

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.

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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

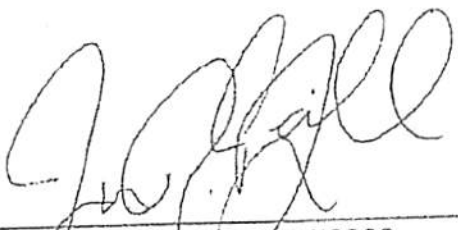
¹ See Dan Roberts, *NSA Snooping: Obama Under Pressure as Senator Denounces 'Act of Treason'*, The Guardian, June 10, 2013, <http://www.guardian.co.uk/world/2013/jun/10/obama-pressured-explain-nsa-surveillance>.

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

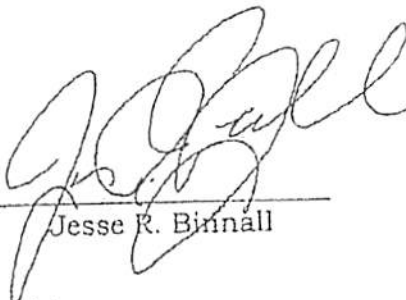


Jesse R. Binnall, VSB# 79292
Bronley & Binnall, PLLC
10387 Main Street, Suite 201
Fairfax, Virginia 22030
(703) 229-0335 Telephone
(703) 537-0780 Facsimile
jbinnall@bblawonline.com
Counsel for Lavabit LLC

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

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

NO. 1:13 SW 522

████████████████████
THAT IS STORED AND CONTROLLED
AT PREMISES CONTROLLED BY
LAVABIT LLC

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]

[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]

[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 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
LAWFUL 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 [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

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." *Halg 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:

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

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

EXHIBIT 18

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

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

NO. 1:13 EC 297

COPY

IN THE MATTER OF THE SEARCH
AND SEIZURE OF INFORMATION
ASSOCIATED WITH

NO. 1:13 SW 522

██████████ THAT
IS STORED AND CONTROLLED AT
PREMISES CONTROLLED BY
LAVABIT, LLC

IN RE GRAND JURY SUBPOENA

NO. 13-1

UNDER SEAL

Alexandria, Virginia
August 1, 2013
10:00 a.m.

TRANSCRIPT OF HEARING

BEFORE THE HONORABLE CLAUDE M. HILTON

UNITED STATES DISTRICT JUDGE

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.

UNDER SEAL

2

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]

UNDER SEAL

3

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

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

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

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

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

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

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

UNDER SEAL

4

1 message and interpret the message as well?

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

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

9 MR. BINNALL: Correct.

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

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

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

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

UNDER SEAL

5

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

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

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

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

21 Now, that is actually information that my client has
22 offered to start logging with the particular user in this case.
23 It is, however, something that is quite burdensome on him. It
24 is something that would be custom code that would take between
25 20 to 40 hours for him to be able to produce. We believe that

UNDER SEAL

6

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

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

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

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

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

UNDER SEAL

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

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

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

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

14 MR. BINNALL: Well --

15 THE COURT: Suggest something to me.

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

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

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

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

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

UNDER SEAL

8

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

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

10 This is actually a way that my client --

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

13 MR. BINNALL: Yes, Your Honor.

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

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

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

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

22 Now, my --

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

25 MR. BINNALL: That is absolutely correct.

UNDER SEAL

9

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

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

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

15 Is there some other route?

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

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

UNDER SEAL

10

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

5 THE COURT: To install it?

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

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

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

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

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

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

180
UNDER SEAL

11

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

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

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

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

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

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

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

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

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

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

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

UNDER SEAL

12

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

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

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

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

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

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

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

UNDER SEAL

13

1 to quash.

2 THE COURT: Search warrant.

3 MR. TRUMP: Excuse me?

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

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

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

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

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

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

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

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

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

2 MR. TRUMP: Thank you.

3 MR. BINNALL: Thank you, Your Honor.

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

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

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

20 So I think 24 hours would be reasonable.

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

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

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

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

184
UNDER SEAL

15

1 recess till 9 o'clock tomorrow morning.

