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

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 [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." *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