date to see that he complies with the pen register?

MR. TRUMP: We can, Your Honor. It's a moot issue without the encryption keys.

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

MR. TRUMP: That's a practical --

THE COURT: -- but I don't think it is a moot issue. I mean, you-all have got the right to go in and put on that pen register. He says that he will do it. That's all that I've ordered.

Now, the other business about ordering that, Judge Buchanan made an order that he's going to have to supply what you say is the encryption codes to make the information useful. I don't know. I didn't enter that order. I have trouble making that connection.

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

REDACTED

do something in front of Judge Buchanan or not.

MR. LEVISON: You see, Judge, though that I've always been willing. They just didn't feel the need to set up an appointment.

THE COURT: What do you want me to do with this case? You want me to continue it? You want me to say it's moot right now and just end it?

MR. TRUMP: No. I think we can continue it. I don't know Mr. Levison's schedule. It can be done within hours of his return to Dallas.

THE COURT: Of course he can. You want to continue it till a week from Friday?

MR. TRUMP: Or a week from today.

MR. LEVISON: I'm not available within hours of my return, but I can meet with you on Thursday.

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

MR. TRUMP: A week from Friday.

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

THE CLERK: 26th.

THE COURT: The 26th?

MR. LEVISON: Acceptable to me.

THE COURT: We'll continue it to the 26th, and that's for determining whether or not that pen register has been installed as you request.

We can make it 10 o'clock.

REDACTED

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

THE COURT: All right. Thank you.

All right. Thank you-all. We'll adjourn till tomorrow morning at 9:30.

* * *

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

REDACTED

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/

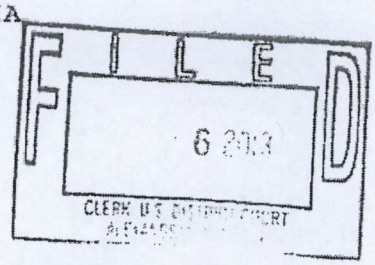
Tracy Westfall, RPR, CMRS, CCR

REDACTED

EXHIBIT 14

REDACTED

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	Criminal No. 1:13EC297

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.

/s/
Claude M. Hilton
United States District Judge

Alexandria, Virginia
July 16, 2013

REDACTED

EXHIBIT 15

REDACTED

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 [redacted] THAT IS STORED AND CONTROLLED AT PREMISES CONTROLLED BY LAVABIT LLC	No. 1:13SW522
In re Grand Jury	No. 13-1

FILED
5 2013
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

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

REDACTED

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 [redacted] ("Lavabit Subpoena and Warrant").

ARGUMENT

If the Government gains access to Lavabit's Master Key, it will have unlimited access to not only [redacted] ("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.

REDACTED

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.

REDACTED

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.

REDACTED

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.

REDACTED

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.

REDACTED

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

REDACTED

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

REDACTED

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

REDACTED

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:

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

Jesse R. Binnall

REDACTED

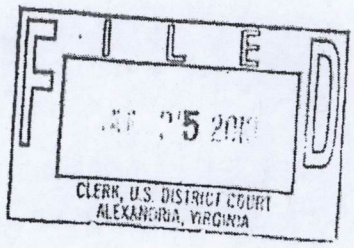
EXHIBIT 16

REDACTED

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 [redacted] 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

REDACTED

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 [redacted], 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

REDACTED

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.

REDACTED

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 [redacted]. However, Mr.

REDACTED

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

REDACTED

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 [redacted]. 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.

REDACTED

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.

REDACTED

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

REDACTED

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

REDACTED

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 [redacted] 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.

REDACTED

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
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

REDACTED

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:

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

Jesse R. Binnall

REDACTED

EXHIBIT 17

REDACTED

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 [redacted] 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

REDACTED

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

REDACTED

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

REDACTED

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 [redacted] for violations of numerous federal statutes [redacted]

REDACTED

A. Section 2703(d) Order

The criminal investigation has revealed that [redacted] has utilized and continues to utilize an e-mail account, [redacted] obtained through Lavabit, an electronic communications service provider. [redacted] 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 [redacted] 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 [redacted] ("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 [redacted] 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 [redacted] 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

REDACTED

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.*

REDACTED

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.

REDACTED

On July 13, 2013, Mr. Levison sent an e-mail to Assistant United States Attorney [redacted] 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 [redacted] 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 [redacted] including encryption keys and SSL keys" and (ii)

REDACTED

"[a]ll information necessary to decrypt data stored in or otherwise associated with the Lavabit account [redacted]" 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 [redacted]. 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

REDACTED

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

REDACTED

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

[redacted]

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

REDACTED

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 [xxxxxxxx@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

REDACTED

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

REDACTED

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 [redacted] including encryption keys and SSL keys;
>
> b. All information necessary to decrypt data stored in or otherwise associated with the Lavabit account [redacted]

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

REDACTED

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.

REDACTED

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 [redacted]. Moreover, the restrictions are narrowly tailored to restrict

REDACTED

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.

REDACTED

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 [redacted]". Mot. to Unseal at 4; *id.* at 6 ("the government has a legitimate interest in tracking" [redacted] 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 [redacted], along with the public, would learn of the monitoring of [redacted]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

REDACTED

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,

REDACTED

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

REDACTED

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.

REDACTED

"[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 [redacted]

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

REDACTED

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

REDACTED

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

REDACTED

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.

REDACTED

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: [redacted]

Assistant United States Attorney
United States Attorney's Office
2100 Jamieson Ave.
Alexandria, VA 22314
[redacted]
703-299-3700

REDACTED

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
[redacted]

[redacted]
Assistant United States Attorney
United States Attorney's Office
2100 Jamieson Ave.
Alexandria, VA 22314
[redacted]
703-299-3700

REDACTED

EXHIBIT 18

REDACTED

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 [redacted] 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.

COPY

TRANSCRIPT OF HEARING

BEFORE THE HONORABLE CLAUDE M. HILTON

UNITED STATES DISTRICT JUDGE

APPEARANCES:

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.

PROCEEDINGS

THE CLERK: *In re:* Case Nos. 1:13 EC 297, 1:13 SW 522, and Grand Jury No. 13-1.

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

THE COURT: Good morning.

MR. BINNALL: Good morning, Your Honor. Jesse Binnall on behalf of Lavabit and Mr. Levison.

THE COURT: All right.

MR. BINNALL: May it please the Court. We're before the Court today on two separate motions, a motion to quash the requirement of Lavabit to produce its encryption keys and the motion to unseal and lift the nondisclosure requirements of Mr. Levison.

Your Honor, the motion to quash in this arises because the privacy of users is at -- of Lavabit's users are at stake. We're not simply speaking of the target of this investigation. We're talking about over 400,000 individuals and entities that are users of Lavabit who use this service because they believe their communications are secure.

By handing over the keys, the encryption keys in this case, they necessarily become less secure. In this case it is true that the face of the warrant itself does limit the documents or -- and communications to be viewed and the specific metadata to be viewed to the target of the case, [redacted]

However, there is a lack of any sort of check or balance in order to ensure that the -- that the encrypted data of other Lavabit users remain secure. The encryption in this case doesn't protect only content. It protects login data and the other -- some of the other metadata involved in this case.

We believe that this is not the least restrictive means in order to provide the government the data that they are looking for. Specifically --

THE COURT: You have two different encryption codes, one for the logins and the messages that are transmitted. You have another code that encrypts the content of the messages, right?

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

From my understanding of the way that this works is that there is one SSL key. That SSL key is what is issue in this case, and that SSL key specifically protects the communication, the over -- the breadth of the communication itself from the user's actual computer to the server to make sure that the user is communicating with exactly who the user intends to be communicating with, the server.

And that's one of the things that SSL does. It ensures that you're talking to the right person via e-mail and there's not a so-called man in the middle who's there to take that message away.

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

message and interpret the message as well?

MR. BINNALL: My understanding is that it does, Your Honor, but because that's not my technical expertise, I'm not going to represent to the Court anything on that one way or another. But my understanding is there is one general key here that is at issue.

THE COURT: Well, why would you set up such? I mean, a telephone, you've got telephone numbers and --

MR. BINNALL: Correct.

THE COURT: -- those can be traced very easily without any look at the content of the message that's there. You-all could have set up something the same way.

MR. BINNALL: We could have, Your Honor. Actually, if you're to --

THE COURT: So if anybody's -- you're blaming the government for something that's overbroad, but it seems to me that your client is the one that set up the system that's designed not to protect that information, because you know that there needs to be access to calls that go back and forth to one person or another. And to say you can't do that just because you've set up a system that everybody has to -- has to be unencrypted, if there's such a word, that doesn't seem to me to be a very persuasive argument.

MR. BINNALL: I understand the Court's point, and this is the way that I understand why it's done that way.

REDACTED

There's different security aspects involved for people who want to protect their privacy, and there certainly is the actual content of the message themselves. That's certainly what I would concede is the highest security interest.

But there's also the security interest to make sure that they're communicating with who you want to be communicating with. That is equally of a concern for privacy issues because that is, at the end of the day, one of the things that secures the content of the message.

In this case it is true that most Internet service providers do log, is what they call it, a lot of the metadata that the government wants in this case without that necessarily being encrypted, things such as who something is going to, who it's going from, the time it's being sent, the IP address from which it is being sent.

Lavabit code is not something that you buy off the shelf. It is code that was custom made. It was custom made in order to secure privacy to the largest extent possible and to be the most secure way possible for multiple people to communicate, and so it has chosen specifically not to log that information.

Now, that is actually information that my client has offered to start logging with the particular user in this case. It is, however, something that is quite burdensome on him. It is something that would be custom code that would take between 20 to 40 hours for him to be able to produce. We believe that

REDACTED

is a better alternative than turning over the encryption key which can be used to get the data for all Lavabit users.

I hope that addresses the Court's concern kind of with regard to the metadata and why it is not more -- why Lavabit hasn't created an encryption system that may honestly be more within the mainstream, but this is a provider that specifically was started in order to have to protect privacy interests more than the average Internet service provider.

THE COURT: I can understand why the system was set up, but I think the government is -- government's clearly entitled to the information that they're seeking, and just because you-all have set up a system that makes that difficult, that doesn't in any way lessen the government's right to receive that information just as they would from any telephone company or any other e-mail source that could provide it easily. Whether it's -- in other words, the difficulty or the ease in obtaining the information doesn't have anything to do with whether or not the government's lawfully entitled to the information.

MR. BINNALL: It is -- and we don't disagree that the government is entitled to the information. We actually --

THE COURT: Well, how are we going to get it? I'm going to have to deny your motion to quash. It's just not overbroad. The government's asking for a very narrow, specific bit of information, and it's information that they're entitled to.

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

MR. BINNALL: Your Honor, what I would still say is the best method for them to get it is, first of all, there be some way for there to be some sort of accountability other than just relying on the government to say we're not going to go outside the scope of the warrant.

This is nothing that is, of course, personal against the government and the, you know, very professional law enforcement officers involved in this case. But quite simply, the way the Constitution is set up, it's set up in a way to ensure that there's some sort of checks and balances and accountability.

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

MR. BINNALL: Well --

THE COURT: Suggest something to me.

MR. BINNALL: I think that the least restrictive means possible here is that the government essentially pay the reasonable expenses, meaning in this case my client's extensive labor costs to be capped at a reasonable amount.

THE COURT: Has the government ever done that in one of these pen register cases?

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

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

MR. BINNALL: And Your Honor's certainly seen more of these than I have.

REDACTED

THE COURT: So would it be reasonable to start now with your client?

MR. BINNALL: I think everyone would agree that this is an unusual case. And that this case, in order to protect the privacy of 400,000-plus other users, some sort of relatively small manner in which to create a log system for this one user to give the government the metadata that they're looking for is the least restrictive mean here, and we can do that in a way that doesn't compromise the security keys.

This is actually a way that my client --

THE COURT: You want to do it in a way that the government has to trust you --

MR. BINNALL: Yes, Your Honor.

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

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

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

MR. BINNALL: Your Honor, because that's what the basis of Fourth Amendment law says is more acceptable, is that the government is the entity that you really need the checks and balances on.

Now, my --

THE COURT: I don't know that the Fourth Amendment says that. This is a criminal investigation.

MR. BINNALL: That is absolutely correct.

THE COURT: A criminal investigation, and I don't know that the Fourth Amendment says that the person being investigated here is entitled to more leeway and more rights than the government is. I don't know.

MR. BINNALL: There certainly is a balance of power there. I, of course, am not here to represent the interest of [redacted] I'm here specifically looking over my client who has sensitive data --

THE COURT: I understand. I'm trying to think of working out something. I'm not sure you're suggesting anything to me other than either you do it and the government has to trust you to give them whatever you want to give them or you have to trust the government that they're not going to go into your other files.

Is there some other route?

MR. BINNALL: I would suggest that the government -- I'm sorry -- that the Court can craft an order to say that we can -- that we should work in concert with each other in order to come up with this coding system that gives the government all of the metadata that we can give them through this logging procedure that we can install in the code, and then using that as a least restrictive means to see if that can get the government the information that they're looking for on the specific account.

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

MR. BINNALL: I mean, 20, 40 hours. So I would suggest that would probably be a week to a week and a half, Your Honor, although I would be willing to talk to my client to see if we can get that expedited.

THE COURT: To install it?

MR. BINNALL: Well, to write the code.

THE COURT: You don't have a code right at the moment. You would have to write something?

MR. BINNALL: That's correct. And the portion of the government's brief that talks about the money that he was looking for is that reasonable expense for him basically to do nothing for that period of time but write code to install in order to take the data from [redacted] and put it in a way that the government will see the logged metadata involved.

THE COURT: All right. I think I understand your position. I don't think you need to argue this motion to unseal. This is a grand jury matter and part of an ongoing criminal investigation, and any motion to unseal will be denied.

MR. BINNALL: If I could have the Court's attention just on one issue of the nondisclosure provision of this. And I understand the Court's position on this, but there is other privileged communications if the Court would be so generous as to allow me very briefly to address that issue?

There's other First Amendment considerations at issue with not necessarily just the sealing of this, but what

REDACTED

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

The First Amendment, of course, doesn't just cover speech and assembly, but the right to petition for a redress of grievances. We're talking about a statute here, and, honestly, a statute that is very much in the public eye and involving issues that are currently pending before Congress.

I think the way that the order currently is written, besides being --

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

MR. BINNALL: I'm talking about the sealing order and the order that prohibits Mr. Levison from disclosing any information.

Now, we don't want to disclose -- we have no intention of disclosing the target, but we would like to be able to, for instance, talk to members of the legislature and their staffs about rewriting this in a way that's --

THE COURT: No. This is an ongoing criminal investigation, and there's no leeway to disclose any information about it.

MR. BINNALL: And so at that point it will remain with only Mr. Levison and his lawyers, and we'll keep it at that.

THE COURT: Let me hear from Mr. Trump.

Is there some way we can work this out or something that I can do with an order that will help this or what?

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

you've already articulated the reason why is that anything done by Mr. Levison in terms of writing code or whatever, we have to trust Mr. Levison that we have gotten the information that we were entitled to get since June 28th. He's had every opportunity to propose solutions to come up with ways to address his concerns and he simply hasn't.

We can assure the Court that the way that this would operate, while the metadata stream would be captured by a device, the device does not download, does not store, no one looks at it. It filters everything, and at the back end of the filter, we get what we're required to get under the order.

So there's no agents looking through the 400,000 other bits of information, customers, whatever. No one looks at that, no one stores it, no one has access to it. All we're going to look at and all we're going to keep is what is called for under the pen register order, and that's all we're asking this Court to do.

THE COURT: All right. Well, I think that's reasonable. So what is this before me for this morning other than this motion to quash and unseal which I've ruled on?

MR. TRUMP: The only thing is to order the production of the encryption keys, which just --

THE COURT: Hasn't that already been done? There's a subpoena for that.

MR. TRUMP: There's a search warrant for it, the motion

REDACTED

to quash.

THE COURT: Search warrant.

MR. TRUMP: Excuse me?

THE COURT: I said subpoena, but I meant search warrant.

MR. TRUMP: We issued both, Your Honor, but Your Honor authorized the seizure of that information. And we would ask the Court to enforce that by directing Mr. Levison to turn over the encryption keys.

If counsel represents that that will occur, we can not waste any more of the Court's time. If he represents that Mr. Levison will not turn over the encryption keys, then we have to discuss what remedial action this Court can take to require compliance with that order.

THE COURT: Well, I will order the production of those -- of those keys.

Is that simply Mr. Levison or is that the corporation as well?

MR. TRUMP: That's one and the same, Your Honor.

Just so the record is clear. We understand from Mr. Levison that the encryption keys were purchased commercially. They're not somehow custom crafted by Mr. Levison. He buys them from a vendor and then they're installed.

THE COURT: Well, I will order that. If you will

REDACTED

present an order to me, I'll enter it later on.

MR. TRUMP: Thank you.

MR. BINNALL: Thank you, Your Honor.

As far as time frame goes, my client did ask me if the Court did order this if the Court could give him approximately five days in order to actually physically get the encryption keys here. And so it will be -- or just some sort of reasonable time frame to get the encryption keys here and in the government's hands. He did ask me to ask exactly the manner that those are to be turned over.

MR. TRUMP: Your Honor, we understand that this can be done almost instantaneously, as soon as Mr. Levison makes contact with an agent in Dallas, and we would ask that he be given 24 hours or less to comply. This has been going on for a month.

THE COURT: Yeah, I don't think 24 -- 24 hours would be reasonable. Doesn't have to do it in the next few minutes, but I would think something like this, it's not anything he has to amass or get together. It's just a matter of sending something.

So I think 24 hours would be reasonable.

MR. BINNALL: Yes. Thank you, Your Honor.

THE COURT: All right. And you'll present me an order?

MR. TRUMP: We will, Your Honor. Thank you.

THE COURT: All right. Thank you-all, and we'll adjourn until -- or stand in recess till 3 o'clock. Well,

REDACTED

recess till 9 o'clock tomorrow morning.

* * *

(Proceedings concluded at 10:25 a.m.)

CERTIFICATION

I certify, this 19th day of August 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

Tracy Westfall, RPR, CMRS, CCR

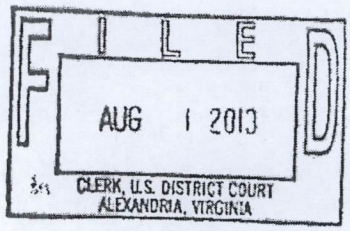
REDACTED

EXHIBIT 19

REDACTED

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 [redacted] 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

REDACTED

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.

/s/
Claude M. Hilton
United States District Judge

Alexandria, Virginia
August 1, 2013

REDACTED

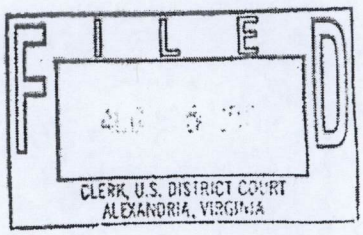
EXHIBIT 20

REDACTED

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 [redacted] THAT IS STORED AT PREMISES CONTROLLED BY LAVABIT LLC	)	No. 1:13SW522
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

REDACTED

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.

REDACTED

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.

REDACTED

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: [redacted]

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

REDACTED

Attachment A

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

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.

REDACTED

EXHIBIT 21

REDACTED

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

Alexandria Division

FILED
AUG 5 2013
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

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 [redacted] 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

REDACTED

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.