2 * * *

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

4

5

6

7

8

9

CERTIFICATION

10

11 I certify, this 19th day of August 2013, that the
12 foregoing is a correct transcript from the record of proceedings
13 in the above-entitled matter to the best of my ability.

14

15

16

17

18

19

20

21

22

23

24

25

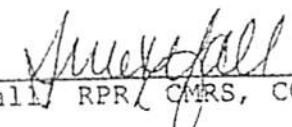
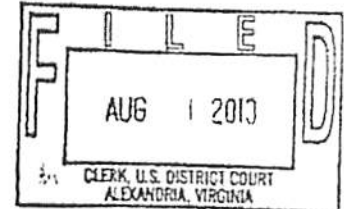
/s/ 
Tracy Westfall, RPR, CMRS, CCR

EXHIBIT 19

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

Alexandria Division

IN THE MATTER OF THE) UNDER SEAL
APPLICATION OF THE UNITED)
STATES OF AMERICA FOR AN ORDER) No. 1:13EC297
AUTHORIZING THE USE OF A PEN)
REGISTER/TRAP AND TRACE DEVICE)
ON AN ELECTRONIC MAIL ACCOUNT)
)
IN THE MATTER OF THE SEARCH AND)
SEIZURE OF INFORMATION)
ASSOCIATED WITH) No. 1:13SW522
[REDACTED] THAT IS)
STORED AT PREMISES CONTROLLED)
BY LAVABIT LLC)
)
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 Levinson shall provide the government with the encryption keys and any other "information, facilities, and technical assistance necessary to accomplish the installation and use of the pen/trap

device" as required by the July 16, 2013 seizure warrant and the June 28, 2013 pen register order.

It is further ORDERED that this Order shall remain under seal until further order of this

Court.

/s/
Claude M. Hilton
United States District Judge

Alexandria, Virginia
August 1, 2013

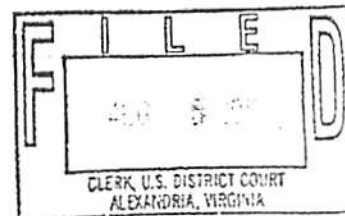
EXHIBIT 20

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

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



MOTION FOR SANCTIONS

The United States, through the undersigned counsel, pursuant to Title 18, United States Code, Section 401, hereby moves for the issuance of an order imposing sanctions on Lavabit LLC and Ladar Levison, its owner and operator, for Lavabit's failure to comply with this Court's order entered August 1, 2013. In support of this motion, the United States represents:

1. At the hearing on August 1, 2013, this Court directed Lavabit to provide the government with the encryption keys necessary for the operation of a pen register/trap and trace order entered June 28, 2013. Lavabit was ordered to provide those keys by 5 p.m. on August 2, 2013. See Order Denying Motions entered August 2, 2013.
2. At approximately 1:30 p.m. CDT on August 2, 2013, Mr. Levison gave the FBI a printout of what he represented to be the encryption keys needed to operate the pen register. This

printout, in what appears to be 4-point type, consists of 11 pages of largely illegible characters. See Attachment A. (The attachment was created by scanning the document provided by Mr. Levison; the original document was described by the Dallas FBI agents as slightly clearer than the scanned copy but nevertheless illegible.) Moreover, each of the five encryption keys contains 512 individual characters – or a total of 2560 characters. To make use of these keys, the FBI would have to manually input all 2560 characters, and one incorrect keystroke in this laborious process would render the FBI collection system incapable of collecting decrypted data.

3. At approximately 3:30 p.m. EDT (2:30 p.m. CDT), the undersigned AUSA contacted counsel for Lavabit LLC and Mr. Levison and informed him that the hard copy format for receipt of the encryption keys was unworkable and that the government would need the keys produced in electronic format. Counsel responded by email at 6:50 p.m. EDT stating that Mr. Levison “thinks” he can have an electronic version of the keys produced by Monday, August 5, 2013.