/s/
Claude M. Hilton
United States District Judge

Alexandria, Virginia
August 5, 2013

REDACTED

EXHIBIT 22

REDACTED

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 [redacted]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

REDACTED

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:

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

Jesse R. Binnall

REDACTED

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

	FILED UNDER SEAL
In re Grand Jury	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

REDACTED

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:

[redacted]

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

[redacted]

Jesse R. Binnall

REDACTED

EXHIBIT 23

REDACTED

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 IN THE MATTER OF THE SEARCH AND SEIZURE OF INFORMATION ASSOCIATED WITH [redacted] THAT IS STORED AND CONTROLLED AT PREMISES CONTROLLED BY LAVABIT LLC	**FILED UNDER SEAL** 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

REDACTED

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:

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

Jesse R. Binnall

REDACTED

EXHIBIT 24

REDACTED

Lavabit Online Media Links

Democracy Now Interview:

[redacted]

Democracy Now Interview Transcript:

[redacted]

Huff Post Interview:

[redacted]

RT Interview:

[redacted]

Ron Paul Interview:

[redacted]

REDACTED

[redacted]

REDACTED

[redacted]

REDACTED

EXHIBIT 25

REDACTED

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 [redacted] 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

PROPOSED ORDER

The United States has proposed partially unsealing records in this matter due to public disclosures made by Ladar Levison and Lavabit, LLC and for the purpose of creating a public record for Mr. Levison's appeal. The Court has considered the original sealing orders, the motions in support of the original sealing orders, the government's ex parte motion to unseal certain documents, and the prior pleadings of Mr. Levison, and hereby finds that:

(1) the government has a compelling interest in keeping certain information in the documents sealed, and the government has proposed redacted versions of the documents that minimizes the information under seal;

(2) the government's interest in keeping the redacted material sealed outweighs any public interest in disclosure; and

REDACTED

(3) having considered alternatives to the proposed redactions none will adequately protect that interest; it is hereby

ORDERED that the redacted versions of certain records filed in the above captioned matter are partially unsealed. The unsealed records are attached to this Order. To the extent any such record is covered by a non-disclosure Order issued pursuant to 18 U.S.C. § 2705(b), the non-disclosure obligation does not apply to the unsealed, redacted version of the document. The Clerk of the Court may publicly release the redacted version of any of the records attached to this Order. Any record not attached to this Order, as well as the unredacted copies of any record filed in the above-captioned matter, including the government's *ex parte*, sealed Motion to Unseal and Statement of Reasons will remain sealed until further Order of the Court.

The Honorable Claude M. Hilton
United States District Judge

Date: _____
Alexandria, VA

REDACTED

EXHIBIT 26

REDACTED

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 [redacted] 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

PROPOSED ORDER

The United States has proposed partially unsealing records in this matter due to public disclosures made by Ladar Levison and Lavabit, LLC and for the purpose of creating a public record for Mr. Levison's appeal. The Court has considered the original sealing orders, the motions in support of the original sealing orders, the government's ex parte motion to unseal certain documents, and the prior pleadings of Mr. Levison, and hereby finds that:

(1) the government has a compelling interest in keeping certain information in the documents sealed, and the government has proposed redacted versions of the documents that minimizes the information under seal;

(2) the government's interest in keeping the redacted material sealed outweighs any public interest in disclosure; and

REDACTED

(3) having considered alternatives to the proposed redactions none will adequately protect that interest; it is hereby

ORDERED that the redacted versions of certain records filed in the above captioned matter are partially unsealed. The unsealed records are attached to this Order. To the extent any such record is covered by a non-disclosure Order issued pursuant to 18 U.S.C. § 2705(b), the non-disclosure obligation does not apply to the unsealed, redacted version of the document. The Clerk of the Court may publicly release the redacted version of any of the records attached to this Order. Any record not attached to this Order, as well as the unredacted copies of any record filed in the above-captioned matter, including the government's *ex parte*, sealed Motion to Unseal and Statement of Reasons will remain sealed until further Order of the Court.

The Honorable Claude M. Hilton
United States District Judge

Date: _____
Alexandria, VA

REDACTED

FILED
OCT - 2 2013
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

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 [redacted] 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

ORDER

The United States has proposed partially unsealing records in this matter due to public disclosures made by Ladar Levison and Lavabit, LLC and for the purpose of creating a public record for Mr. Levison's appeal. The Court has considered the original sealing orders, the motions in support of the original sealing orders, the government's ex parte motion to unseal certain documents, and the prior pleadings of Mr. Levison, and hereby finds that:

(1) the government has a compelling interest in keeping certain information in the documents sealed, and the government has proposed redacted versions of the documents that minimizes the information under seal;

(2) the government's interest in keeping the redacted material sealed outweighs any public interest in disclosure; and

REDACTED

(3) having considered alternatives to the proposed redactions none will adequately protect that interest; it is hereby

ORDERED that the redacted versions of certain records filed in the above captioned matter are partially unsealed. The unsealed records are attached to this Order. To the extent any such record is covered by a non-disclosure Order issued pursuant to 18 U.S.C. § 2705(b), the non-disclosure obligation does not apply to the unsealed, redacted version of the document. The Clerk of the Court may publicly release the redacted version of any of the records attached to this Order. Any record not attached to this Order, as well as the unredacted copies of any record filed in the above-captioned matter, including the government's *ex parte*, sealed Motion to Unseal and Statement of Reasons will remain sealed until further Order of the Court.

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

Date: Oct. 2, 2013
Alexandria, VA

REDACTED

EXHIBIT 1

REDACTED

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. § 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

REDACTED

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.

/s/
John F. Anderson
United States Magistrate Judge

June 10, 2013
Date

A TRUE COPY, TESTE:
CLERK, U.S. DISTRICT COURT
BY [redacted]
DEPUTY CLERK

REDACTED

ATTACHMENT A

I. The Account(s)

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

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).

REDACTED

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

REDACTED

EXHIBIT 2

REDACTED

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 INSTALLATION AND USE OF A PEN REGISTER/TRAP AND TRACE DEVICE ON AN ELECTRONIC MAIL ACCOUNT	)	(Under Seal) 1:13 EC 297

ORDER

This matter having come before the Court pursuant to an Application under 18 U.S.C. § 3122, by [redacted], 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 [redacted] that is registered to subscriber [redacted] 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 [redacted].

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

REDACTED

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

REDACTED

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

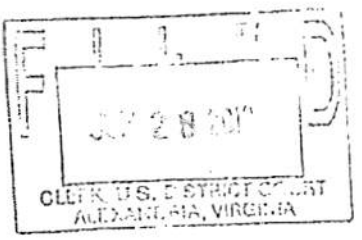
Hon. Theresa C. Buchanan
United States Magistrate Judge

Date: 9/28/13

REDACTED

EXHIBIT 3

REDACTED



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 [redacted]. 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

REDACTED

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

REDACTED

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: [redacted]
Assistant United States Attorney

REDACTED

EXHIBIT 4

REDACTED

FILED
JUN 28 2013
CLERK, U.S. DISTRICT COURT
ALEXANDRIA

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 INSTALLATION AND USE OF A PEN REGISTER/TRAP AND TRACE DEVICE ON AN ELECTRONIC MAIL ACCOUNT	)	(Under Seal) 1:13 EC 297

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 [redacted], 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;"

REDACTED

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

/s/
Theresa Carroll Buchanan
United States Magistrate Judge

Hon. Theresa C. Buchanan
United States Magistrate Judge

REDACTED

EXHIBIT 5

REDACTED

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

FILED
JUL - 9 2013
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

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 [redacted]

[redacted]

REDACTED

[redacted]

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.

REDACTED

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 [redacted] 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

REDACTED

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: [redacted]

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

REDACTED

PROPOSED
ORDER TO SHOW CAUSE

REDACTED

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

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

REDACTED

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

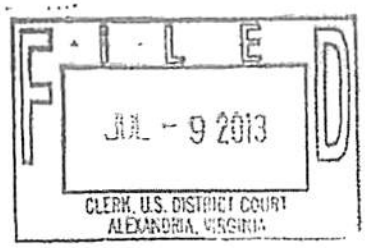
REDACTED

EXHIBIT 6

REDACTED

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)))	

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

REDACTED

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

/s/
Claude M. Hilton
United States District Judge

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

BY [redacted]
DEPUTY CLERK

REDACTED

EXHIBIT 7

AO 83 (Rev. 06/09) Summons in a Criminal Case

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

REDACTED

UNDER SEAL

United States of America
v.

Ladar Levison

Defendant

Case No. 1:13ec297

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

[redacted]

Issuing officer's signature

[redacted] – Deputy Clerk

Printed name and title

I declare under penalty of perjury that I have:

☐ Executed and returned this summons ☐ Returned this summons unexecuted

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

Date:

[redacted]
DEPUTY CLERK

Printed name and title

REDACTED

EXHIBIT 8

REDACTED

AO 110 (Rev. 01/09) Subpoena to Testify Before a Grand Jury — 13-1 / 13GJ527 / 13-2451

United States District Court
for the
Eastern District of Virginia

SUBPOENA TO TESTIFY BEFORE THE GRAND JURY

TO: Ladar Norman Levison
[redacted]
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 testify 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:	Date and Time:
UNITED STATES DISTRICT COURT 401 Courthouse Square Alexandria, Virginia 22314	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

[redacted]

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:

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

REDACTED

AO 110 (Rev. 01/09) Subpoena to Testify Before a Grand Jury (Page 2)

PROOF OF SERVICE

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

☒ I personally served the subpoena on the individual at (place) [redacted]
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 individual) _____, 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, 2013

[redacted]

PBP - Dallas
Server's address

Additional information regarding attempted services, etc:

REDACTED

EXHIBIT 9

AO 93 (Rev. 12/09) Search and Seizure Warrant

UNDER SEAL

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

REDACTED

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 [redacted]
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

/s/
Claude M. Hilton
United States District Judge

City and state: Alexandria, Virginia

REDACTED

ATTACHMENT A

Property to Be Searched

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

REDACTED

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 [redacted] including encryption keys and SSL keys;

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

REDACTED

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. §§ [redacted], those violations involving [redacted] 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 [redacted], including encryption keys and SSL keys;

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

REDACTED

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

REDACTED

EXHIBIT 10

UNDER SEAL

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

FILED
[illegible] 16 2013
CLERK U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

IN THE MATTER OF THE SEARCH OF	)	UNDER SEAL
	)	(Local Rule 49(B))
INFORMATION ASSOCIATED WITH [redacted]	)	No. 1:13sw522
	)	
THAT IS STORED AT PREMISES	)	REDACTED
CONTROLLED BY LAVABIT, LLC	)	

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.

/s/
Claude M. Hilton
United States District Judge

Date: July 16, 2013
Alexandria, Virginia

REDACTED

EXHIBIT 11

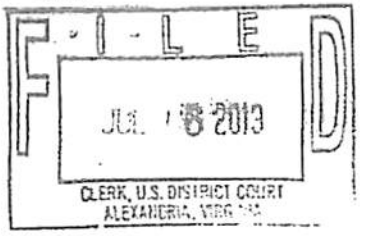
UNDER SEAL

REDACTED

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



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

/s/
Claude M. Hilton
United States District Judge

REDACTED

EXHIBIT 12

IN THE UNITED STATES DISTRICT COURT FOR T

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

FILED
JUL 15 2013
CLERK, U.S. DISTRICT COURT

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

REDACTED

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.

REDACTED

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 [redacted] 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.

REDACTED

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 [redacted]

REDACTED

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

REDACTED

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 [redacted]

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

REDACTED

EXHIBIT 13

REDACTED

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

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

COPY

TRANSCRIPT OF HEARING

BEFORE THE HONORABLE CLAUDE M. HILTON

UNITED STATES DISTRICT JUDGE

APPEARANCES:

For the United States: James Trump, Esq.
Andrew Peterson, Esq.
Brandon Van Grack, Esq.
Michael Ben'Ary, Esq.

For the Respondent: Ladar Levison, Respondent

Court Reporter: Tracy L. Westfall, RPR, CMRS, CCR

Proceedings reported by machine shorthand, transcript produced by computer-aided transcription.

REDACTED

PROCEEDINGS

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

MR. TRUMP: Good morning, Judge. Jim Trump on behalf of the United States. With me is Andy Peterson, Brandon Van Grack from the United States Department of Justice, Mr. Ben'Ary behind me, and Matt Braverman, special agent for the FBI.

THE COURT: All right.

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

THE COURT: All right. Mr. Trump.

MR. TRUMP: Your Honor, we submitted our supplemental paper this morning describing the communication we've had with Lavabit, LLC, through Mr. Levison. And I think, very simply, we would like this Court to inquire of Mr. Levison whether he intends to comply with the pen register order which would require him to allow the FBI access to his server to install a device which will extract data, filter that data, and provide that data to the FBI, and to provide the FBI with the encryption keys to the extent there is encrypted information, included among within the body of information called for by the pen register order.

As the Court is aware, and as we will provide with Mr. Levison, we obtained a search warrant this morning from Your Honor for the same encryption keys. Thus, to the extent there's

REDACTED

any question as to whether Mr. Levison would be required to provide these keys, it's now subject both to the pen register order and the search warrant, the seizure warrant.

That's where we stand, Your Honor. If Mr. Levison agrees to comply with the order, we would not seek any sanctions. We would ask that he be directed to forthwith make his servers available so the FBI can install that device and to extract the encryption keys.

If, however, he informs the Court he is not willing to comply with the order, we would ask the Court to impose sanctions. We suggested in our pleading a thousand dollars a day to be paid to the United States government until he complies. If he doesn't comply with that sanction, then we would be back in court seeking additional sanctions or charging additional offenses.

THE COURT: All right. Mr. Levison.

MR. LEVISON: Good morning, Your Honor. I'm not sure what order I should make these in, but I would like to request a couple of things by motion.

I'd like to move that all of the nonsensitive portions of the documents that were provided, i.e., everything except the account in question, be unsealed. I believe it's important for the industry and the people to understand what the government is requesting by demanding that I turn over these encryption keys for the entire service.

THE COURT: All right. What do you say to that, Mr. Trump? Deal with the motions before I --

MR. TRUMP: What Mr. Levison is trying to do, Your Honor, is invite industry to come in and litigate as a surrogate for him the issue of whether the encryption keys are part and parcel of the pen register order. And that's one of the reasons we sought the search warrant, to make it clear, whether through the search warrant or pen register order, he is required to provide these keys.

We know he's been in contact with attorneys who also represent industry groups and others who have litigated issues like this in the WikiLeaks context and others. But we would object to unsealing this matter because it's just Mr. --

THE COURT: And they've done that in connection with the issuance of a pen register?

MR. TRUMP: They have litigated privacy-related issues in the context of process under 2703. I'm not sure -- not a pen register, but with respect to 2703.

But we discussed this issue with Mr. Levison and his counsel by conference call. We indicated that the only data that the government seeks is that which is required by the pen register order. That it's just the basic header to e-mail traffic, sender, recipient, time, duration, that sort of thing.

If Mr. Levison wants to object to providing the keys, he can certainly object to doing that and then we can proceed

REDACTED

from there, but I don't think he's entitled to try to make this a public proceeding to invite others in to litigate those issues on his behalf.

THE COURT: All right. Well, I believe that to be correct. I mean, this is a criminal investigation. A pen register has been ordered and is here at issue, and any motion to unseal that will be denied.

You said you had another motion, I believe?

MR. LEVISON: Yeah. My issue is only with the SSL keys. So if that is litigated separately and that portion of the proceeding is unsealed, I'm comfortable with that.

THE COURT: I don't understand what you're saying, separate proceedings.

MR. LEVISON: Sorry. I have always agreed to the installation of the pen register device. I have only ever objected to turning over the SSL keys because that would compromise all of the secure communications in and out of my network, including my own administrative traffic.

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

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

THE COURT: Did my initial order -- I don't recall at the moment. Did my initial order recall the encrypted devices with the installation of a pen register?

MR. TRUMP: The pen register, as issued, just required all assistance, technical assistance, facilities, and

REDACTED

information, to facilitate the pen register.

This morning the search warrant required --

THE COURT: Yeah, but the search warrant's a different matter now. That's not before me this morning. The only thing that's before me this morning is the pen register.

MR. TRUMP: Correct.

THE COURT: So as I understand it, my initial order ordered nothing but that the pen register be put in place.

MR. TRUMP: And all technical assistance, information, and facilities necessary to implement the pen register. And it's our position that without the encryption keys, the data from the pen register will be meaningless. So to facilitate the actual monitoring required by the pen register, the FBI also requires the encryption keys.

THE COURT: Well, that could be, but I don't know that I need -- I don't know that I need to reach that because I've issued a search warrant for that.

MR. TRUMP: Correct, Your Honor. That the -- to avoid litigating this issue, we asked the Court to enter the seizure warrant.

THE COURT: Well, what I'm saying is if he agrees that the pen register be established, and that the only thing he doesn't want to do in connection with the pen register is to give up the encryption device or code --

MR. LEVISON: I've always maintained that.

THE COURT: -- so we've got no issue here. You're ready to do that?

MR. LEVISON: I've been ready to do that since Agent Howard spoke to me the first time.

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

MR. TRUMP: Well, then we have to inquire of Mr. Levison whether he will produce the encryption keys pursuant to the search warrant that Your Honor just signed.

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

MR. TRUMP: Well, it's the same issue. You could ask him, Your Honor. We can serve him with the warrant and ask him if he's going to comply rather than --

MR. LEVISON: Your Honor, I've also been issued a subpoena demanding those same keys, which I brought with me in the event that we would have to address that subpoena.

THE COURT: I don't know, Mr. Trump. I don't think I want to get involved in asking him. You can talk with him and see whether he's going to produce them or not and let him tell you. But I don't think I ought to go asking what he's going to do and what he's not going to do because I can't take any action about it anyway.

If he does not comply with the subpoena, there are remedies for that one way or another.

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

REDACTED

followed by a compulsion order from Judge Buchanan. The compulsion order required the encryption keys to be produced.

So, yes, part of the show cause order is to require compliance both with the pen register order and the compulsion order issued by Judge Buchanan.

And that order, which was attached to the show cause order, states, "To the extent any information, facilities, or technical assistance are under the control of Lavabit are needed to provide the FBI with the encrypted data, Lavabit shall provide such information, facilities, or technical assistance forthwith."

MR. LEVISON: I would object to that statement. I don't know if I'm wording this correctly, but what was in that order to compel was a statement that was incorrect.

Agent Howard seemed to believe that I had the ability to encrypt the e-mail content stored on our servers, which is not the case. I only have the keys that govern communications into and out of the network, and those keys are used to secure the traffic for all users, not just the user in question.

So the statement in that order compelling me to decrypt stuff and Agent Howard stating that I have the ability to do that is technically false or incorrect. There was never an explicit demand that I turn over these keys.

THE COURT: I don't know what bearing that would have, would it? I mean, I don't have a problem -- Judge Buchanan

REDACTED

issued an order in addition to mine, and I'm not sure I ought to be enforcing Judge Buchanan's order.

My order, if he says that he will produce or allow the installation of the pen register, and in addition I have issued a search warrant for the codes that you want, which I did this morning, that's been entered, it seems that this issue is over as far as I'm concerned except I need to see that he allows the pen register and complies with the subpoena.

MR. TRUMP: Correct.

THE COURT: If he doesn't comply -- if he doesn't comply with the subpoena, then that has -- I have to address that.

MR. TRUMP: Right.

THE COURT: But right now there's nothing for me to address here unless he is not telling me correctly about the pen register.

MR. TRUMP: Well, we can -- Your Honor, if we can talk to Mr. Levison for five minutes, we can ask him whether he will honor the warrant that you just issued.

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

THE COURT: Well, what can I do about it if he doesn't, if he tells you he's not going to? You've got the right to go out and search and get it.

MR. TRUMP: Well, we can't get the information without his assistance. He's the only who knows and has possession of

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

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

THE COURT: Wait just a second.

You're trying to get me ahead. You're trying to get me to deal with a contempt before there's any contempt, and I have a problem with that.

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

THE COURT: I know you are. And I'd love for you-all to get together and do that. I don't want to deal with it either. But I don't think we can sit around and agree that there's going to be a default and I will address it before it occurs.

MR. TRUMP: I'm just trying to figure out whether there's going to be a default. We'll take care of that, Judge.

THE COURT: You can. I think the way we've got to do this -- and I'll listen to you. I'm cutting you off, I know, but I'll listen to you in a minute.

The way we have to do this, the hearing that's before me this morning on this issue of the pen register, that's been resolved, or so he's told me. I don't know whether you want to continue this one week and see if he complies with that, which I guess would be prudent to do, or a few days for him to comply with the pen register. Then we will wait and see what happens with the subpoena.