4. On August 4, 2013, the undersigned AUSA sent an e-mail to counsel for Lavabit LLC and Mr. Levison stating that we expect to receive an electronic version of the encryption keys by 10:00 a.m. CDT on Monday, August 5, 2013. The e-mail indicated that we expect the keys to be produced in PEM format, an industry standard file format for digitally representing SSL keys. See Attachment B. The e-mail further stated that the preferred medium for receipt of these keys would be a CD hand-delivered to the Dallas office of the FBI (with which Mr. Levison is familiar). The undersigned AUSA informed counsel for Lavabit LLC and Mr. Levison that the government would seek an order imposing sanctions if we did not receive the encryption keys in electronic format by Monday morning.

5. The government did not receive the electronic keys as requested. The undersigned AUSA spoke with counsel for Lavabit and Mr. Levison at approximately 10:00 a.m. this morning, and he stated that Mr. Levison might be able to produce the keys in electronic format by 5 p.m. on August 5, 2013. The undersigned AUSA told counsel that was not acceptable given that it should take Mr. Levison 5 to 10 minutes to put the keys onto a CD in PEM format. The undersigned AUSA told counsel that if there was some reason why it cannot be accomplished sooner, to let him know by 11:00 a.m. this morning. The government has not received an answer from counsel.

6. The government therefore moves the Court to impose sanctions on Lavabit LLC and Mr. Levison in the amount of \$5000 per day beginning at noon (EDT) on August 5, 2013, and continuing each day in the same amount until Lavabit LLC and Mr. Levison comply with this Court's orders.

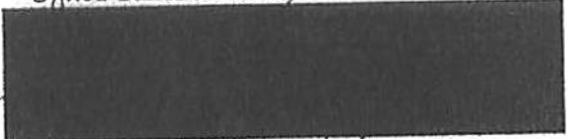
7. As noted, Attachment A to this motion is a copy of the printout provided by Mr. Levison on August 2, 2013. Attachment B is a more detailed explanation of how these encryption keys can be given to the FBI in an electronic format. Attachment C to this motion is a proposed order.

8. A copy of this motion, filed under seal, was delivered by email to counsel for Lavabit LLC on August 5, 2013.

Respectfully submitted,

Neil H. MacBride
United States Attorney

By:



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

Attachment A

[illegible]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
84

[The following text is extremely faint and largely illegible due to extreme blurring and low contrast. It appears to be a multi-paragraph document, possibly a letter or report, containing several lines of text per page. The visible fragments suggest a discussion of various topics, but no specific details can be reliably transcribed.]

[illegible]

The document contains several pages of handwritten text, likely from a ledger or account book. The handwriting is cursive and somewhat faded. The text appears to be organized into columns, possibly representing dates, descriptions, and monetary amounts. There are some legible fragments such as "Jan 1st", "Feb 1st", "Mar 1st", etc., suggesting a chronological record. The overall quality of the scan is poor, with significant noise and artifacts.

[illegible]

[The page contains extremely faint, illegible text, likely bleed-through from the reverse side of the document.]

1000
 1001
 1002
 1003
 1004
 1005
 1006
 1007
 1008
 1009
 1010
 1011
 1012
 1013
 1014
 1015
 1016
 1017
 1018
 1019
 1020
 1021
 1022
 1023
 1024
 1025
 1026
 1027
 1028
 1029
 1030
 1031
 1032
 1033
 1034
 1035
 1036
 1037
 1038
 1039
 1040
 1041
 1042
 1043
 1044
 1045
 1046
 1047
 1048
 1049
 1050
 1051
 1052
 1053
 1054
 1055
 1056
 1057
 1058
 1059
 1060
 1061
 1062
 1063
 1064
 1065
 1066
 1067
 1068
 1069
 1070
 1071
 1072
 1073
 1074
 1075
 1076
 1077
 1078
 1079
 1080
 1081
 1082
 1083
 1084
 1085
 1086
 1087
 1088
 1089
 1090
 1091
 1092
 1093
 1094
 1095
 1096
 1097
 1098
 1099
 1100
 1101
 1102
 1103
 1104
 1105
 1106
 1107
 1108
 1109
 1110
 1111
 1112
 1113
 1114
 1115
 1116
 1117
 1118
 1119
 1120
 1121
 1122
 1123
 1124
 1125
 1126
 1127
 1128
 1129
 1130
 1131
 1132
 1133
 1134
 1135
 1136
 1137
 1138
 1139
 1140
 1141
 1142
 1143
 1144
 1145
 1146
 1147
 1148
 1149
 1150
 1151
 1152
 1153
 1154
 1155
 1156
 1157
 1158
 1159
 1160
 1161
 1162
 1163
 1164
 1165
 1166
 1167
 1168
 1169
 1170
 1171
 1172
 1173
 1174
 1175
 1176
 1177
 1178
 1179
 1180
 1181
 1182
 1183
 1184
 1185
 1186
 1187
 1188
 1189
 1190
 1191
 1192
 1193
 1194
 1195
 1196
 1197
 1198
 1199
 1200
 1201
 1202
 1203
 1204
 1205
 1206
 1207
 1208
 1209
 1210
 1211
 1212
 1213
 1214
 1215
 1216
 1217
 1218
 1219
 1220
 1221
 1222
 1223
 1224
 1225
 1226
 1227
 1228
 1229
 1230
 1231
 1232
 1233
 1234
 1235
 1236
 1237
 1238
 1239
 1240
 1241
 1242
 1243
 1244
 1245
 1246
 1247
 1248
 1249
 1250
 1251
 1252
 1253
 1254
 1255
 1256
 1257
 1258
 1259
 1260
 1261
 1262
 1263
 1264
 1265
 1266
 1267
 1268
 1269
 1270
 1271
 1272
 1273
 1274
 1275
 1276
 1277
 1278
 1279
 1280
 1281
 1282
 1283
 1284
 1285
 1286
 1287
 1288
 1289
 1290
 1291
 1292
 1293
 1294
 1295
 1296
 1297
 1298
 1299
 1300
 1301
 1302
 1303
 1304
 1305
 1306
 1307
 1308
 1309
 1310
 1311
 1312
 1313
 1314
 1315
 1316
 1317
 1318
 1319
 1320
 1321
 1322
 1323
 1324
 1325
 1326
 1327
 1328
 1329
 1330
 1331
 1332
 1333
 1334
 1335
 1336
 1337
 1338
 1339
 1340
 1341
 1342
 1343
 1344
 1345
 1346
 1347
 1348
 1349
 1350
 1351
 1352
 1353
 1354
 1355
 1356
 1357
 1358
 1359
 1360
 1361
 1362
 1363
 1364
 1365
 1366
 1367
 1368
 1369
 1370
 1371
 1372
 1373
 1374
 1375
 1376
 1377
 1378
 1379
 1380
 1381
 1382
 1383
 1384
 1385
 1386
 1387
 1388
 1389
 1390
 1391
 1392
 1393
 1394
 1395
 1396
 1397
 1398
 1399
 1400
 1401
 1402
 1403
 1404
 1405
 1406
 1407
 1408
 1409
 1410
 1411
 1412
 1413
 1414
 1415
 1416
 1417
 1418
 1419
 1420
 1421
 1422
 1423
 1424
 1425
 1426
 1427
 1428
 1429
 1430
 1431
 1432
 1433
 1434
 1435
 1436
 1437
 1438
 1439
 1440
 1441
 1442
 1443
 1444
 1445
 1446
 1447
 1448
 1449
 1450
 1451
 1452
 1453
 1454