Because as far as my pen register order is concerned, he says he's going to comply with it. So that issue's over and done with. The next issue will be whether or not he complies with the subpoena. And I don't know and I don't want to presume, and I don't want him to represent to me what he intends to do when he can very well go home and decide he's going to do something different.

When that warrant is served, we'll know what he's going to do. I think we've got -- I don't see another way to do it.

MR. TRUMP: That's fine, Your Honor. We will serve the warrant on him as soon as we conclude this hearing, and we'll find out whether he will provide the keys or not.

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

MR. LEVISON: Well, I mean, I've always maintained that all the government needs to do is contact me and set up an appointment to install that pen register. So I don't know why there has never been any confusion about my willingness to install it. I've only ever objected to the providing of those keys which secure any sensitive information going back and forth.

But my motion, and I'm not sure if it's relevant or not because it deals more with the issue of the subpoena demanding the keys and for what will be the forthcoming search warrant, would be a continuance so that I can retain counsel to address

REDACTED

that particular issue.

THE COURT: Well, I mean, there's nothing before me with that. I've issued the subpoena. Whatever happens with that, that's -- you're trying to get me to do what Mr. Trump wanted to do and to arrange this beforehand.

MR. LEVISON: Well, I don't know if I have to appear before that grand jury right now and give the keys over or face arrest. I'm not a lawyer so I don't understand the procedure.

THE COURT: I don't know either. You need to have -- it would be wise to have a lawyer.

MR. LEVISON: Okay.

THE COURT: I don't know what's going to happen. I don't know. They haven't served the warrant yet. I have no idea. Don't know what's going to happen with it. You'll just have to figure that out, and it be wise to have a lawyer to do it, I would think.

MR. LEVISON: I guess while I'm here in regards to the pen register, would it be possible to request some sort of external audit to ensure that your orders are followed to the letter in terms of the information collected and preserved?

THE COURT: No. The law provides for those things, and any other additional or extra monitoring you might want or think is appropriate will be denied, if that's what you're requesting.

MR. LEVISON: Okay. I mean, it requests that the government return to the Court records --

REDACTED

THE COURT: You need to talk to a lawyer about what the law requires for the issuance of a pen register.

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

THE COURT: The law sets out what is done in that regard. Your lawyer can fill you in if you want to know.

MR. LEVISON: I've always been willing to accept the device. I just have some concern about ensuring that it's used properly.

THE COURT: Should we continue this to some specific date to see that he complies with the pen register?

MR. TRUMP: We can, Your Honor. It's a moot issue without the encryption keys.

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

MR. TRUMP: That's a practical --

THE COURT: -- but I don't think it is a moot issue. I mean, you-all have got the right to go in and put on that pen register. He says that he will do it. That's all that I've ordered.

Now, the other business about ordering that, Judge Buchanan made an order that he's going to have to supply what you say is the encryption codes to make the information useful. I don't know. I didn't enter that order. I have trouble making that connection.

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

REDACTED

do something in front of Judge Buchanan or not.

MR. LEVISON: You see, Judge, though that I've always been willing. They just didn't feel the need to set up an appointment.

THE COURT: What do you want me to do with this case? You want me to continue it? You want me to say it's moot right now and just end it?

MR. TRUMP: No. I think we can continue it. I don't know Mr. Levison's schedule. It can be done within hours of his return to Dallas.

THE COURT: Of course he can. You want to continue it till a week from Friday?

MR. TRUMP: Or a week from today.

MR. LEVISON: I'm not available within hours of my return, but I can meet with you on Thursday.

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

MR. TRUMP: A week from Friday.

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

THE CLERK: 26th.

THE COURT: The 26th?

MR. LEVISON: Acceptable to me.

THE COURT: We'll continue it to the 26th, and that's for determining whether or not that pen register has been installed as you request.

We can make it 10 o'clock.

REDACTED

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

THE COURT: All right. Thank you.

All right. Thank you-all. We'll adjourn till tomorrow morning at 9:30.

* * *

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

REDACTED

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/

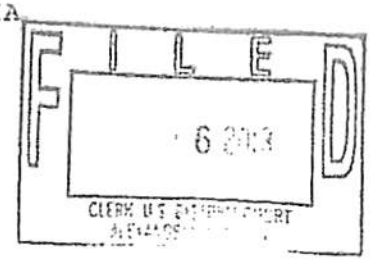
Tracy Westfall, RPR, CMRS, CCR

REDACTED

EXHIBIT 14

REDACTED

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

Criminal No. 1:13EC297

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.

/s/
Claude M. Hilton
United States District Judge

Alexandria, Virginia
July 16, 2013

REDACTED

EXHIBIT 15

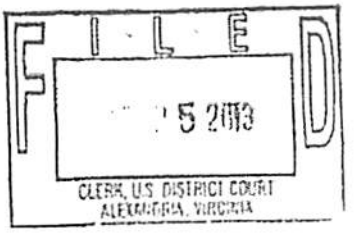
REDACTED

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 [redacted] 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

REDACTED

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 [redacted] ("Lavabit Subpoena and Warrant").

ARGUMENT

If the Government gains access to Lavabit's Master Key, it will have unlimited access to not only [redacted] ("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.

REDACTED

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.

REDACTED

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.

REDACTED

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.

REDACTED

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.

REDACTED

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

REDACTED

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

REDACTED

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

REDACTED

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:

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

Jesse R. Binnall

REDACTED

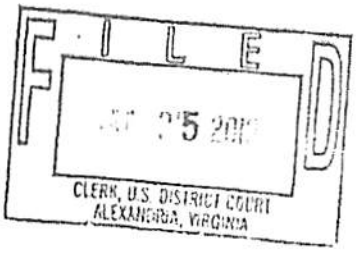
EXHIBIT 16

REDACTED

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 [redacted] 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

REDACTED

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 [redacted], 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

REDACTED

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.

REDACTED

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 [redacted]. However, Mr.

REDACTED

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

REDACTED

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 [redacted]. 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.

REDACTED

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.

REDACTED

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

REDACTED

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

REDACTED

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 [redacted] 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.

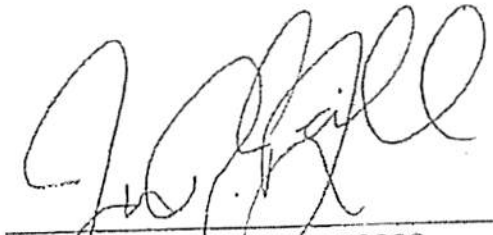
REDACTED

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

REDACTED

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:

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

Jesse R. Binnall

REDACTED

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 [redacted] 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

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 [redacted] for violations of numerous federal statutes [redacted]

A. Section 2703(d) Order

The criminal investigation has revealed that [redacted] has utilized and continues to utilize an e-mail account, [redacted] obtained through Lavabit, an electronic communications service provider. [redacted] 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 [redacted] 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 [redacted] ("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 [redacted] 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 [redacted] 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 [redacted] 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 [redacted] 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 [redacted] including encryption keys and SSL keys" and (ii)

"[a]ll information necessary to decrypt data stored in or otherwise associated with the Lavabit account [redacted]." 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 [redacted]. 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

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

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

[redacted]

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

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 [xxxxxxxx@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

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 [redacted] including encryption keys and SSL keys;
>
> b. All information necessary to decrypt data stored in or otherwise associated with the Lavabit account [redacted]

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

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 [redacted]. Moreover, the restrictions are narrowly tailored to restrict

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.

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 [redacted]". Mot. to Unseal at 4; *id.* at 6 ("the government has a legitimate interest in tracking" [redacted] 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 [redacted], along with the public, would learn of the monitoring of [redacted] 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

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 [redacted]

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

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: [redacted]
Assistant United States Attorney
United States Attorney's Office
2100 Jamieson Ave.
Alexandria, VA 22314
[redacted]
703-299-3700

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
[redacted]

[redacted]
Assistant United States Attorney
United States Attorney's Office
2100 Jamieson Ave.
Alexandria, VA 22314
[redacted]
703-299-3700

REDACTED

EXHIBIT 18

REDACTED

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 [redacted] 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.

COPY

TRANSCRIPT OF HEARING

BEFORE THE HONORABLE CLAUDE M. HILTON

UNITED STATES DISTRICT JUDGE

APPEARANCES:

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.

PROCEEDINGS

THE CLERK: *In re:* Case Nos. 1:13 EC 297, 1:13 SW 522, and Grand Jury No. 13-1.

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

THE COURT: Good morning.

MR. BINNALL: Good morning, Your Honor. Jesse Binnall on behalf of Lavabit and Mr. Levison.

THE COURT: All right.

MR. BINNALL: May it please the Court. We're before the Court today on two separate motions, a motion to quash the requirement of Lavabit to produce its encryption keys and the motion to unseal and lift the nondisclosure requirements of Mr. Levison.

Your Honor, the motion to quash in this arises because the privacy of users is at -- of Lavabit's users are at stake. We're not simply speaking of the target of this investigation. We're talking about over 400,000 individuals and entities that are users of Lavabit who use this service because they believe their communications are secure.

By handing over the keys, the encryption keys in this case, they necessarily become less secure. In this case it is true that the face of the warrant itself does limit the documents or -- and communications to be viewed and the specific metadata to be viewed to the target of the case, [redacted]

REDACTED

However, there is a lack of any sort of check or balance in order to ensure that the -- that the encrypted data of other Lavabit users remain secure. The encryption in this case doesn't protect only content. It protects login data and the other -- some of the other metadata involved in this case.

We believe that this is not the least restrictive means in order to provide the government the data that they are looking for. Specifically --

THE COURT: You have two different encryption codes, one for the logins and the messages that are transmitted. You have another code that encrypts the content of the messages, right?

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

From my understanding of the way that this works is that there is one SSL key. That SSL key is what is issue in this case, and that SSL key specifically protects the communication, the over -- the breadth of the communication itself from the user's actual computer to the server to make sure that the user is communicating with exactly who the user intends to be communicating with, the server.

And that's one of the things that SSL does. It ensures that you're talking to the right person via e-mail and there's not a so-called man in the middle who's there to take that message away.

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

REDACTED

message and interpret the message as well?

MR. BINNALL: My understanding is that it does, Your Honor, but because that's not my technical expertise, I'm not going to represent to the Court anything on that one way or another. But my understanding is there is one general key here that is at issue.

THE COURT: Well, why would you set up such? I mean, a telephone, you've got telephone numbers and --

MR. BINNALL: Correct.

THE COURT: -- those can be traced very easily without any look at the content of the message that's there. You-all could have set up something the same way.

MR. BINNALL: We could have, Your Honor. Actually, if you're to --

THE COURT: So if anybody's -- you're blaming the government for something that's overbroad, but it seems to me that your client is the one that set up the system that's designed not to protect that information, because you know that there needs to be access to calls that go back and forth to one person or another. And to say you can't do that just because you've set up a system that everybody has to -- has to be unencrypted, if there's such a word, that doesn't seem to me to be a very persuasive argument.

MR. BINNALL: I understand the Court's point, and this is the way that I understand why it's done that way.

There's different security aspects involved for people who want to protect their privacy, and there certainly is the actual content of the message themselves. That's certainly what I would concede is the highest security interest.

But there's also the security interest to make sure that they're communicating with who you want to be communicating with. That is equally of a concern for privacy issues because that is, at the end of the day, one of the things that secures the content of the message.

In this case it is true that most Internet service providers do log, is what they call it, a lot of the metadata that the government wants in this case without that necessarily being encrypted, things such as who something is going to, who it's going from, the time it's being sent, the IP address from which it is being sent.

Lavabit code is not something that you buy off the shelf. It is code that was custom made. It was custom made in order to secure privacy to the largest extent possible and to be the most secure way possible for multiple people to communicate, and so it has chosen specifically not to log that information.

Now, that is actually information that my client has offered to start logging with the particular user in this case. It is, however, something that is quite burdensome on him. It is something that would be custom code that would take between 20 to 40 hours for him to be able to produce. We believe that

is a better alternative than turning over the encryption key which can be used to get the data for all Lavabit users.

I hope that addresses the Court's concern kind of with regard to the metadata and why it is not more -- why Lavabit hasn't created an encryption system that may honestly be more within the mainstream, but this is a provider that specifically was started in order to have to protect privacy interests more than the average Internet service provider.

THE COURT: I can understand why the system was set up, but I think the government is -- government's clearly entitled to the information that they're seeking, and just because you-all have set up a system that makes that difficult, that doesn't in any way lessen the government's right to receive that information just as they would from any telephone company or any other e-mail source that could provide it easily. Whether it's -- in other words, the difficulty or the ease in obtaining the information doesn't have anything to do with whether or not the government's lawfully entitled to the information.

MR. BINNALL: It is -- and we don't disagree that the government is entitled to the information. We actually --

THE COURT: Well, how are we going to get it? I'm going to have to deny your motion to quash. It's just not overbroad. The government's asking for a very narrow, specific bit of information, and it's information that they're entitled to.

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

MR. BINNALL: Your Honor, what I would still say is the best method for them to get it is, first of all, there be some way for there to be some sort of accountability other than just relying on the government to say we're not going to go outside the scope of the warrant.

This is nothing that is, of course, personal against the government and the, you know, very professional law enforcement officers involved in this case. But quite simply, the way the Constitution is set up, it's set up in a way to ensure that there's some sort of checks and balances and accountability.

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

MR. BINNALL: Well --

THE COURT: Suggest something to me.

MR. BINNALL: I think that the least restrictive means possible here is that the government essentially pay the reasonable expenses, meaning in this case my client's extensive labor costs to be capped at a reasonable amount.

THE COURT: Has the government ever done that in one of these pen register cases?

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

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

MR. BINNALL: And Your Honor's certainly seen more of these than I have.

REDACTED

THE COURT: So would it be reasonable to start now with your client?

MR. BINNALL: I think everyone would agree that this is an unusual case. And that this case, in order to protect the privacy of 400,000-plus other users, some sort of relatively small manner in which to create a log system for this one user to give the government the metadata that they're looking for is the least restrictive mean here, and we can do that in a way that doesn't compromise the security keys.

This is actually a way that my client --

THE COURT: You want to do it in a way that the government has to trust you --

MR. BINNALL: Yes, Your Honor.

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

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

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

MR. BINNALL: Your Honor, because that's what the basis of Fourth Amendment law says is more acceptable, is that the government is the entity that you really need the checks and balances on.

Now, my --

THE COURT: I don't know that the Fourth Amendment says that. This is a criminal investigation.

MR. BINNALL: That is absolutely correct.

THE COURT: A criminal investigation, and I don't know that the Fourth Amendment says that the person being investigated here is entitled to more leeway and more rights than the government is. I don't know.

MR. BINNALL: There certainly is a balance of power there. I, of course, am not here to represent the interest of [redacted] I'm here specifically looking over my client who has sensitive data --

THE COURT: I understand. I'm trying to think of working out something. I'm not sure you're suggesting anything to me other than either you do it and the government has to trust you to give them whatever you want to give them or you have to trust the government that they're not going to go into your other files.

Is there some other route?

MR. BINNALL: I would suggest that the government -- I'm sorry -- that the Court can craft an order to say that we can -- that we should work in concert with each other in order to come up with this coding system that gives the government all of the metadata that we can give them through this logging procedure that we can install in the code, and then using that as a least restrictive means to see if that can get the government the information that they're looking for on the specific account.

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

MR. BINNALL: I mean, 20, 40 hours. So I would suggest that would probably be a week to a week and a half, Your Honor, although I would be willing to talk to my client to see if we can get that expedited.

THE COURT: To install it?

MR. BINNALL: Well, to write the code.

THE COURT: You don't have a code right at the moment. You would have to write something?

MR. BINNALL: That's correct. And the portion of the government's brief that talks about the money that he was looking for is that reasonable expense for him basically to do nothing for that period of time but write code to install in order to take the data from [redacted] and put it in a way that the government will see the logged metadata involved.

THE COURT: All right. I think I understand your position. I don't think you need to argue this motion to unseal. This is a grand jury matter and part of an ongoing criminal investigation, and any motion to unseal will be denied.

MR. BINNALL: If I could have the Court's attention just on one issue of the nondisclosure provision of this. And I understand the Court's position on this, but there is other privileged communications if the Court would be so generous as to allow me very briefly to address that issue?

There's other First Amendment considerations at issue with not necessarily just the sealing of this, but what

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

The First Amendment, of course, doesn't just cover speech and assembly, but the right to petition for a redress of grievances. We're talking about a statute here, and, honestly, a statute that is very much in the public eye and involving issues that are currently pending before Congress.

I think the way that the order currently is written, besides being --

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

MR. BINNALL: I'm talking about the sealing order and the order that prohibits Mr. Levison from disclosing any information.

Now, we don't want to disclose -- we have no intention of disclosing the target, but we would like to be able to, for instance, talk to members of the legislature and their staffs about rewriting this in a way that's --

THE COURT: No. This is an ongoing criminal investigation, and there's no leeway to disclose any information about it.

MR. BINNALL: And so at that point it will remain with only Mr. Levison and his lawyers, and we'll keep it at that.

THE COURT: Let me hear from Mr. Trump.

Is there some way we can work this out or something that I can do with an order that will help this or what?

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

you've already articulated the reason why is that anything done by Mr. Levison in terms of writing code or whatever, we have to trust Mr. Levison that we have gotten the information that we were entitled to get since June 28th. He's had every opportunity to propose solutions to come up with ways to address his concerns and he simply hasn't.

We can assure the Court that the way that this would operate, while the metadata stream would be captured by a device, the device does not download, does not store, no one looks at it. It filters everything, and at the back end of the filter, we get what we're required to get under the order.

So there's no agents looking through the 400,000 other bits of information, customers, whatever. No one looks at that, no one stores it, no one has access to it. All we're going to look at and all we're going to keep is what is called for under the pen register order, and that's all we're asking this Court to do.

THE COURT: All right. Well, I think that's reasonable. So what is this before me for this morning other than this motion to quash and unseal which I've ruled on?

MR. TRUMP: The only thing is to order the production of the encryption keys, which just --

THE COURT: Hasn't that already been done? There's a subpoena for that.

MR. TRUMP: There's a search warrant for it, the motion

REDACTED

to quash.

THE COURT: Search warrant.

MR. TRUMP: Excuse me?

THE COURT: I said subpoena, but I meant search warrant.

MR. TRUMP: We issued both, Your Honor, but Your Honor authorized the seizure of that information. And we would ask the Court to enforce that by directing Mr. Levison to turn over the encryption keys.

If counsel represents that that will occur, we can not waste any more of the Court's time. If he represents that Mr. Levison will not turn over the encryption keys, then we have to discuss what remedial action this Court can take to require compliance with that order.

THE COURT: Well, I will order the production of those -- of those keys.

Is that simply Mr. Levison or is that the corporation as well?

MR. TRUMP: That's one and the same, Your Honor.

Just so the record is clear. We understand from Mr. Levison that the encryption keys were purchased commercially. They're not somehow custom crafted by Mr. Levison. He buys them from a vendor and then they're installed.

THE COURT: Well, I will order that. If you will

present an order to me, I'll enter it later on.

MR. TRUMP: Thank you.

MR. BINNALL: Thank you, Your Honor.

As far as time frame goes, my client did ask me if the Court did order this if the Court could give him approximately five days in order to actually physically get the encryption keys here. And so it will be -- or just some sort of reasonable time frame to get the encryption keys here and in the government's hands. He did ask me to ask exactly the manner that those are to be turned over.

MR. TRUMP: Your Honor, we understand that this can be done almost instantaneously, as soon as Mr. Levison makes contact with an agent in Dallas, and we would ask that he be given 24 hours or less to comply. This has been going on for a month.

THE COURT: Yeah, I don't think 24 -- 24 hours would be reasonable. Doesn't have to do it in the next few minutes, but I would think something like this, it's not anything he has to amass or get together. It's just a matter of sending something.

So I think 24 hours would be reasonable.

MR. BINNALL: Yes. Thank you, Your Honor.

THE COURT: All right. And you'll present me an order?

MR. TRUMP: We will, Your Honor. Thank you.

THE COURT: All right. Thank you-all, and we'll adjourn until -- or stand in recess till 3 o'clock. Well,

REDACTED

recess till 9 o'clock tomorrow morning.

* * *

(Proceedings concluded at 10:25 a.m.)

CERTIFICATION

I certify, this 19th day of August 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

Tracy Westfall, RPR, CMRS, CCR

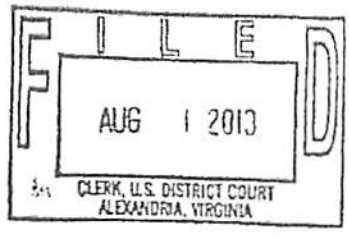
REDACTED

EXHIBIT 19

REDACTED

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 [redacted] 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

REDACTED

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.

/s/
Claude M. Hilton
United States District Judge

Alexandria, Virginia
August 1, 2013

REDACTED

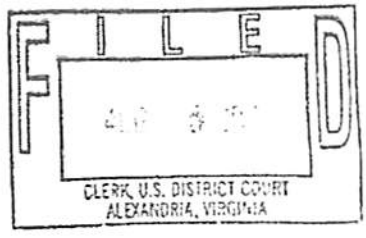
EXHIBIT 20

REDACTED

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 [redacted] THAT IS STORED AT PREMISES CONTROLLED BY LAVABIT LLC	)	No. 1:13SW522
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

REDACTED

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.

REDACTED

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.

REDACTED

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: [redacted]

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

REDACTED

Attachment A

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

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.

REDACTED

EXHIBIT 21

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

Alexandria Division

FILED
AUG 5 2013
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

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 [redacted] THAT IS STORED AT PREMISES CONTROLLED BY LAVABIT LLC	)	No. 1:13SW522
In re Grand Jury	)	No. 13-1

REDACTED

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

REDACTED

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.

/s/
Claude M. Hilton
United States District Judge

Alexandria, Virginia
August 5, 2013

REDACTED

EXHIBIT 22

REDACTED

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 [redacted] 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

REDACTED

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:

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

Jesse R. Binnall

REDACTED

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

	FILED UNDER SEAL
In re Grand Jury	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

REDACTED

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:

[redacted]

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

[redacted]

Jesse R. Binnall

REDACTED

EXHIBIT 23

REDACTED

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 IN THE MATTER OF THE SEARCH AND SEIZURE OF INFORMATION ASSOCIATED WITH [redacted] THAT IS STORED AND CONTROLLED AT PREMISES CONTROLLED BY LAVABIT LLC	**FILED UNDER SEAL** 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

REDACTED

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:

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

Jesse R. Binnall

IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

FILED
OCT - 2 2013
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

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 [redacted] THAT IS STORED AND CONTROLLED AT PREMISES CONTROLLED BY LAVABIT LLC	NO. 1:13 SW 522
IN RE GRAND JURY SUBPOENA	NO. 13-1

REDACTED

UNDER SEAL

ORDER

The United States has proposed partially unsealing records in this matter due to public disclosures made by Ladar Levison and Lavabit, LLC and for the purpose of creating a public record for Mr. Levison's appeal. The Court has considered the original sealing orders, the motions in support of the original sealing orders, the government's ex parte motion to unseal certain documents, and the prior pleadings of Mr. Levison, and hereby finds that:

(1) the government has a compelling interest in keeping certain information in the documents sealed, and the government has proposed redacted versions of the documents that minimizes the information under seal;

(2) the government's interest in keeping the redacted material sealed outweighs any public interest in disclosure; and

REDACTED

(3) having considered alternatives to the proposed redactions none will adequately protect that interest; it is hereby

ORDERED that the redacted versions of certain records filed in the above captioned matter are partially unsealed. The unsealed records are attached to this Order. To the extent any such record is covered by a non-disclosure Order issued pursuant to 18 U.S.C. § 2705(b), the non-disclosure obligation does not apply to the unsealed, redacted version of the document. The Clerk of the Court may publicly release the redacted version of any of the records attached to this Order. Any record not attached to this Order, as well as the unredacted copies of any record filed in the above-captioned matter, including the government's *ex parte*, sealed Motion to Unseal and Statement of Reasons will remain sealed until further Order of the Court.

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

Date: Oct. 2, 2013
Alexandria, VA

REDACTED

PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 13-4625

In Re: UNDER SEAL

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

v.

LAVABIT, LLC.; LADAR LEVISON,

Parties-in-Interest - Appellants.

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION OF VIRGINIA; EMPEOPLED, LLC.; ELECTRONIC FRONTIER FOUNDATION,

Amici Supporting Appellants.

No. 13-4626

In Re: GRAND JURY PROCEEDINGS

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

v.

REDACTED

LAVABIT, LLC.; LADAR LEVISON,

Parties-in-Interest - Appellants.

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION OF VIRGINIA; EMPEOPLED, LLC.; ELECTRONIC FRONTIER FOUNDATION,

Amici Supporting Appellants.

Appeals from the United States District Court for the Eastern District of Virginia, at Alexandria. Claude M. Hilton, Senior District Judge. (1:13-sw-00522-CMH-1; 1:13-dm-00022-CMH-1)

Argued: January 28, 2014 Decided: April 16, 2014

Before NIEMEYER, GREGORY, and AGEE, Circuit Judges.

Affirmed by published opinion. Judge Agee wrote the opinion, in which Judge Niemeyer and Judge Gregory joined.

ARGUED: Ian James Samuel, New York, New York, for Appellants. Andrew Peterson, OFFICE OF THE UNITED STATES ATTORNEY, Alexandria, Virginia, for Appellee. **ON BRIEF:** Jesse R. Binnall, BRONLEY & BINNALL, PLLC, Fairfax, Virginia; Marcia Hofmann, LAW OFFICE OF MARCIA HOFMANN, San Francisco, California; David Warrington, Laurin Mills, LECLAIRRYAN, Alexandria, Virginia, for Appellants. Mythili Raman, Acting Assistant Attorney General, Criminal Division, Nathan Judish, Josh Goldfoot, Benjamin Fitzpatrick, Brandon Van Grack, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C.; Dana J. Boente, Acting United States Attorney, Michael Ben'Ary, James L. Trump, OFFICE OF THE UNITED STATES ATTORNEY, Alexandria, Virginia, for Appellee. Alexander A. Abdo, Brian M. Hauss, Catherine Crump, Nathan F. Wessler, Ben Wizner, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, New York, New York; Rebecca K. Glenberg, AMERICAN CIVIL LIBERTIES UNION OF VIRGINIA FOUNDATION, INC., Richmond, Virginia, for Amici American Civil Liberties Union and ACLU of Virginia. Kurt Opsahl, Jennifer Lynch, Hanni Fakhoury, ELECTRONIC FRONTIER

REDACTED

FOUNDATION, San Francisco, California, for Amicus Electronic Frontier Foundation. Richard M. Martinez, Mahesha P. Subbaraman, ROBINS, KAPLAN, MILLER & CIRESI, L.L.P., Minneapolis, Minnesota, for Amicus Empeopled, LLC.

REDACTED

AGEE, Circuit Judge:

Lavabit LLC is a limited liability company that provided email service. Ladar Levison is the company's sole and managing member.[1]

In 2013, the United States sought to obtain certain information about a target[2] in a criminal investigation. To further that goal, the Government obtained court orders under both the Pen/Trap Statute, 18 U.S.C. §§ 3123-27, and the Stored Communications Act, 18 U.S.C. §§ 2701-12, requiring Lavabit to turn over particular information related to the target. When Lavabit and Levison failed to comply with those orders, the district court held them in contempt and imposed monetary sanctions. Lavabit and Levison now appeal the sanctions.

For the reasons below, we affirm the judgment of the district court.

---

[1] The record does not reflect the state of Lavabit's organization or registration to do business. Neither does the record contain documents that verify the ownership of Lavabit's membership interests or the identity of its managing member. The parties and the district court assumed below that Lavabit and Levison were "[o]ne and the same." (J.A. 115.) As no party has indicated otherwise, we will also assume that Levison owns all interests in Lavabit and is fully authorized to act in all matters on Lavabit's behalf.

[2] Because of the nature of the underlying criminal investigation, portions of the record, including the target's identity, are sealed.

REDACTED

I.

A.

This case concerns the encryption processes that Lavabit used while providing its email service. Encryption describes the process through which readable data, often called "plaintext," is converted into "ciphertext," an unreadable jumble of letters and numbers. Decryption describes the reverse process of changing ciphertext back into plaintext. Both processes employ mathematical algorithms involving "keys," which facilitate the change of plaintext into ciphertext and back again.

Lavabit employed two stages of encryption for its paid subscribers: storage encryption and transport encryption. Storage encryption protects emails and other data that rests on Lavabit's servers. Theoretically, no person other than the email user could access the data once it was so encrypted. By using storage encryption, Lavabit held a unique market position in the email industry, as many providers do not encrypt stored data.

Although Lavabit's use of storage encryption was novel, this case primarily concerns Lavabit's second stage of encryption, transport encryption. This more common form of encryption protects data as it moves in transit between the client and the server, creating a protected transmission channel

REDACTED

for internet communications. Transport encryption protects not just email contents, but also usernames, passwords, and other sensitive information as it moves. Without this type of encryption, internet communications move exposed en route to their destination, allowing outsiders to "listen in." Transport encryption also authenticates -- that is, it helps ensure that email clients and servers are who they say they are, which in turn prevents unauthorized parties from exploiting the data channel.

Like many online companies, Lavabit used an industry-standard protocol called SSL (short for "Secure Sockets Layer") to encrypt and decrypt its transmitted data. SSL relies on public-key or asymmetric encryption, in which two separate but related keys are used to encrypt and decrypt the protected data. One key is made public, while the other remains private. In Lavabit's process, email users would have access to Lavabit's public keys, but Lavabit would retain its protected, private keys. This technology relies on complex algorithms, but the basic idea is akin to a self-locking padlock: if Alice wants to send a secured box to Bob, she can lock the box with a padlock (the public key) and Bob will open it with his own key (the

REDACTED

private key). Anyone can lock the padlock, but only the key-holder can unlock it.[3]

The security advantage that SSL offers disappears if a third party comes to possess the private key. For example, a third party holding a private key could read the encrypted communications tied to that key as they were transmitted. In some circumstances, a third party might also use the key to decrypt past communications (although some available technologies can thwart that ability). And, with the private key in hand, the third party could impersonate the server and launch a man-in-the-middle attack.

When a private key becomes anything less than private, more than one user may be compromised. Like some other email providers, Lavabit used a single set of SSL keys for all its various subscribers for technological and financial reasons. Lavabit in particular employed only five key-pairs, one for each

---

[3] Our description oversimplifies a very complicated process that can vary depending on what cipher suites and protocols are used. In reality, a client and a server engage in an SSL "handshake" involving several different communication steps between the client and the server: initial "hellos," server authentication using an SSL certificate, potential client authentication, sending (by the client) and decryption (by the server) of a pre-master secret, generation of a master secret, generation of session keys, and formal completion of the handshake. Later communications within the same session then use the generated session keys to both encrypt and decrypt all the information transmitted during the session. It is also possible to conduct an abbreviated handshake.

REDACTED

of the mail protocols that it supported.[4] As a result, exposing one key-pair could affect all of Lavabit's estimated 400,000-plus email users.

B.

With this technical background in mind, we turn to the case before us.

1.

On June 28, 2013, the Government sought and obtained an order ("the Pen/Trap Order") from a magistrate judge authorizing the placement of a pen register and trace-and-trap device on Lavabit's system. This "pen/trap" device is intended to allow the Government to collect certain information, on a real-time basis, related to the specific investigatory target's Lavabit email account.[5] In accordance with the Pen/Trap Statute, 18 U.S.C. §§ 3121-27, the Pen/Trap Order permitted the Government to "capture all non-content dialing, routing, addressing, and

---

[4] Email protocols are the technical means by which users and servers transmit messages over a network. A given user may choose to use one of a variety of email protocols, so Lavabit was equipped to handle that choice.

[5] A pen register captures outgoing signaling and addressing information, while a trap/trace device captures that information for incoming messages. See 18 U.S.C. § 3127(3), (4). As to email, the same device often performs both functions and is frequently referred to as a pen/trap device.

REDACTED

signaling information . . . sent from or sent to" the target's account. (J.A. 10.) In other words, the Pen/Trap Order authorized the Government to collect metadata[6] relating to the target's account, but did not allow the capture of the contents of the target's emails. The Pen/Trap Order further required Lavabit to "furnish [to the Government] . . . all information, facilities, and technical assistance necessary to accomplish the installation and use of the pen/trap device unobtrusively and with minimum interference." (J.A. 11.)

On the same day that the Pen/Trap Order issued, FBI agents met with Levison, who indicated that he did not intend to comply with the order. Levison informed the agents that he could not provide the requested information because the target-user "had enabled Lavabit's encryption services," presumably referring to Lavabit's storage encryption. (J.A. 7.) But, at the same time, Levison led the Government to believe that he "had the technical capability to decrypt the [target's] information." (J.A. 6.) Nevertheless, Levison insisted that he would not exercise that

[6] Metadata, sometimes called envelope information, describes "the how, when, and where of the message." Orin S. Kerr, The Next Generation Communications Privacy Act, 162 U. Pa. L. Rev. 373, 384 (2014). It includes "IP addresses, to-from information on emails, login times, and locations." Id. The Pen/Trap Order described what specific metadata the Government was authorized to collect.

REDACTED

ability because "Lavabit did not want to 'defeat [its] own system.'" (J.A. 6.)

In view of Levison's response, the Government obtained an additional order that day compelling Lavabit to comply with the Pen/Trap Order. This "June 28 Order," again issued by a magistrate judge, instructed Lavabit to "provide the [FBI] with unencrypted data pursuant to the [Pen/Trap] Order" and reiterated that Lavabit was to provide "any information, facilities, or technical assistance . . . under the control of Lavabit . . . [that was] needed to provide the FBI with the unencrypted data." (J.A. 9.) Further, the June 28 Order put Lavabit and Levison on notice that any "[f]ailure to comply" could result in "any penalty within the power of the Court, including the possibility of criminal contempt of Court." (J.A. 9.)

2.

Over the next eleven days, the Government attempted to talk with Levison about implementing the Pen/Trap Order. Levison, however, ignored the FBI's repeated requests to confer and did not give the Government the unencrypted data that the June 28 Order required. As each day passed, the Government lost forever the ability to collect the target-related data for that day.

REDACTED

Because Lavabit refused to comply with the prior orders, the Government obtained an order to show cause from the district court on July 9. The show cause order directed both Lavabit and Levison, individually, to appear and "show cause why Lavabit LLC ha[d] failed to comply with the orders entered June 28, 2013[] in this matter and why [the] Court should not hold Mr. Levison and Lavabit LLC in contempt for its disobedience and resist[a]nce to these lawful orders." (J.A. 21.) Entry of the show cause order spurred a conference call between Levison, his counsel, and representatives from the Government on July 10. During that call, the parties discussed how the Government could install the pen/trap device, what information the device could capture, and how the Government could view and preserve that information. In addition, the Government asked whether Levison would provide the keys necessary to decrypt the target's encrypted information. Although the Government again stressed that it was permitted to collect only non-content data, neither Levison nor his counsel indicated whether Lavabit would allow the Government to install and use the pen/trap device.[7]

[7] Levison contacted the Government the day after the July 10 call to say that he would not appear at the show cause hearing unless the Government reimbursed his travel expenses. In response, the Government issued a grand jury subpoena to Levison, which permitted it to cover his expenses. That subpoena, which was later withdrawn, also required Levison to produce Lavabit's encryption keys.

REDACTED

On July 13, 2013, four days after the show cause order issued, Levison contacted the Government with his own proposal as to how he would comply with the court's orders. In particular, Levison suggested that Lavabit would itself collect the Government's requested data:

> 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 [several] non-content headers . . . from any future emails sent or received using the subject account. . . . Note that additional header fields could be captured if provided in advance of my implementation effort.

(J.A. 83.) Levison conditioned his proposal with a requirement that the Government pay him $2,000 for his services. More importantly, Levison also intended to provide the data only "at the conclusion of the 60[-]day period required by the [Pen/Trap] Order . . . [or] intermittently[,] . . . as [his] schedule allow[ed]." (J.A. 83.) If the Government wanted daily updates, Levison demanded an additional $1,500.[8]

The Government rejected Levison's proposal, explaining that it needed "real-time transmission of results." (J.A. 83.) Moreover, the Government would have no means to verify the

[8] Although the Pen/Trap Order authorized compensation for "reasonable expenses" to Lavabit (J.A. 11), neither Lavabit nor Levison ever requested compensation from the district court. Levison also did not attempt to show the Government that his proposed fees were requests for "reasonable expenses" that could be reimbursed.

REDACTED

accuracy of the information that Lavabit proposed to provide -- a concerning limit given Lavabit's apparent hostility toward the Government. Levison responded by insisting that the Pen/Trap Order did not require real-time access, but did not otherwise attempt to comply with the Pen/Trap Order or the June 28 Order.

3.

On July 16, 2013, three days after the Government received Levison's proposal and the same day as the show cause hearing, the Government obtained a seizure warrant from the district court under the Stored Communications Act ("SCA"). See 18 U.S.C. §§ 2701-12. The seizure warrant provided that Lavabit was to turn over "[a]ll information necessary to decrypt communications sent to or from [the target's] Lavabit email account . . ., including encryption keys and SSL keys." (J.A. 27.) In addition, the warrant covered "[a]ll information necessary to decrypt data stored in or otherwise associated with [the target's] Lavabit account." (J.A. 27.)

REDACTED

4.

On July 16, Levison appeared before the district court pro se,[9] on behalf of himself and Lavabit, for the show cause hearing. When asked whether he planned to comply with the Pen/Trap Order, Levison responded that he had "always agreed to the installation of the pen register device." (J.A. 42.) Nonetheless, Levison objected to turning over his private SSL encryption keys "because that would compromise all of the secure communications in and out of [his] network, including [his] own administrative traffic." (J.A. 42.) He also maintained that "[t]here was never an explicit demand [from the Government] that [he] turn over the keys." (J.A. 45.)

The district court and the parties initially discussed whether the Pen/Trap Order required Lavabit to produce its encryption keys. The district court observed that the Pen/Trap Order's "technical assistance" provision may or may not encompass the keys, but it declined to reach the issue during the show cause hearing "because [he had] issued a search warrant for that." (J.A. 43.) The Government agreed that it had sought the seizure warrant to "avoid litigating [the] issue" of whether the Pen/Trap Order reached the encryption keys (J.A. 43), but

[9] The record does not reflect why Lavabit and Levison's prior counsel was no longer representing them.

REDACTED

contended that the Pen/Trap Order and the June 28 Order "required the encryption keys to be produced" (J.A. 45).

After Levison assured the district court that he would permit the Government to install a pen/trap device on Lavabit's system, the district court did not inquire further into whether Levison would turn over his encryption keys. The district court concluded that it need not yet resolve the matter because Levison had not been served with the seizure warrant and had not been called before the grand jury (as was anticipated by the then-outstanding grand jury subpoena). The district court then scheduled another hearing for July 26 to confirm that Lavabit had fully complied.

After the show cause hearing, Lavabit did permit the Government to install a pen/trap device. But, without the encryption keys, much of the information transmitted to and from Lavabit's servers remained encrypted, indecipherable, and useless. The pen/trap device was therefore unable to identify what data within the encrypted data stream was target-related and properly collectable.

5.

Shortly before the scheduled hearing on compliance, Lavabit and Levison, now again represented by counsel, moved to quash the seizure warrant. In relevant part, their motion argued that

REDACTED

the warrant (1) amounted to an impermissible general warrant barred by the Fourth Amendment; (2) sought immaterial information; and (3) imposed an undue burden on Lavabit's business.

In response, the Government contended that the warrant merely "re-state[d] and clarif[ied] Lavabit's obligations under the Pen-Trap Act to provide that same information." (J.A. 86.) The Government noted that four different legal obligations, including the Pen/Trap Order and the June 28 Order, required Lavabit to produce the encryption keys. Lavabit's motion to quash, however, did not mention either the Pen/Trap Order or the June 28 Order.

6.

On August 1, over a month after the Pen/Trap Order first issued, the district court held its second hearing.[10] The court remarked that "[t]he difficulty or the ease in obtaining the information [didn't] have anything to do with whether or not the government's lawfully entitled to that information." (J.A. 108.) For that reason, the district court denied the motion to quash the Government's "very narrow, specific" warrant. (J.A. 108.) The court also found it reasonable that the Government

[10] Nothing in the record indicates why the hearing, originally set for July 26, 2013, was delayed to August 1.

REDACTED

would not collect all users' data, even if the encryption keys would practically enable the Government to access all that data.

The district court then entered an order (the "August 1 Order") directing Lavabit to turn over its encryption keys. The order further instructed Lavabit to provide the Government "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 [Pen/Trap Order]." (J.A. 118-19.) The August 1 Order directed Lavabit and Levison to turn over the encryption keys by 5:00 pm on August 2, 2013.

7.

Despite the unequivocal language of the August 1 Order, Lavabit dallied and did not comply. Just before the 5:00 pm August 2 deadline, for instance, Levison provided the FBI with an 11-page printout containing largely illegible characters in 4-point type, which he represented to be Lavabit's encryption keys. The Government instructed Lavabit to provide the keys in an industry-standard electronic format by the morning of August 5. Lavabit did not respond.

On August 5, nearly six weeks after the Government first obtained the Pen/Trap Order, the Government moved for sanctions against Levison and Lavabit for their continuing "failure to

REDACTED

comply with [the] Court's order entered August 1." (J.A. 120.) The Government sought penalties of $5,000 a day until Lavabit provided the encryption keys to the Government. The district court granted the motion for sanctions that day.

Two days later, Levison provided the keys to the Government. By that time, six weeks of data regarding the target had been lost.[11]

8.

Lavabit and Levison timely appealed, and we have jurisdiction under 28 U.S.C. § 1291. See United States v. Myers, 593 F.3d 338, 344 n.9 (4th Cir. 2010) ("[A] civil-contempt order may be immediately appealed by a non[-]party [to the underlying action]."); see also Buffington v. Balt. Cnty., Md., 913 F.2d 113, 133 (4th Cir. 1990) (explaining that civil contempt includes "a fine that would be payable to the court . . . when the [contemnor] can avoid paying the fine simply by performing the affirmative act required by the court's order"). We further note that the appeal presents a live controversy even

[11] After Levison provided the keys to the Government, he also shut Lavabit down entirely. In a public statement, Levison did not reveal the specific reasons behind his decision to close Lavabit. He did post, however, a statement on the Lavabit website explaining that he would not "become complicit in crimes against the American people." Lavabit, http://www.lavabit.com (last visited Mar 3, 2014).

REDACTED

though Lavabit has now complied with the underlying orders, as Lavabit and Levison still face potential assessments based on their conduct in refusing to comply with the district court's orders. See In re Grand Jury Subpoena (T-112), 597 F.3d 189, 195 (4th Cir. 2010).

II.

A.

As a party appealing from a civil contempt order, Lavabit[12] may ask us to consider "whether contempt was proper" and may challenge "the order alleged to have been violated" unless "earlier appellate review was available." United States v. Myers, 593 F.3d at 344. In the ordinary case, we review the ultimate decision as to whether the contempt was proper for abuse of discretion, the underlying legal questions de novo, In re Grand Jury Subpoena, 597 F.3d at 195, and any factual findings for clear error, Oaks of Mid City Resident Council v. Sebelius, 723 F.3d 581, 584 (5th Cir. 2013); cf. United States v. Peoples, 698 F.3d 185, 189 (4th Cir. 2012) (same as to criminal contempt). Lavabit failed, however, to raise most of

[12] For simplicity's sake, we refer only to "Lavabit" for the remainder of the opinion. That term, however, includes both Lavabit and Levison unless the context reflects otherwise.

REDACTED

its present arguments before the district court; that failure significantly alters the standard of review.

B.

In the district court, Lavabit failed to challenge the statutory authority for the Pen/Trap Order, or the order itself, in any way. Yet on appeal, Lavabit suggests that the district court's demand for the encryption keys required more assistance from it than the Pen/Trap Statute requires. Lavabit never mentioned or alluded to the Pen/Trap Statute below, much less the district court's authority to act under that statute. In fact, with the possible exception of an undue burden argument directed at the seizure warrant, Lavabit never challenged the district court's authority to act under either the Pen/Trap Statute or the SCA.

"The matter of what questions may be taken up and resolved for the first time on appeal is one left primarily to the discretion of the courts of appeals, to be exercised on the facts of individual cases." Singleton v. Wulff, 428 U.S. 106, 121 (1976). In this circuit, we exercise that discretion sparingly. Our settled rule is simple: "[a]bsent exceptional circumstances, . . . we do not consider issues raised for the first time on appeal." Robinson v. Equifax Info. Servs., LLC, 560 F.3d 235, 242 (4th Cir. 2009); see also Agra, Gill & Duffus,

REDACTED

Inc. v. Benson, 920 F.2d 1173, 1176 (4th Cir. 1990) ("We will not accept on appeal theories that were not raised in the district court except under unusual circumstances.").

When a party in a civil case fails to raise an argument in the lower court and instead raises it for the first time before us, we may reverse only if the newly raised argument establishes "fundamental error" or a denial of fundamental justice. Stewart v. Hall, 770 F.2d 1267, 1271 (4th Cir. 1985). "Fundamental error" is "more limited" than the "plain error" standard that we apply in criminal cases. Id.; accord Shcherbakovskiy v. Da Capo Al Fine, Ltd., 490 F.3d 130, 142 (2d Cir. 2007) ("To meet this [fundamental error] standard, a party must demonstrate even more than is necessary to meet the plain error standard in a criminal trial."). So, when a party in a civil case fails to meet the plain-error standard, we can say with confidence that he has not established fundamental error. See, e.g., In re Celotex Corp., 124 F.3d 619, 631 (4th Cir. 1997) (describing the criminal plain-error standard as a "minimum" standard that must be met before undertaking discretionary review of a waived argument in a civil case).[13]

[13] Two things might explain the higher standard that applies in civil cases. First, "Federal Rule of Criminal Procedure 52(b) affords federal appellate courts the discretion to correct certain forfeited errors in the criminal context," but in the civil context (excepting jury instructions), "such discretion is (Continued)

REDACTED

Thus, we may use the criminal, plain-error standard -- articulated by United States v. Olano, 507 U.S. 705, 730 (1993) -- as something of an intermediate step in a civil case. See, e.g., Brickwood Contractors, Inc. v. Datanet Eng'g, Inc., 369 F.3d 385, 396 (4th Cir. 2004) (applying Olano standard in civil case). Under that familiar standard, we cannot reverse if the party fails to establish: "(1) there is an error; (2) the error is plain; (3) the error affects substantial rights; and (4) the court determines . . . that the error seriously affects the fairness, integrity or public reputation of judicial proceedings." Celotex, 124 F.3d at 630-31. Even the lesser showing needed for "[p]lain error review is strictly circumscribed, and meeting all four prongs is difficult, as it should be." United States v. Byers, 649 F.3d 197, 213 (4th Cir. 2011) (quotation marks and alteration omitted).

We employ these rules not to trap unwary litigants, but to advance several important and "obvious" purposes. Wheatley v. Wicomico Cnty., Md., 390 F.3d 328, 335 (4th Cir. 2004). Among

---

judicially created." Celotex, 124 F.3d 619, 630 n.6 (4th Cir. 1997). As a judicial construction, it should be narrowly construed. Cf. In re ESA Envtl. Specialists, Inc., 70 F.3d 388, 394 n.5 (4th Cir. 2013) (stating that a "judicially created exception" to a rule should be "narrowly construed"). Second, plain-error review arose in the criminal context to protect the defendant's "substantial liberty interests," but "[s]uch interests normally are not at stake in civil litigation." Deppe v. Tripp, 863 F.2d 1356, 1364 (7th Cir. 1988).

REDACTED

other things, forfeiture and waiver rules offer "respect for the [integrity of the] lower court, [avoid] unfair surprise to the other party, and [acknowledge] the need for finality in litigation and conservation of judicial resources." Holly Hill Farm, 447 F.3d at 267. Our sister circuits have suggested other reasons beyond these: waiver rules ensure that the parties develop the necessary evidence below, In re Diet Drugs Prod. Liab. Litig., 706 F.3d 217, 226 (3d Cir. 2013), and "prevent parties from getting two bites at the apple by raising two distinct arguments," Fleishman v. Cont'l Cas. Co., 698 F.3d 598, 608 (7th Cir. 2012); see also HTC Corp. v. IPCom GmbH & Co., KG, 667 F.3d 1270, 1282 (Fed. Cir. 2012) (collecting cases). The Supreme Court has likewise warned us not to lightly dismiss the many interests underlying preservation requirements. See, e.g., Wood v. Milyard, 132 S. Ct. 1826, 1834 (2012) ("Due regard for the trial court's processes and time investment is also a consideration appellate courts should not overlook."); Exxon Shipping Co. v. Baker, 554 U.S. 471, 487 n.6 (2008) ("[T]he complexity of a case does not eliminate the value of waiver and forfeiture rules, which ensure that parties can determine when an issue is out of the case, and that litigation remains, to the extent possible, an orderly progression.").

Forfeiture and waiver principles apply with equal force to contempt proceedings. See, e.g., In re Gates, 600 F.3d 333, 337

REDACTED

(4th Cir. 2010) (applying plain-error standard to unpreserved claim of error in criminal contempt proceedings); United States v. Neal, 101 F.3d 993, 996 (4th Cir. 1996) (same). If anything, "[t]he axiom that an appellate court will not ordinarily consider issues raised for the first time on appeal takes on added significance in the context of contempt." In re Bianchi, 542 F.2d 98, 100 (1st Cir. 1976) (internal citation omitted). After all, "[d]enying the court of which [a party] stands in contempt the opportunity to consider the objection or remedy is in itself a contempt of [that court's] authority and an obstruction of its processes." Id. (quotation marks omitted).

C.

Lavabit argues that it preserved an appellate challenge to the Pen/Trap Order when Levison objected to turning over the encryption keys at the initial show cause hearing. We disagree.

In making his statement against turning over the encryption keys to the Government, Levison offered only a one-sentence remark: "I have only ever objected to turning over the SSL keys because that would compromise all of the secure communications in and out of my network, including my own administrative traffic." (J.A. 42.) This statement -- which we recite here verbatim -- constituted the sum total of the only objection that Lavabit ever raised to the turnover of the keys under the

REDACTED

Pen/Trap Order. We cannot refashion this vague statement of personal preference into anything remotely close to the argument that Lavabit now raises on appeal: a statutory-text-based challenge to the district court's fundamental authority under the Pen/Trap Statute. Levison's statement to the district court simply reflected his personal angst over complying with the Pen/Trap Order, not his present appellate argument that questions whether the district court possessed the authority to act at all.

Arguments raised in a trial court must be specific and in line with those raised on appeal. "To preserve an issue for appeal, an objection [or argument] must be timely and state the grounds on which it is based." Kollsman, a Div. of Sequa Corp. v. Cohen, 996 F.2d 702, 707 (4th Cir. 1993). It follows then that "an objection on one ground does not preserve objections based on different grounds." United States v. Massenburg, 564 F.3d 337, 342 n.2 (4th Cir. 2009).[14] Similarly, a party does not go far enough by raising a non-specific objection or claim.

[14] We have emphasized this point many times before. See, e.g., United States v. Zayyad, 741 F.3d 452, 459 (4th Cir. 2014) ("To preserve an argument on appeal, the [party] must object on the same basis below as he contends is error on appeal."); Laber v. Harvey, 438 F.3d 404, 429 n.24 (4th Cir. 2006) ("These are different arguments entirely, and making the one does not preserve the other."); United States v. Banisadr Bldg. Joint Venture, 65 F.3d 374, 379 (4th Cir. 1995) ("[A] theory not raised at trial cannot be raised on appeal.").

REDACTED

"[I]f a party wishes to preserve an argument for appeal, the party must press and not merely intimate the argument during the proceedings before the district court." Dallas Gas Partners, L.P. v. Prospect Energy Corp., 733 F.3d 148, 157 (5th Cir. 2013); see also United States v. Bennett, 698 F.3d 194, 199 (4th Cir. 2012) (finding defendant waived argument where his argument below was "too general to alert the district court to the specific [objection]").

In arguing that it can still pursue the issue despite its failure to raise any specific argument challenging the Pen/Trap Order below, Lavabit gives far too broad a reading to Yee v. City of Escondido, 503 U.S. 519, 534 (1992). Yee explained that, "[o]nce a federal claim is properly presented, a party can make any argument in support of that claim; parties are not limited to the precise arguments they made below." 503 U.S. at 534. We, too, have recognized our need to "consider any theory plainly encompassed by the submissions in the underlying litigation." Volvo Constr. Equip. N. Am., Inc. v. CLM Equip. Co., 386 F.3d 581, 604 (4th Cir. 2004).

Yet Lavabit neither "plainly" nor "properly" identified these issues for the district court, and a comparison between this case and Yee illustrates why. In Yee, the parties raised before the district court a Fifth Amendment takings claim premised on physical occupation. 503 U.S. at 534-35. Before

REDACTED

the Supreme Court, however, they argued that the taking occurred by regulation. Id. The difference in form there was immaterial because the appealing party asked both courts to evaluate the same fundamental question: whether the challenged acts constituted a taking. In other words, the appellant/petitioner in Yee raised two variations of the same basic argument. In contrast, the difference in the case at bar is marked and material: Lavabit never challenged the statutory validity of the Pen/Trap Order below or the court's authority to act. To the contrary, Lavabit's only point below alluded to the potential damage that compliance could cause to its chosen business model.[15]

Neither the district court nor the Government therefore had any signal from Lavabit that it contested the district court's authority under the Pen/Trap Statute to enter the Pen/Trap Order or the June 28th Order. In fact, by conceding at the August 1 hearing "that the [G]overnment [was] entitled to the [requested] information," it likely led the district court to believe exactly the opposite. (J.A. 108.) Accordingly, Lavabit failed to preserve any issue for appeal related to the Pen/Trap Statute or the district court's authority to act under it. See Nelson

[15] We might characterize this argument as some type of undue burden challenge. But, on appeal, Lavabit does not raise any undue burden argument as to the Pen/Trap Order. Instead, it limits its burden arguments to the seizure warrant.

REDACTED

v. Adams USA, Inc., 529 U.S. 460, 469 (2000) ("[T]he general rule that issues must be raised in lower courts in order to be preserved as potential grounds of decision in higher courts . . . requires that the lower court be fairly put on notice as to the substance of the issue.").

D.

Lavabit contends that, even if it failed to raise a cognizable objection to the Pen/Trap Order in the district court, then the Government and the district court induced it to forfeit its present challenges. We know of no case recognizing an "invited" or "induced" waiver exception to the traditional forfeiture and waiver principles. Lavabit has not identified any basis for such an exception, other than its subjective belief that it is now in an "unfair" position. But that is not an argument that permits us to cast aside the well-understood interests underlying our preservation requirements. Cf. Hawkins v. United States, 724 F.3d 915, 918 (7th Cir. 2013) ("Finality is an institutional value and it is tempting to subordinate such a value to the equities of the individual case. But there are dangers, especially if so vague a term as 'fairness' is to be the touchstone.").

REDACTED

In any event, we disagree with Lavabit's factual premise, as neither the Government nor the district court induced or invited Lavabit to waive anything.

The Government did not lead Lavabit to believe that the Pen/Trap Order was somehow irrelevant. To be sure, the Government focused more on the seizure warrant than the Pen/Trap Order at certain times in the proceedings. At the August 1 hearing, for example, the Government concentrated on the seizure warrant and the later-withdrawn grand jury subpoena because the motion under consideration -- Lavabit's motion to quash -- only addressed those two objects. The Government, however, never stopped contending that the Pen/Trap Order, in and of itself, also required Lavabit to turn over the encryption keys. For example, the Government specifically invoked the Pen/Trap Order in its written response to Lavabit's motion to quash by noting that "four separate legal obligations" required Lavabit to provide its encryption keys, including the Pen/Trap Order and the June 28 Order. (J.A. 86.) If Lavabit truly believed the Pen/Trap Order to be an invalid request for the encryption keys, then the Government's continuing reliance on that order should have spurred Lavabit to challenge it.

The district court's actions also put Lavabit on notice that the Pen/Trap Order implicated Lavabit's encryption keys. The June 28 Order referred to encryption, and the August 1 order

REDACTED

compelling Lavabit to turn over its keys relied upon two independent sources of authority: "the July 16, 2013 seizure warrant and the June 28, 2013 [Pen/Trap Order]." (J.A. 119 (emphasis added).) The August 1 Order, with its plain and unequivocal citation to the Pen/Trap Order, informed Lavabit that the Pen/Trap Order needed to be addressed because it was the cited authority for the turnover of the encryption keys. Even if the district court had earlier equivocated about whether the Pen/Trap Order reached Lavabit's encryption keys, those doubts were dispelled once the August 1 Order issued.[16] "When the terms of a judgment conflict with either a written or oral opinion or observation, the judgment must govern." Murdaugh Volkswagen, Inc. v. First Nat'l Bank of S.C., 741 F.2d 41, 44 (4th Cir. 1984); see also id. ("Courts must speak by orders and judgments, not by opinions, whether written or oral, or by chance observations or expressed intentions made by courts during, before or after trial, or during argument."). At an absolute minimum, if Lavabit believed that the turnover of the keys was invalid under the Pen/Trap Order, then it should have

[16] Similarly, if Lavabit believed that the district court mistakenly relied upon the Pen/Trap Order in its August 1 Order, then it should have moved the district court to revise its order. See Segars. v. Atl. Coast Line R.R. Co., 286 F.2d 767, 770 (4th Cir. 1961) (finding that party waived argument that written order did not conform with trial court's actual findings, where party did not move to revise order below).

REDACTED

acted once the district court's August 1 order issued. It did not.

E.

Lavabit tenders other reasons why we should exercise our discretion to hear its Pen/Trap Statute argument, but we find no merit in those arguments. We doubt that Lavabit's listed factors could ever justify de novo review of an argument raised for the first time on appeal in a civil case in this circuit.

Many years ago, this circuit held that, "at a minimum, the requirements of [the plain-error standard] must be satisfied before we may exercise our discretion to correct an error not raised below in a civil case." In re Celotex, 124 F.3d at 631 (emphasis added). It makes no difference then that Lavabit's Pen/Trap Statute argument presents a supposedly "pure question of law" (Reply Br. 6), or that Lavabit was unrepresented during some of the proceedings below, or that Lavabit believes this case to be one of "public concern" (Reply Br. 6).

At the outset, we do not agree that the issue is a "purely legal" one. At the very least, interpreting the Pen/Trap Statute's third-party-assistance provision would require us to consider technological questions of fact that have little to do with "pure law." But even if the question were legal, that would not alone justify our review. Though some circuits will

REDACTED

sometimes put aside the plain-error framework when a case presents this sort of question, see, e.g., Villas at Parkside Partners v. City of Farmers Branch, 726 F.3d 524, 582 n.26 (5th Cir. 2013), our precedents do not embrace that approach. To the contrary, we have taken a more structured view, recognizing that the forfeiture rule "is a salutary rule even where the ground urged for reversal is a pure question of law." Legg's Estate v. Comm'r, 114 F.2d 760, 766 (4th Cir. 1940); accord Richison v. Ernest Grp., Inc., 634 F.3d 1123, 1128-30 (10th Cir. 2011) (rejecting a party's contention that a forfeited but "purely legal" issue could be considered outside the plain-error framework).

Nor does it matter that Lavabit and Levison were unrepresented by counsel during parts of the proceedings below.[17]

[17] As a limited liability company, Lavabit likely should not have been permitted to proceed pro se at all. "It has been the law for the better part of two centuries, for example, that a corporation may appear in the federal courts only through licensed counsel. As the courts have recognized, the rationale for that rule applies equally to all artificial entities. Thus, save in a few aberrant cases, the lower courts have uniformly held that 28 U.S.C. § 1654, providing that 'parties may plead and conduct their own cases personally or by counsel,' does not allow corporations, partnerships, or associations to appear in federal court otherwise than through a licensed attorney." Rowland v. Cal. Men's Colony, Unit II Men's Advisory Council, 506 U.S. 194, 202 (1993) (footnote omitted); see also, e.g., United States v. Hagerman, 545 F.3d 579, 581-82 (7th Cir. 2008) (holding that LLCs may not proceed pro se); United States ex rel. Mergent Servs. v. Flaherty, 540 F.3d 89, 92 (2d Cir. 2008) (Continued)

"Although pro se complaints [and arguments] are to be liberally construed, the failure to first present claims to the district court generally forecloses our consideration of these matters on appeal." United States v. Ferguson, 918 F.2d 627, 630 (6th Cir. 1990); cf. Williams v. Ozmint, 716 F.3d 801, 810-11 (4th Cir. 2013) ("We long have recognized that, despite our expansive consideration of the pleadings of pro se litigants, . . . appellate courts should not permit . . . fleeting references to preserve questions on appeal."). Neither this Court nor the Supreme Court has ever "suggested that procedural rules in ordinary civil litigation should be interpreted so as to excuse mistakes by those who proceed without counsel." McNeil v. United States, 508 U.S. 106, 113 (1993). Especially given Lavabit's on-again-off-again relationship with various legal counsel, no reason exists to do so here.[18]

Finally, Lavabit proposes that we hear its challenge to the Pen/Trap Order because Lavabit views the case as a matter of "immense public concern." (Reply Br. 6.) Yet there exists a perhaps greater "public interest in bringing litigation to an

---

(explaining that lay persons cannot represent corporations, partnerships, or limited liability companies).

[18] Litigating this case did not evidently present any particular financial hardship, as Lavabit and Levison have never claimed a lack of funds as a reason for their sometimes-pro-se status.

REDACTED

end after fair opportunity has been afforded to present all issues of law and fact." United States v. Atkinson, 297 U.S. 157, 159 (1936). And exhuming forfeited arguments when they involve matters of "public concern" would present practical difficulties. For one thing, identifying cases of a "public concern" and "non-public concern" -- divorced from any other consideration -- is a tricky task governed by no objective standards. See, e.g., Tony A. Weigand, Raise or Lose: Appellate Discretion and Principled Decision-Making, 17 Suffolk J. Trial & App. Advoc. 179, 280-87 (2012) (describing vagueness and other problems with a "public importance" approach); Barry A. Miller, Sua Sponte Appellate Rulings: When Courts Deprive Litigants of an Opportunity to Be Heard, 39 San Diego L. Rev. 1253, 1306-07 (2002) ("[W]hat is an important public interest to one court will be unimportant to another. The line will be particularly difficult to draw and will often appear nakedly political."). For another thing, if an issue is of public concern, that concern is likely more reason to avoid deciding it from a less-than-fully litigated record. See, e.g., Kingman Park Civic Ass'n v. Williams, 348 F.3d 1033, 1039 (D.C. Cir. 2003) ("The issue presented, however, is of sufficient public importance and complexity to counsel strongly against deciding it in this posture."); Carducci v. Regan, 714 F.2d 171, 177 (D.C. Cir. 1983) (refusing to excuse procedural waiver where case involved

REDACTED

"important questions of far-reaching significance"). Accordingly, we decline to hear Lavabit's new arguments merely because Lavabit believes them to be important.

In sum, Lavabit's assorted reasons to exercise any discretionary review authority do not convince us to review its Pen/Trap Statute arguments de novo. If Lavabit is to succeed on its Pen/Trap Statute claim, it must at least show plain error.

III.

A.

The Pen/Trap Statute requires law enforcement authorities to obtain court orders to install and use pen registers and trap/trace devices. The requirements for these orders are less onerous than the requirements that apply to Government requests for the "content" of communications, as pen/trap devices do not collect "content" but only information associated with the transfer of that content.[19] As to internet communications, pen/trap devices collect only metadata, such as an email's "To:" and "From:" fields, the date and time of transmissions, and user login information. See 18 U.S.C. § 3127(3), (4) (forbidding pen

[19] For example, in the more historically common use of a pen/trap device on a landline telephone, the only information collected would be information such as the telephone numbers of incoming and outgoing calls.

REDACTED

registers and trap/trace devices from collecting "the contents of any communication").

The Pen/Register Statute also includes provisions requiring third parties to provide technical assistance to the Government in connection with those devices. See 18 U.S.C. §§ 3124(a), (b). Under the pen-register provision, for instance, Lavabit must provide:

> all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place.

Id. § 3124(a). Similarly, under the trap/trace provision, Lavabit must furnish:

> all additional information, facilities and technical assistance including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such installation and assistance is directed by a court order as provided in section 3123(b)(2) of this title.

Id. § 3124(b) (emphasis added).

Thus, Sections 3124(a) and (b) are similar, but not identical. The pen-register provision refers only to information "necessary to accomplish the installation," id. § 3124(a), while the trap/trace provision references information "including installation and operation," id. § 3124(b).

REDACTED

B.

Lavabit now argues that the third-party-assistance provisions found in Sections 3124(a) and (b) do not reach the SSL keys. It reads those provisions to require only enough assistance to attach the pen/trap device to Lavabit's system, not any assistance necessary to make the device operationally effective. Further, Lavabit contends that it needed to offer only enough help to make the installation unobtrusive. And it insists that Congress never could have intended to grant the Government the broad power to ask for encryption keys through the more general language found in the third-party-assistance provisions.

All these new arguments notwithstanding, Lavabit failed to make its most essential argument anywhere in its briefs or at oral argument: it never contended that the district court fundamentally or even plainly erred in relying on the Pen/Trap Statute to compel Lavabit to produce its keys. Yet Lavabit bears the burden of showing, "at a minimum," plain error. Cf. United States v. Carthorne, 726 F.3d 503, 510 (4th Cir. 2013) (noting, in criminal context, that the appealing defendant bears the burden of showing plain error); see also, e.g., Abernathy v. Wandes, 713 F.3d 538, 553 n.12 (10th Cir. 2003) (noting in civil context that the party that failed to preserve his argument bears the burden of showing plain error). And "[a] party's

failure to raise or discuss an issue in his brief is to be deemed an abandonment of that issue." Mayfield v. Nat'l Ass'n for Stock Car Auto Racing, Inc., 674 F.3d 369, 377 (4th Cir. 2012); see also IGEN Int'l, Inc. v. Roche Diagnostics GmbH, 335 F.3d 303, 308 (4th Cir. 2003) ("Failure to present or argue assignments of error in opening appellate briefs constitutes a waiver of those issues."). Taken together, these two principles carry us to one inevitable conclusion: Lavabit's "failure to argue for plain error and its application on appeal . . . surely marks the end of the road for [its] argument for reversal not first presented to the district court." Richison, 634 F.3d at 1131; see also Jackson v. Parker, 627 F.3d 634, 640 (7th Cir. 2010) (rejecting party's plain error argument where, among other things, he "ha[d] not made an attempt -- either in his briefs or at oral argument -- to show that the elements for plain error review ha[d] been satisfied").

Lavabit abandoned any argument that the district court plainly erred, much less fundamentally erred, in relying upon the Pen/Trap Order to find Lavabit in contempt. Moreover, Lavabit fails to identify any potential "denial of fundamental justice" that would justify further review. For the same reason, then, Lavabit has abandoned that argument as well.

REDACTED

C.

We reiterate that our review is circumscribed by the arguments that Lavabit raised below and in this Court. We take this narrow course because an appellate court is not a freestanding open forum for the discussion of esoteric hypothetical questions. See Swann v. Charlotte-Mecklenburg Bd. of Educ., 489 F.2d 966, 967 (4th Cir. 1974) ("[The] Court does not sit to render decisions on abstract legal propositions or advisory opinions."). Rather, we adjudicate the legal arguments actually raised. See Erilin Co. S.A. v. Johnson, 440 F.3d 648, 654 (4th Cir. 2006) (observing that our "system of justice" is one "in which the parties are obliged to present facts and legal arguments before a neutral and relatively passive decision-maker"). Our conclusion, then, must tie back to the contempt, as the actual order on appeal, and the proceedings below, as the record that constrains us.

IV.

Lavabit also raises several challenges to the seizure warrant, but we need not, should not, and do not reach those arguments. The district court's orders compelling Lavabit to turn over its encryption keys relied on two, separate independent grounds: the Pen/Trap Order and the seizure warrant. Thus, the court's later finding of contempt found that Lavabit

REDACTED

violated both the two prior orders. When two independent bases support a district court's contempt order, it is enough for us to find that one of those bases was appropriate. See Consol. Coal Co. v. Local 1702, United Mineworkers of Am., 683 F.2d 827, 831-32 (4th Cir. 1982) (declining to address second of two independent bases for contempt order where first basis was properly affirmed). This contempt-specific rule flows from the more general maxim that, "[t]o obtain reversal of a district court judgment based on multiple, independent grounds, an appellant must convince us that every stated ground for the judgment against him is incorrect." Sapuppo v. Allstate Floridian Ins. Co., 739 F.3d 678, 680 (11th Cir. 2014).

Furthermore, some of Lavabit's additional arguments implicate constitutional concerns. Those concerns provide even more reason to avoid addressing Lavabit's new arguments. "The principle of constitutional avoidance . . . requires the federal courts to avoid rendering constitutional rulings unless absolutely necessary." Norfolk S. Ry. Co. v. City of Alexandria, 608 F.3d 150, 157 (4th Cir. 2010) (citing Ashwander v. Tenn. Valley Auth., 297 U.S. 288, 347 (1936) (Brandeis, J., concurring)); see also Bell Atl. Md., Inc. v. Prince George's Cnty., Md., 212 F.3d 863, 865 (4th Cir. 2000) ("[C]ourts should avoid deciding constitutional questions unless they are essential to the disposition of a case."). So, we "will not

REDACTED

decide a constitutional question, particularly a complicated constitutional question, if another ground adequately disposes of the controversy." Strawser v. Atkins, 290 F.3d 720, 730 (4th Cir. 2002). The long-established constitutional-avoidance rule applies squarely to this case.

V.

In view of Lavabit's waiver of its appellate arguments by failing to raise them in the district court, and its failure to raise the issue of fundamental or plain error review, there is no cognizable basis upon which to challenge the Pen/Trap Order. The district court did not err, then, in finding Lavabit and Levison in contempt once they admittedly violated that order. The judgment of the district court is therefore

AFFIRMED.

FILED: April 16, 2014

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

REDACTED

No. 13-4625 (L)
(1:13-sw-00522-CMH-1)
(1:13-dm-00022-CMH-1)

In re: UNDER SEAL

UNITED STATES OF AMERICA

Plaintiff - Appellee

v.

LAVABIT, LLC.; LADAR LEVISON

Parties-in-Interest - Appellants

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION OF VIRGINIA; EMPEOPLED, LLC.; ELECTRONIC FRONTIER FOUNDATION

Amici Supporting Appellant

No. 13-4626
(1:13-dm-00022-CMH-1)
(1:13-sw-00522-CMH-1)

In re: GRAND JURY PROCEEDINGS

REDACTED

UNITED STATES OF AMERICA

Plaintiff - Appellee

v.

LAVABIT, LLC.; LADAR LEVISON

Parties-in-Interest - Appellants

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION OF VIRGINIA; EMPEOPLED, LLC.; ELECTRONIC FRONTIER FOUNDATION

Amici Supporting Appellant

J U D G M E N T

In accordance with the decision of this court, the judgment of the district court is affirmed.

This judgment shall take effect upon issuance of this court's mandate in accordance with Fed. R. App. P. 41.

/s/ PATRICIA S. CONNOR, CLERK

FILED: April 16, 2014

REDACTED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 13-4625 (L), In re: Under Seal
1:13-sw-00522-CMH-1, 1:13-dm-00022-CMH-1

NOTICE OF JUDGMENT

Judgment was entered on this date in accordance with Fed. R. App. P. 36. Please be advised of the following time periods:

PETITION FOR WRIT OF CERTIORARI: To be timely, a petition for certiorari must be filed in the United States Supreme Court within 90 days of this court's entry of judgment. The time does not run from issuance of the mandate. If a petition for panel or en banc rehearing is timely filed, the time runs from denial of that petition. Review on writ of certiorari is not a matter of right, but of judicial discretion, and will be granted only for compelling reasons. (www.supremecourtus.gov)

VOUCHERS FOR PAYMENT OF APPOINTED OR ASSIGNED COUNSEL: Vouchers are sent to counsel appointed or assigned by the court in a separate transmission at the time judgment is entered. CJA 30 vouchers are sent to counsel in capital cases. CJA 20 vouchers are sent to counsel in criminal, post-judgment, habeas, and § 2255 cases. Assigned counsel vouchers are sent to counsel in civil, civil rights, and agency cases. Vouchers should be completed and returned within 60 days of the later of entry of judgment, denial of a petition for rehearing, or the grant or denial of a petition for writ of certiorari. If counsel appointed or assigned by the court did not receive a voucher, forms and instructions are available from the court's web site, www.ca4.uscourts.gov, or from the clerk's office.

BILL OF COSTS: A party to whom costs are allowable, who desires taxation of costs, shall file a Bill of Costs within 14 calendar days of entry of judgment. (FRAP 39, Loc. R. 39(b)).

REDACTED

PETITION FOR REHEARING AND PETITION FOR REHEARING EN BANC: A petition for rehearing must be filed within 14 calendar days after entry of judgment, except that in civil cases in which the United States or its officer or agency is a party, the petition must be filed within 45 days after entry of judgment. A petition for rehearing en banc must be filed within the same time limits and in the same document as the petition for rehearing and must be clearly identified in the title. The only grounds for an extension of time to file a petition for rehearing are the death or serious illness of counsel or a family member (or of a party or family member in pro se cases) or an extraordinary circumstance wholly beyond the control of counsel or a party proceeding without counsel.

Each case number to which the petition applies must be listed on the petition to identify the cases to which the petition applies and to avoid companion cases proceeding to mandate during the pendency of a petition for rehearing in the lead case. A timely filed petition for rehearing or petition for rehearing en banc stays the mandate and tolls the running of time for filing a petition for writ of certiorari.

A petition for rehearing must contain an introduction stating that, in counsel's judgment, one or more of the following situations exist: (1) a material factual or legal matter was overlooked; (2) a change in the law occurred after submission of the case and was overlooked; (3) the opinion conflicts with a decision of the U.S. Supreme Court, this court, or another court of appeals, and the conflict was not addressed; or (4) the case involves one or more questions of exceptional importance. A petition for rehearing, with or without a petition for rehearing en banc, may not exceed 15 pages. Copies are not required unless requested by the court. (FRAP 35 & 40, Loc. R. 40(c)).

MANDATE: In original proceedings before this court, there is no mandate. Unless the court shortens or extends the time, in all other cases, the mandate issues 7 days after the expiration of the time for filing a petition for rehearing. A timely petition for rehearing, petition for rehearing en banc, or motion to stay the mandate will stay issuance of the mandate. If the petition or motion is denied, the mandate will issue 7 days later. A motion to stay the mandate will ordinarily be denied, unless the motion presents a substantial question or otherwise sets forth good or probable cause for a stay. (FRAP 41, Loc. R. 41).

REDACTED

FILED: May 8, 2014

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 13-4625 (L)
(1:13-sw-00522-CMH-1)
(1:13-dm-00022-CMH-1)

In re: UNDER SEAL

UNITED STATES OF AMERICA

Plaintiff - Appellee

v.

LAVABIT, LLC.; LADAR LEVISON

Parties-in-Interest - Appellants

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION OF VIRGINIA; EMPEOPLED, LLC.; ELECTRONIC FRONTIER FOUNDATION

Amici Supporting Appellant

REDACTED

No. 13-4626
(1:13-dm-00022-CMH-1)
(1:13-sw-00522-CMH-1)

In re: GRAND JURY PROCEEDINGS

UNITED STATES OF AMERICA

Plaintiff - Appellee

v.

LAVABIT, LLC.; LADAR LEVISON

Parties-in-Interest - Appellants

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION OF VIRGINIA; EMPEOPLED, LLC.; ELECTRONIC FRONTIER FOUNDATION

Amici Supporting Appellant

M A N D A T E

The judgment of this court, entered April 16, 2014, takes effect today.

This constitutes the formal mandate of this court issued pursuant to Rule 41(a) of the Federal Rules of Appellate Procedure.

/s/Patricia S. Connor, Clerk

REDACTED FILED

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

2015 DEC 11 P 3:30

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

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**
IN THE MATTER OF THE SEARCH AND SEIZURE OF INFORMATION ASSOCIATED WITH [redacted] THAT IS STORED AND CONTROLLED AT PREMISES CONTROLLED BY LAVABIT LLC	No. 1:13SW522
In re Grand Jury	No. 13-1

MOTION TO UNSEAL RECORDS AND VACATED NON-DISCLOSURE ORDERS AND MEMORANDUM OF LAW IN SUPPORT OF MOTION

Lavabit, LLC ("Lavabit") and Mr. Ladar Levison ("Mr. Levison") (collectively "Movants") move this Court to fully unseal records and vacate non-disclosure orders that are over two years old. While these records have been partially unsealed, Mr. Levison is still prevented from disclosing the target of the subpoenas, specifically the named individual and the email address(es) searched, and the non-disclosure orders are still in effect. The account holder at issue is [redacted].

REDACTED

The Facts

Mr. Levison, a resident of Texas, formed Lavabit in 2004 as a secure and encrypted email service provider. At its peak, Lavabit provided email service to approximately 410,000 users worldwide.

In the spring of 2013, the United States launched a criminal investigation into the activities of [redacted]. As part of this investigation, the federal government (1) subpoenaed Lavabit for billing and subscriber information related to [redacted] email account with Lavabit, (2) obtained an order requiring Lavabit to install a pen-trap device to intercept all electronic communications involving [redacted] account, and (3) issued a search warrant to Lavabit for all information necessary to access their encrypted data, Exhibit A through C. The latter involved a request for Lavabit's private encryption keys[1] which would allow the government to access the plain-text for all the traffic traversing the Lavabit network, including emails and customer passwords. After exhausting its options in court, and subsequently finding itself the subject of a contempt charge, Lavabit surrendered its private encryption key. Concurrently Mr. Levison chose to suspend the operation of Lavabit's email service.

[1] Lavabit employed an industry standard to provide transport layer security ("TLS"), sometimes called a secure socket layer ("SSL"), to ensure the privacy and security of communications between Lavabit and its users. TLS makes use of two "keys", one public, and the other private, which work together to verify the identity of Lavabit's servers and setup an encrypted network connection. This encryption protects the data sent between the server and a user's email client, or web browser.

REDACTED

[redacted] the subject of the investigation, which led to the government demanding unfettered access to the private communications for all of Lavabit's customers, [redacted] foreseeable future.

On [redacted] the United States filed a criminal complaint against [redacted] in the District Court for the Eastern District of Virginia, charging him with [redacted] Act. Though initially filed under seal, the United States unsealed the complaint [redacted]

Lavabit and Mr. Levison challenged the validity and constitutionality of the search warrant and orders. This Court denied Lavabit's request to quash the search warrant and grand jury subpoena, and twice denied the movants' motion to unseal court records. Lavabit appealed the decision to the Fourth Circuit Court of Appeals, and while the appeal was pending, this Court partially unsealed portions of the record, Exhibit D. The Court continued to redact the target's name and email addresses.

REDACTED

Two years later, a lifetime, in today's media cycle, the search warrant, grand jury subpoena, and other pleadings and orders remain partially sealed, and Mr. Levison is still subject to the non-disclosure orders of June 10, 28 and July 16, 2013 ("the non-disclosure orders"). As such, he may *never* disclose [redacted] email accounts are what spawned the government's request and led to the subsequent legal proceedings.

I. THE NON-DISCLOSURE ORDERS ARE INVALID BECAUSE THEY VIOLATE MR. LEVISON'S FIRST AMENDMENT RIGHT TO FREE SPEECH

All three non-disclosure orders were issued by the Court pursuant to the Stored Communications Act ("SCA") at 18 U.S.C. § 2705(b). These orders constitute notice preclusion authorized by the SCA. Such an order is "a type of gag order." *In re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 879-80 (S.D. Tex. 2008). A restriction on speech survives judicial scrutiny only "if it 'is necessary to serve a compelling state interest and is narrowly drawn to achieve that end.'" *IOTA XI Chapter of Sigma Chi Fraternity v. George Mason Univ.*, 993 F.2d 386, 394 (4th Cir. 1993) (Murnaghan, J., concurring) (quoting *Simon & Schuster, Inc. v. New York Crime Victims Board*, 502 U.S. 105, 118 (1991)).

By requesting a gag order, the government's purpose is to preclude Mr. Levison from speaking about an entire topic, namely, the object of the search and seizure warrants to Lavabit and the underlying criminal investigation of [redacted] *See Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989) (opining

that "the government's purpose is the controlling consideration. A regulation that serves purposes unrelated to the content of expression is deemed neutral..."). In fact, the non-disclosure orders prohibit Mr. Levison from disclosing the link between the federal government's, now public, investigation of [redacted], and his email accounts with Lavabit. Such restrictions qualify as content-based regulation of speech.[2] *See Bartnicki v. Vopper*, 532 U.S. 514, 526 (2001). The Supreme Court has held that content-based regulation of speech is "presumptively invalid." *R.A.V. v. City of St. Paul*, 505 U.S. 377, 381-82 (1992) (noting that the "First Amendment generally prevents government from proscribing speech, or even expressive conduct, because of disapproval of the ideas expressed.").

Within First Amendment jurisprudence, government action in the form of an administrative or judicial order forbidding certain speech has been described as a "prior restraint." *Alexander v. United States*, 509 U.S. 544, 550 (1993) (quoting M. Nimmer, *Nimmer on Freedom of Speech* § 4.03, p. 4–14 (1984)) ("The term 'prior restraint' is used 'to describe administrative and judicial orders forbidding certain communications when issued in advance of the time that such communications are to occur.'"). "Temporary restraining

---

[2] Although the government action at issue in this case does not involve a law in the ordinary sense, the Supreme Court has held that a government investigation is nonetheless subject to First Amendment scrutiny. *Watkins v. United States*, 354 U.S. 178, 197 (1957) ("While it is true that there is no statute to be reviewed, and that an investigation is not a law, nevertheless an investigation is part of law-making. It is justified solely as an adjunct to the legislative process. The First Amendment may be invoked against infringement of the protected freedoms by law or by lawmaking").

orders and permanent injunctions—i.e., court orders that actually forbid speech activities—are classic examples of prior restraints." Nimmer, at 4-16. *See, e.g., New York Times Co. v. United States*, 403 U.S. 713, 714 (1971) (per curiam) (striking down injunctions barring the New York Times and Washington Post from publishing excerpts from the "Pentagon Papers"). The gag order issued in this case is also a speech restrictive injunction and, thus, an example of prior restraint that is "constitutionally disfavored in this nation nearly to the point of extinction." *In re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 882 (S.D. Tex. 2008) (quoting *United States v. Brown*, 250 F.3d 907, 915 (5th Cir. 2001)).

Moreover, "[a]ny prior restraint on expression [arrives in court] with a 'heavy presumption' against its constitutional validity," with the government having the burden of proving that such a restriction is justified. *See Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 558-59 (1976) (quoting *Organization for a Better Austin v. Keefe*, 402 U.S. 415, 418-20 (1971). In *Nebraska Press*, the Supreme Court noted that a prior restraint is an immediate and irreversible sanction because it "freezes" speech, which is "the most serious and the least tolerable infringement on First Amendment rights." *Id.* at 559. Applying this reasoning, other courts have held that the Stored Communications Act and federal pen/trap statute do not permit gag orders of indefinite duration. *See, e.g. In re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 895 (S.D. Tex. 2008) (holding that a 180-day period is "most reasonable as a default setting for sealing and non-disclosure" orders); *Matter*

of Grand Jury Subpoena for: [Redacted]@yahoo.com, No. 5:15-CR-90096-PSG, 2015 WL 604267, at *1 (N.D. Cal. Feb. 5, 2015) (denying government's motion to gag Yahoo!, pursuant to 18 U.S.C. 2705(b), "until further order of the court")).

In this case, the federal government has prohibited Mr. Levison from disclosing the target in the Lavabit proceedings, and freely discussing the underlying investigation concerning [redacted]. This specific prohibition of an entire topic is a content-based restriction of Mr. Levison's speech under the First Amendment. For such a gag order to be constitutional, it must be narrowly tailored to serve a compelling government interest. *IOTA XI*, 993 F.2d at 394. In addition, the gag order in this case applies to Mr. Levison "until otherwise authorized" by the Court. Indeed, even in the very serious context of national security, the Supreme Court has found that a prior restraint is permissible only if the speech will "surely result in direct, immediate, and irreparable harm to our Nation or its people." *New York Times v. United States* (*Pentagon Papers*), 403 U.S. 713, 730 (1971) (per curium) (Stewart & White, JJ., concurring).[3]

---

[3] The Stewart-White concurrence is the holding of the case because, of the six Justices who concurred in the judgment, Justices Stewart and White concurred on the narrowest grounds. *See Marks v. United States*, 430 U.S. 188, 193 (1977) ("[w]hen a fragmented Court decides a case and no single rationale explaining the result enjoys the assent of five Justices, the holding of the Court may be viewed as that position taken by those Members who concurred in the judgment on the narrowest grounds") (internal quotation omitted); accord, *City of Lakewood v. Plain Dealer Publ'g Co.*, 486 U.S. 750, 764 n. 9 (1988). In *New York Times v. United States*, Justices Black and Douglas would clearly have refused to enjoin publication even if the Government had

18 U.S.C. § 2705(b) authorizes notice preclusion, 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).

First, there is no evidence or insinuation in the government's filings to suggest that a disclosure by Mr. Levison or Lavabit of the sealed information would somehow endanger somebody's life or safety. Second, there is no risk that [redacted] will flee from prosecution, as a result of such disclosure, because he has already fled from prosecution. Third, there is no risk that [redacted] will tamper with his Lavabit accounts or otherwise alter his behavior if Mr. Levison were to disclose the information under seal because Lavabit is no

---

met Stewart's test. *See, e.g., New York Times*, 403 U.S. at 730 (Black, J., concurring) (Black & Douglas, JJ., concurring) (no evidence that disclosure would cause "direct, immediate, and irreparable damage...") Justice Brennan also would likely have held more broadly. "[T]he First Amendment tolerates absolutely no prior judicial restraints of the press predicated upon surmise or conjecture that untoward consequences may result. . . . [O]nly governmental . . . proof that publication must inevitably, directly, and immediately cause the occurrence of an event kindred to imperiling the safety of a transport already at sea can support even the issuance of an interim restraining order. In no event may mere conclusions be sufficient: for if the Executive Branch seeks judicial aid in preventing publication, it must inevitably submit the basis upon which that aid is sought to scrutiny by the judiciary." *Id.* at 725-27 (Brennan, J., concurring).

REDACTED

longer operating its email service. This makes it impossible for [redacted] to access, let alone tamper with his accounts. The investigation is already two years old, so any compelling interest the government may have had, as defined in 18 U.S.C. § 2705(b), has long since expired. Without a compelling government interest, the continued suppression of Mr. Levison's speech cannot pass constitutional muster. *See United States v. O'Brien*, 391 U.S. 367, 376-77 (1968).[4]

"[The Government] must demonstrate that the recited harms are real, not merely conjectural, and that the regulation will in fact alleviate these harms in a direct and material way." *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 664 (1994) (internal quotation marks and citations omitted). The government cannot meet this burden here because it cannot demonstrate that any actual harm will occur as a result of fully unsealing these documents. Indeed, its recited harms are now two years old, and any urgency to their claims, if it existed, has vanished with the passage of time. Even if the government had a compelling interest when the gag order was issued, the passage of time has tipped the scales and now favors the movant's First Amendment right to free speech. The Southern District of Texas recognized as much when it held that a 180-day period is "reasonable as a default setting for sealing and non-

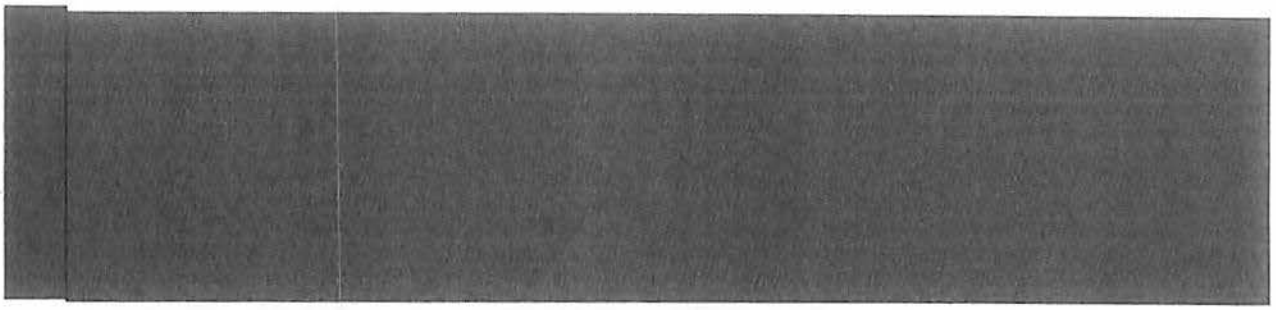
[4] In *United States v. O'Brien*, the Supreme Court held that the government may regulate speech if: (1) the regulation is within the government's constitutional power; (2) the regulation furthers an important or substantial government interest; (3) the governmental interest is unrelated to the suppression of free expression; and (4) the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.

disclosure" orders. *In re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 895 (S.D. Tex. 2008). The gag order in this case, which prohibits Mr. Levison from speaking freely, has already eclipsed this "reasonable" period, as cited in *In re Sealing & Non-Disclosure*, by a factor of five.

Fourth, the gag order does not relate to other witnesses; it simply prohibits Mr. Levison from confirming that the [redacted] investigation led to the Lavabit proceedings, and discussing the investigation in its proper context. Despite [redacted] was the target, Mr. Levison has been required to tread carefully, and discuss them separately; an act of verbal contortion. He is perpetually in fear that a misstep will result in this Court holding him in contempt for violating its gag orders.

Fifth, there is no risk that a disclosure would jeopardize the investigation because the government's investigation of [redacted] is public knowledge. The [redacted] that the government actually sought to search Lavabit for evidence related to [redacted]. The government's prohibitions on speech do not protect the secrecy of, or otherwise imperil a government investigation, but rather prevent Mr. Levison from fully engaging in the public discourse involving [redacted], and the subsequent government investigation. *See In re A 18 U.S.C. § 2703 Order Issued to Google on June 10, 2011*, 2012 U.S. Dist. LEXIS 25770, at *2 (E.D. Va. 2012) (Jones, Jr., J.) (stating that the government's concern of confidentiality is moot, because the use of the government's tools in this matter have been widely publicized). *See,*

REDACTED



The gag orders preventing the release of information that this motion seeks to unseal are not narrowly tailored or designed to achieve a specific and important purpose. Instead, they are a prior restraint on Mr. Levison's speech, of unlimited duration, which have greatly affected Mr. Levison and Lavabit, while doing nothing to further the government investigation. As such, the gag orders represent a violation of the movants First Amendment's right to free speech.

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

Despite the lack of statutory authority, the 2703(d) search warrant and other related documents, along with the 2705(b) Order, remain partially under seal and the subject of non-disclosure, or "gag" orders. 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) (citing *Stone v. University of Md. Med. Sys. Corp.*, 855 F.2d 178, 180 (4th Cir. 1988)); *see Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 580 (1980) (the press and public have a First Amendment right to attend a criminal trial); *Press-Enterprise Co. v. Superior*

[5] The title of this article was chosen by [redacted] not Mr. Levison.

REDACTED

Court, 478 U.S. 1, 2 (1986) (the public has a First Amendment right of access to preliminary hearing and transcript).

a. The Common Law Right Of Access Attaches To The Search Warrant

"For a right of access to exist under the First Amendment or common law, the document must be a 'judicial record.'" *United States v. Applebaum*, 707 F.3d 283, 290 (4th Cir. 2013) (citing *Baltimore Sun Co. v. Goetz*, 886 F.2d 60, 63–64 (4th Cir. 1989)). In *Applebaum*, the Fourth Circuit held that § 2703(d) orders and subsequent orders issued by the court are judicial records because they are judicially created. *Id.* at 290. The Court also held that the common law presumption of access attaches to such documents. *Id.* at 291. In this case, the 2705(b) Order was issued pursuant to 18 U.S.C. § 2703(d), therefore it is a judicial record and a presumption of access attaches to it.

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. *Id.* at 293. Under the common law, the decision to seal or grant access to warrant papers lies within the discretion of the judicial officer who issued the warrant. *Media Gen. Operations, Inc. v. Buchanan*, 417 F.3d 424, 429 (4th Cir. 2005). If a judicial officer determines that full public access is not appropriate, he or she "must consider alternatives to sealing the documents," including granting some public access or releasing a redacted version of the documents. *Id.* (quoting *Baltimore Sun*, 886 F.2d at 66). In the present case, now, two years later, there is no longer a need for such

partial redactions because the government's investigation of [redacted] is well known and widely publicized.

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

There are no provisions in the SCA to seal orders or other documents. By 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. §§ 3123. 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). Thus, Congress has specifically provided for sealing provisions when it has so desired. Additionally, where Congress includes particular language in one section of a statute but omits it in another, it is assumed that Congress acted intentionally. *Keene Corp. v. United States*, 508 U.S. 200, 208 (1993). Therefore, Congress has provided no statutory basis for sealing an application or order under the SCA that would overcome the common law right to access.

c. The First Amendment Right To Petition The Government For Redress Of Grievances Demands Public Access

The Petition Clause of the First Amendment protects the public's right to petition the government for redress of grievances. *Borough of Duryea, Pa. v. Guarnieri*, 131 S.Ct. 2488, 2494 (2011). "It was not by accident or coincidence that the rights to freedom in speech and press were coupled in a single guaranty with the rights... to petition for redress of grievances." *Id.* at 2495 (quoting *Thomas v. Collins*, 323 U.S. 516, 530 (1945)). Free speech allows the

REDACTED

public to state its grievances and the right to petition ensures that it can communicate those grievances to the government. *Id.* The non-disclosure orders in this case deny Mr. Levison these fundamental rights and forbid him from discussing portions of his experience with the world freely and without fear.

The non-disclosure orders prohibit Mr. Levison from disclosing any information regarding the target of the underlying investigation. A representative democracy depends upon the people being afforded the opportunity to air their grievances to their representatives. Mr. Levison has been and continues to be denied the ability to petition the government for redress. These orders are the hallmark of an extremely unsettling expansion of government power that jeopardizes the privacy of thousands to aid the investigation of an individual. Even a partial concealment of these proceedings undermines Mr. Levison right to voice his political opinions and threatens the free formation of opinions on a matter of public import.

Conclusion

For the foregoing reasons, Lavabit and Ladar Levison respectfully move this Court to lift fully the non-disclosure orders issued to Mr. Levison.

LAVABIT LLC
By Counsel

Jesse R. Binnall, VSB# 79292
Louise T. Gitcheva, VSB# 86200
Harvey & Binnall, PLLC
717 King Street, Suite 300

REDACTED

Alexandria, Virginia 22314
(703) 888-1943 Telephone
(703) 888-1930- Facsimile
jbinnall@harveybinnall.com
lgitcheva@harveybinnall.com
Counsel for Lavabit LLC

REDACTED

Certificate of Service

I certify that on this 11th day of December, 2015, this Motion to Unseal Records and Vacate Non-Disclosure Orders and Memorandum of Law in Support of Motion was hand delivered to the person at the addresses listed below:

James L. Trump
Senior Litigation Counsel
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314
jim.trump@usdoj.gov

Jesse R. Binnall

REDACTED

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
IN THE MATTER OF THE SEARCH AND SEIZURE OF INFORMATION ASSOCIATED WITH [redacted] THAT IS STORED AT PREMISES CONTROLLED BY LAVABIT LLC	)	No. 1:13SW522
In re Grand Jury	)	No. 13-1

SEALING ORDER

Upon the motion of the United States, good cause having been shown, it is hereby ORDERED that:

The grand jury subpoena issued to Ladar Norman Levison for an appearance on July 16, 2013, shall be placed under seal until further order of this Court;

It is further ORDERED that the government shall serve Mr. Levison with a copy of this Order along with a copy of its motion to seal; and

It is further ORDERED that the government's motion to seal the grand jury subpoena and this Order shall be placed under seal.

Claude M. Hilton
United States District Judge

Alexandria, Virginia
July 16, 2013

REDACTED

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 INSTALLATION AND USE OF A PEN REGISTER/TRAP AND TRACE DEVICE ON AN ELECTRONIC MAIL ACCOUNT	)	(Under Seal) 1:13 EC 297

ORDER

This matter having come before the Court pursuant to an Application under 18 U.S.C. § 3122, by Andrew Peterson, 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 [redacted] that is registered to subscriber [redacted] 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. §§ [redacted] by [redacted].

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

EXHIBIT B

REDACTED

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

REDACTED

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

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

JUN 10 201
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

REDACTED

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

EXHIBIT
C

REDACTED

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

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

ATTACHMENT A

REDACTED

I. The Account(s)

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

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).

REDACTED

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

IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

FILED
OCT - 2 2013
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

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 [redacted] THAT IS STORED AND CONTROLLED AT PREMISES CONTROLLED BY LAVABIT LLC	NO. 1:13 SW 522
IN RE GRAND JURY SUBPOENA	NO. 13-1

REDACTED

UNDER SEAL

ORDER

The United States has proposed partially unsealing records in this matter due to public disclosures made by Ladar Levison and Lavabit, LLC and for the purpose of creating a public record for Mr. Levison's appeal. The Court has considered the original sealing orders, the motions in support of the original sealing orders, the government's ex parte motion to unseal certain documents, and the prior pleadings of Mr. Levison, and hereby finds that:

(1) the government has a compelling interest in keeping certain information in the documents sealed, and the government has proposed redacted versions of the documents that minimizes the information under seal;

(2) the government's interest in keeping the redacted material sealed outweighs any public interest in disclosure; and

EXHIBIT
D

REDACTED

(3) having considered alternatives to the proposed redactions none will adequately protect that interest; it is hereby

ORDERED that the redacted versions of certain records filed in the above captioned matter are partially unsealed. The unsealed records are attached to this Order. To the extent any such record is covered by a non-disclosure Order issued pursuant to 18 U.S.C. § 2705(b), the non-disclosure obligation does not apply to the unsealed, redacted version of the document. The Clerk of the Court may publicly release the redacted version of any of the records attached to this Order. Any record not attached to this Order, as well as the unredacted copies of any record filed in the above-captioned matter, including the government's *ex parte*, sealed Motion to Unseal and Statement of Reasons will remain sealed until further Order of the Court.

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

Date: Oct. 2, 2013
Alexandria, VA

REDACTED

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

FILED
DEC 16 2015
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

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	UNDER SEAL Criminal No. 1:13EC297
IN THE MATTER OF THE SEARCH AND SEIZURE OF INFORMATION ASSOCIATED WITH [redacted] THAT IS STORED AND CONTROLLED AT PREMISES CONTROLLED BY LAVABIT, LLC.	Criminal No. 1:13SW522
IN RE: GRAND JURY	Criminal No. 1:13-1

ORDER

This matter comes before the Court on Lavabit, LLC and Mr. Ladar Levinson's ("Movants") Motion to Unseal Records and Vacate Non-Disclosure Orders. It is hereby

ORDERED that the Government shall have until January 6, 2016 to file a response to the Movants' Motion.

Claude M. Hilton
CLAUDE M. HILTON
UNITED STATES DISTRCT JUDGE

Alexandria, Virginia
December 16, 2015

REDACTED

FILED

2016 JAN -7 A 9:45

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

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	)	No. 1:13EC297
IN THE MATTER OF THE SEARCH AND SEIZURE OF INFORMATION ASSOCIATED WITH [**REDACTED**] THAT IS STORED AT PREMISES CONTROLLED BY LAVABIT LLC	)	No. 1:13SW522
In re Grand Jury	)	No. 13-1

RESPONSE OF THE UNITED STATES TO MOTION TO UNSEAL RECORDS AND VACATE NON-DISCLOSURE ORDERS

Lavabit LLC and Ladar Levison have moved this Court for an order authorizing the public disclosure of all information currently under seal in the referenced dockets. The United States opposes Lavabit's motion and asks that the Court instead enter the attached Protective Order.

The history of these proceedings is well-documented. *See In re Under Seal*, 749 F.3d 276, 279 (4th Cir. 2014). And while this Court's sealing and non-disclosure orders remain in effect, the only information not publicly disclosed is the identity of the target of the investigation and that person's email address. *See In re Under Seal*, Fourth Circuit Appeal 13-4625, Joint Appendix Volume I, Docket Entry 27, filed October 10, 10, 2013. The government opposes the

REDACTED

public disclosure of the identity of the target of the investigation and the target's email address, as such disclosure would reveal a matter occurring before the grand jury, which is prohibited under Rule 6(e)(2) of the Federal Rules of Criminal Procedure. Lavabit, on the other hand, seeks an order requiring the government to reveal that information so that Ladar Levison can "freely discuss the underlying investigation" involving this one subscriber.

The question before this Court is whether the information at issue, the identity of a target of a grand jury investigation, which is contained in pleadings and orders under both the Pen/Trap Statute, 18 U.S.C. §§ 3123–27, and the Stored Communications Act, 18 U.S.C. §§ 2701–12, is subject to a public right of access under the First Amendment and/or common law. The First Amendment analysis is frequently called the "experience and logic" test. Courts ask (1) whether the place and process have historically been open to the press and general public, and (2) whether public access plays a significant positive role in the functioning of the particular process in question. *See Baltimore Sun v. Goetz*, 886 F.2d 60, 64 (4th Cir. 1989), quoting *Press Enterprises Co. v. Superior Court*, 478 U.S. 1, 8-1-)1988). The common law right of access, on the other hand, involves a balancing of interests whereby a court must consider whether the public's right to access is outweighed by a significant countervailing interest in continued sealing. *See Under Seal v. Under Seal*, 326 F.3d 479, 486 (4th Cir. 2003).

The information Lavabit wants to unseal (Lavabit's subscriber and the subscriber's email address) is revealed in the un-redacted pleadings and orders that are a part of the pre-indictment investigation of the case. *See Application of the United States of America for an Order Pursuant to 18 U.S.C. Section 2703(d)*, 707 F.3d 283, 292 and 295 (4th Cir. 2013) (finding that §2703(d) orders, pen registers, and wiretaps are pre-indictment investigative matters akin to grand jury

REDACTED

investigations). As noted above, the government is barred by Rule 6(e)(2) of the Federal Rules of Criminal Procedure from disclosing publicly the identity of a target of a grand jury investigation, an investigation that is not closed but ongoing.

In this context, the Fourth Circuit has said that public access does not play a significant role in the functioning of investigations involving §2703(d) orders, and there is, accordingly, no First Amendment right to access them. *Id.* at 292, quoting *In re Sealed Case*, 199 F.3d 522, 526 (D.C.Cir. 2000). The Fourth Circuit reasoned:

> Section 2703(d) proceedings can be likened to grand jury proceedings. In fact, they are a step removed from grand jury proceedings, and are perhaps even more sacrosanct. Proceedings for the issuance of § 2703(d) orders are also like proceedings for the issuance of search warrants, which we have noted are not open. *See Goetz*, 886 F.2d at 64 (observing that the Supreme Court has twice "recognized that proceedings for the issuance of search warrants are not open"). Because secrecy is necessary for the proper functioning of the criminal investigations at this § 2703(d) phase, openness will frustrate the government's operations. Because § 2703(d) orders and proceedings fail the logic prong, we hold that there is no First Amendment right to access them.

707 F.3d at 292 (footnote omitted).

As to whether there is a common law right of access to the identity of Lavabit's subscriber, Lavabit explains very little about the public's interest in this matter other than to say that Lavabit has been precluded from "freely discussing the underlying investigation." To the contrary, Lavabit can – and has – discussed the underlying investigation publicly in the context of its appeal to Fourth Circuit, resulting in a lengthy published opinion. In addition, a cursory internet search reveals that Ladar Levison has spoken out publicly on numerous other occasions about the case, his appeal, and internet privacy and encrypted email topics generally. Whether the government should be able to compel Lavabit – or any other service provider – to turn over unencrypted email account information for users of encrypted email service is certainly an issue

REDACTED

that can be debated and discussed in public forums without identifying a specific subscriber. Indeed, if Ladar Levison is to be believed (based on what he has said in a number of articles and videotaped interviews), he fought the government's demands on principle for all of his encrypted email customers. Revealing the name of the particular subscriber at issue in this case does not change the nature of the dialogue in which Levison plans to engage. Moreover, whether or not this is a high-profile investigation does not justify public access to the target's identity and should play no role in the Court's analysis. *Id.* at 293-94.

The government concedes that Lavabit should be able to notify its subscriber of the existence of the proposed orders and underlying pleadings in this case. The subscriber, of course, much like the grand jury witness, is under no obligation of secrecy with regard to any of the underlying sealed information.

The United States proposes that the Court enter the attached Protective Order. The protective order would allow Lavabit to notify its subscriber and would give the public access to all of the pleadings and orders in these several dockets with only the identity of the target and the target's email account information redacted from the public record. The proposed order would

REDACTED

also require the government to move to unseal the protected information promptly once the grand jury investigation is completed.

Respectfully submitted,

Dana J. Boente
United States Attorney

By: /s/

James L. Trump
Assistant United States Attorney
2100 Jamieson Avenue
Alexandria, Virginia 22314
Phone: 703-299-3700
Email: jim.trump@usdoj.gov

REDACTED

CERTIFICATE OF SERVICE

I hereby certify that on the 6th day of January, 2016, I electronically filed the foregoing *Response of the United States to Motion to Unseal Records and Vacate Non-Disclosure Orders* with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to the following:

Jesse R. Binnall
Harvey & Binnall, PLLC
717 King street, suite 300
Alexandria, Virginia 22314
jbinnall@harveybinnall.com

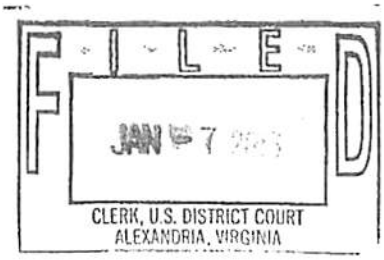
By: /s/
James L. Trump
Assistant United States Attorney
2100 Jamieson Avenue
Alexandria, Virginia 22314
(703) 299-3726
jim.trump@usdoj.gov

REDACTED

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	)	No. 1:13EC297
IN THE MATTER OF THE SEARCH AND SEIZURE OF INFORMATION ASSOCIATED WITH [REDACTED] THAT IS STORED AT PREMISES CONTROLLED BY LAVABIT LLC	)	No. 1:13SW522
In re Grand Jury	)	No. 13-1

PROTECTIVE ORDER

Lavabit LLC and Ladar Levison have moved this Court for an order directing the unsealing of all information in these proceedings. The United States opposes this motion. Based on the reasons set forth in the government's response, good cause having been shown,

It is hereby ORDERED that the Motion to Unseal Records and Vacate Non-Disclosure Orders is denied;

It is further ORDERED that Lavabit LLC or Ladar Levison may disclose to its subscriber the nature of these proceedings and the underlying un-redacted pleadings and orders;

It is further ORDERED that the United States shall file on the public docket copies of all of the previously filed pleadings, transcripts, and orders with redactions for only the identity of the subscriber and the subscriber's email address; and

REDACTED

It is further ORDERED that the United States shall, upon completion of the grand jury investigation, promptly move to unseal any information remaining under seal in these matters.

Entered in Alexandria, Virginia, this 7th day of January, 2016.

Claude M. Hilton
Senior United States District Judge

REDACTED

FILED

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 [redacted] 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

REDACTED

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

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

REDACTED

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 [redacted] for violations of numerous federal statutes, including 18 U.S.C. § [redacted] 18 U.S.C. § [redacted] and 18 U.S.C. § [redacted] On [redacted] a criminal complaint was filed charging [redacted] with these offenses. ([redacted] remains a fugitive.

REDACTED

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 or about June 8, 2013, a grand jury subpoena was served on Lavabit for billing and subscriber information for Lavabit e-mail account. Lavabit provided that information, which showed that the subject e-mail account is registered to 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

REDACTED

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.*

REDACTED

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.

REDACTED

On July 13, 2013, Mr. Levison sent an e-mail to Assistant United States Attorney Andrew Peterson 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 Peterson 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 [redacted] including encryption keys and SSL keys" and (ii)

REDACTED

"[a]ll information necessary to decrypt data stored in or otherwise associated with the Lavabit account [redacted] 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 [redacted] 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

REDACTED

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

REDACTED

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

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

REDACTED

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

REDACTED

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

REDACTED

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 [redacted] including encryption keys and SSL keys;
>
> b. All information necessary to decrypt data stored in or otherwise associated with the Lavabit account [redacted]

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

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.

REDACTED

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 of [redacted] Moreover, the restrictions are narrowly tailored to restrict

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.

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 [redacted]". Mot. to Unseal at 4; *id.* at 6 ("the government has a legitimate interest in tracking" [redacted] 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 [redacted] along with the public, would learn of the monitoring of [redacted] 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

REDACTED

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 [redacted]

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

REDACTED

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.

REDACTED

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: _____

Andrew Peterson
Assistant United States Attorney
United States Attorney's Office
2100 Jamieson Ave.
Alexandria, VA 22314
Andy.peterson@usdoj.gov
703-299-3700

REDACTED

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
jbinnall@bbllawonline.com

Andrew Peterson
Assistant United States Attorney
United States Attorney's Office
2100 Jamieson Ave.
Alexandria, VA 22314
Andy.peterson@usdoj.gov
703-299-3700

REDACTED

U.S. District Court
Eastern District of Virginia - (Alexandria)
CRIMINAL DOCKET FOR CASE #: 1:13-sw-00522-CMH-1 *SEALED*
Internal Use Only

Case title: USA v. In Re: Information Associated with [redacted]

Date Filed: 07/16/2013
Date Terminated: 03/24/2015

Assigned to: District Judge Claude M. Hilton

Appeals court case number: 13-4625

Defendant (1)

In Re: Information Associated with [redacted]

TERMINATED: 03/24/2015

Pending Counts	**Disposition**
None	

Highest Offense Level (Opening)

None

Terminated Counts	**Disposition**
None	

Highest Offense Level (Terminated)

None

Complaints	**Disposition**
None	

Interested Party

Ladar Levinson
TERMINATED: 03/24/2015
doing business as
Lavabit LLC
TERMINATED: 03/24/2015

represented by **Jesse R. Binnall**
Harvey & Binnall PLLC
717 King Street
Suite 300
Alexandria, VA 22314
703-888-1943
Fax: 703-888-1930

REDACTED

Email: jbinnall@harveybinnall.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED
Designation: Retained

Plaintiff

USA

represented by **James L. Trump**
United States Attorney's Office
2100 Jamieson Ave
Alexandria, VA 22314
(703)299-3700
Email: jim.trump@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Michael Ben'Ary
US Attorney's Office (Alexandria-NA)
2100 Jamieson Avenue
Alexandria, VA 22314
NA
703-299-3700
Email: michael.ben'ary2@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
07/16/2013	1	Application and Affidavit for a Search Warrant as to In Re: Information Associated with [redacted] Signed by District Judge Claude M. Hilton on 7/16/13. (krob,) (Entered: 08/16/2013)
07/16/2013	2	Search Warrant Issued in case as to In Re: Information Associated with [redacted] (krob,) (Entered: 08/16/2013)
07/16/2013	3	MOTION to Seal Case by USA as to In Re: Information Associated with [redacted] (krob,) (Entered: 08/16/2013)
07/16/2013	4	ORDER granting 3 Motion to Seal Case as to In Re: Information Associated with [redacted] (1). Signed by District Judge Claude M. Hilton on 7/16/13. (krob,) (Entered: 08/16/2013)
07/16/2013	5	APPLICATION for Order Commanding Lavabit not to Notify any Person of the Existence of SWby USA as to In Re: Information Associated with [redacted] (krob,) Modified on 8/16/2013 (krob,). (Entered: 08/16/2013)
07/16/2013	6	ORDER granting 5 APPLICATION for Order Commanding Lavabit not to Notify any Person of the Existence of SW by USA as to In Re:

REDACTED

		Information Associated with [redacted]. Signed by District Judge Claude M. Hilton on 7/16/13. (krob,) (Entered: 08/16/2013)
07/25/2013	7	WAIVER of Personal Appearance by Ladar Levinson as to In Re: Information Associated with [redacted] (krob,) (Entered: 08/16/2013)
07/25/2013	8	MOTION 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 by In Re: Information Associated with [redacted] (krob,) (Entered: 08/16/2013)
07/25/2013	9	MOTION to Quash Subpoena ans Search Warrant by In Re: Information Associated with [redacted] (krob,) (Entered: 08/16/2013)
08/01/2013	10	ORDER denying 8 Motion to Unseal Case as to In Re: Information Associated with [redacted] (1); denying 9 Motion to Quash as to In Re: Information Associated with [redacted] (1). Signed by District Judge Claude M. Hilton on 8/1/13. (krob,) (Entered: 08/16/2013)
08/01/2013	11	Minute Entry: for proceedings held before District Judge Claude M. Hilton: Motion Hearing as to In Re: Information Associated with [redacted] held on 8/1/2013. Lavabit's Motion to Quash - Denied, Mr. Levison Ordered to turn over the encryption keys. Respondent's request for 5 days to do so Denied, Respondant given 24 hours. Lavabit's Motion to Unseal - Denied. (Court Reporter: Westfall) (tarm). (Entered: 08/16/2013)
08/05/2013	12	MOTION for Sanctions by USA as to In Re: Information Associated with [redacted] (krob,) (Entered: 08/16/2013)
08/05/2013	13	ORDER granting 12 Motion for Sanctions; 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;and 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 as to In Re: Information Associated with [redacted] (1). Signed by District Judge Claude M. Hilton on 8/5/13. (krob,) (Entered: 08/16/2013)
08/15/2013	14	NOTICE OF APPEAL by Ladar Levinson as to In Re: Information Associated with [redacted] as to 13 Order on Motion for Sanctions 10 Order on Motion to Unseal Case and Order on Motion to

REDACTED

		Quash. Filing fee $ 455. (Attachments: # 1 Receipt)(krob,) (Main Document 14 replaced on 8/16/2013) (krob,). (Entered: 08/16/2013)
08/16/2013	15	Transmission of Notice of Appeal to 4CCA as to In Re: Information Associated with [redacted] to US Court of Appeals re 14 Notice of Appeal, (All case opening forms, plus the transcript guidelines, may be obtained from the Fourth Circuit's website at www.ca4.uscourts.gov) (krob,) (Entered: 08/16/2013)
08/21/2013	16	UNDER SEAL Transcript of Proceedings from 8/1/2013 before District Judge Claude M. Hilton. (rban,) (Entered: 08/21/2013)
08/29/2013	17	USCA Case Number 13-4625. Case Manager: RJ Warren for 14 Notice of Appeal filed by Ladar Levinson. (krob,) (Entered: 08/29/2013)
08/29/2013	18	ORDER of USCA (certified copy) consolidating Case No. 13-4625 and Case No. 13-4626. Entry of appearance forms and disclosure statements filed by counsel and parties to the lead case are deemed filed in the secondary case as to In Re: Information Associated with [redacted] (krob,) (Entered: 08/29/2013)
09/20/2013	19	UNDER SEAL EX PARTE MOTION by USA as to In Re: Information Associated with [redacted] (Attachments: # 1 Exhibit 1, # 2 Exhibit 2, # 3 Exhibit 3, # 4 Exhibit 4, # 5 Exhibit 5, # 6 Exhibit 6, # 7 Exhibit 7, # 8 Exhibit 8, # 9 Exhibit 9, # 10 Exhibit 10, # 11 Exhibit 11, # 12 Exhibit 12, # 13 Exhibit 13, # 14 Exhibit 14, # 15 Exhibit 15, # 16 Exhibit 16, # 17 Exhibit 17, # 18 Exhibit 18, # 19 Exhibit 19, # 20 Exhibit 20, # 21 Exhibit 21, # 22 Exhibit 22, # 23 Exhibit 23, # 24 Exhibit 24, # 25 Exhibit 25, # 26 Exhibit 26)(rban,) (Entered: 10/02/2013)
10/02/2013	20	Sealed Order re 19 UNDER SEAL EX PARTE MOTION by USA as to In Re: Information Associated with [redacted]. Signed by District Judge Claude M. Hilton on 10/2/2013. (Attachments: # 1 Exhibit 1, # 2 Exhibit 2, # 3 Exhibit 3, # 4 Exhibit 4, # 5 Exhibit 5, # 6 Exhibit 6, # 7 Exhibit 7, # 8 Exhibit 8, # 9 Exhibit 9, # 10 Exhibit 10, # 11 Exhibit 11, # 12 Exhibit 12, # 13 Exhibit 13, # 14 Exhibit 14, # 15 Exhibit 15, # 16 Exhibit 16, # 17 Exhibit 17, # 18 Exhibit 18, # 19 Exhibit 19, # 20 Exhibit 20, # 21 Exhibit 21, # 22 Exhibit 22, # 23 Exhibit 23) (rban,) (Entered: 10/02/2013)
10/02/2013	21	Redacted version of 20 Sealed Order. (rban,) (Entered: 10/02/2013)
10/02/2013		(Court only) ***Motions terminated as to In Re: Information Associated with [redacted]: 19 MOTION filed by USA. (rban,) (Entered: 10/02/2013)
04/16/2014	22	PUBLISHED OPINION of the USCA, decided 4/16/2014, re 14 Notice of Appeal as to 13 Order on Motion for Sanctions and 10 Order on Motion to Unseal Case and Order on Motion to Quash, Affirmed. (rban,) (Entered: 04/16/2014)
04/16/2014	23	JUDGMENT of the USCA re 14 Notice of Appeal. In accordance with the

REDACTED

		decision of this court, the judgment of the district court is affirmed. This judgment shall take effect upon issuance of this court's mandate in accordance with FRAP 41. (rban,) (Entered: 04/16/2014)
05/08/2014	24	USCA Mandate re 14 Notice of Appeal. The judgment of this court, entered April 16, 2014, takes effect today. This constitutes the formal mandate of this court issued pursuant to Rule 41(a) of the Federal Rules of Appellate Procedure. (nhall) (Entered: 05/12/2014)
03/24/2015		(Court only) ***Terminated defendant In Re: Information Associated with [redacted] and Ladar Levinson, pending deadlines, and motions. (rban,) (Entered: 03/24/2015)
12/14/2015	25	MOTION to Unseal Case by Lavabit, LLC and Mr Ladar Levinson as to In Re: Information Associated with [redacted]. (krob,) (Entered: 12/15/2015)
12/16/2015	26	ORDER to Respond re 25 MOTION to Unseal Case filed by Ladar Levinson. ORDERED that the Government shall have until January 6, 2016 to file a response to the Movants' Motion as to In Re: Information Associated with [redacted] Signed by District Judge Claude M. Hilton on 12/16/2015. (c/s)(lbru,) Modified on 12/17/2015 (lbru,). (Entered: 12/17/2015)
01/07/2016	27	Reply to Motion by USA as to In Re: Information Associated with [redacted] re 25 MOTION to Unseal Case (krob,) (Entered: 01/07/2016)
01/07/2016	28	Protective Order as to In Re: Information Associated with [redacted] Signed by District Judge Claude M. Hilton on 1/7/16. (c/s) (krob,) (Entered: 01/07/2016)