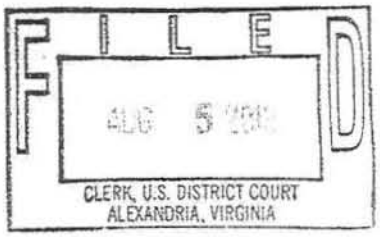
IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division



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

MOTION FOR SANCTIONS

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

1. At the hearing on August 1, 2013, this Court directed Lavabit to provide the government with the encryption keys necessary for the operation of a pen register/trap and trace order entered June 28, 2013. Lavabit was ordered to provide those keys by 5 p.m. on August 2, 2013. *See* Order Denying Motions entered August 2, 2013.

2. At approximately 1:30 p.m. CDT on August 2, 2013, Mr. Levison gave the FBI a printout of what he represented to be the encryption keys needed to operate the pen register. This

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.

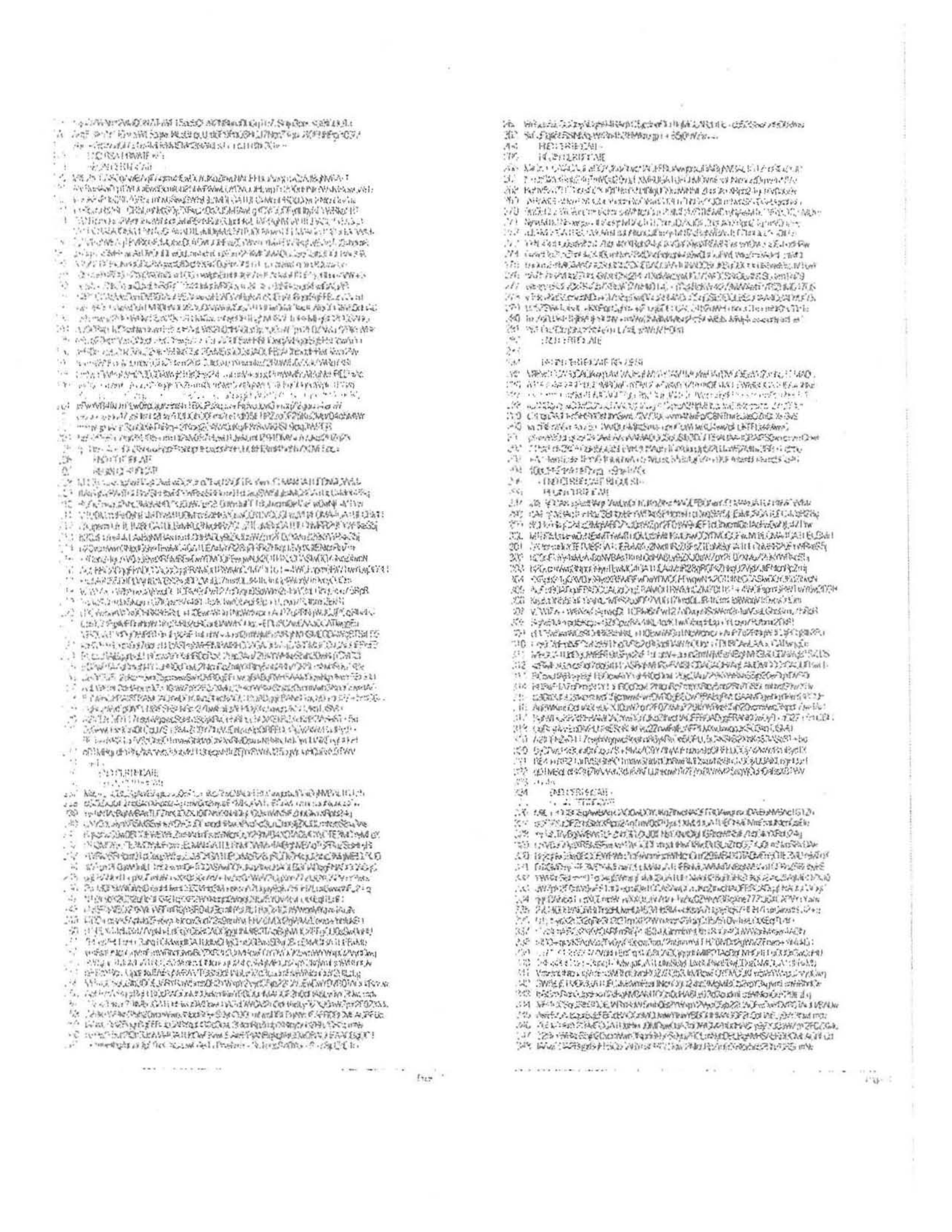
Respectfully submitted,

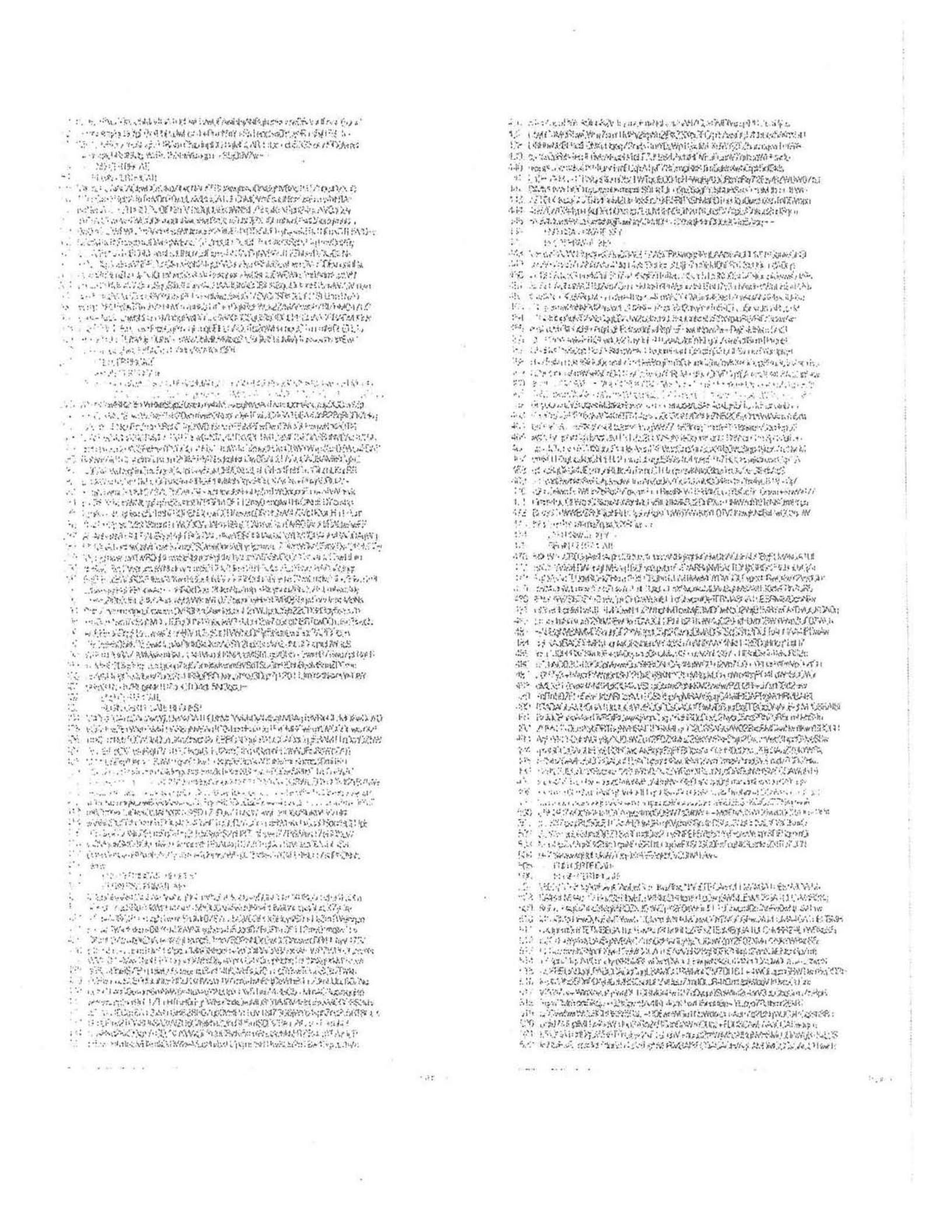
Neil H. MacBride
United States Attorney

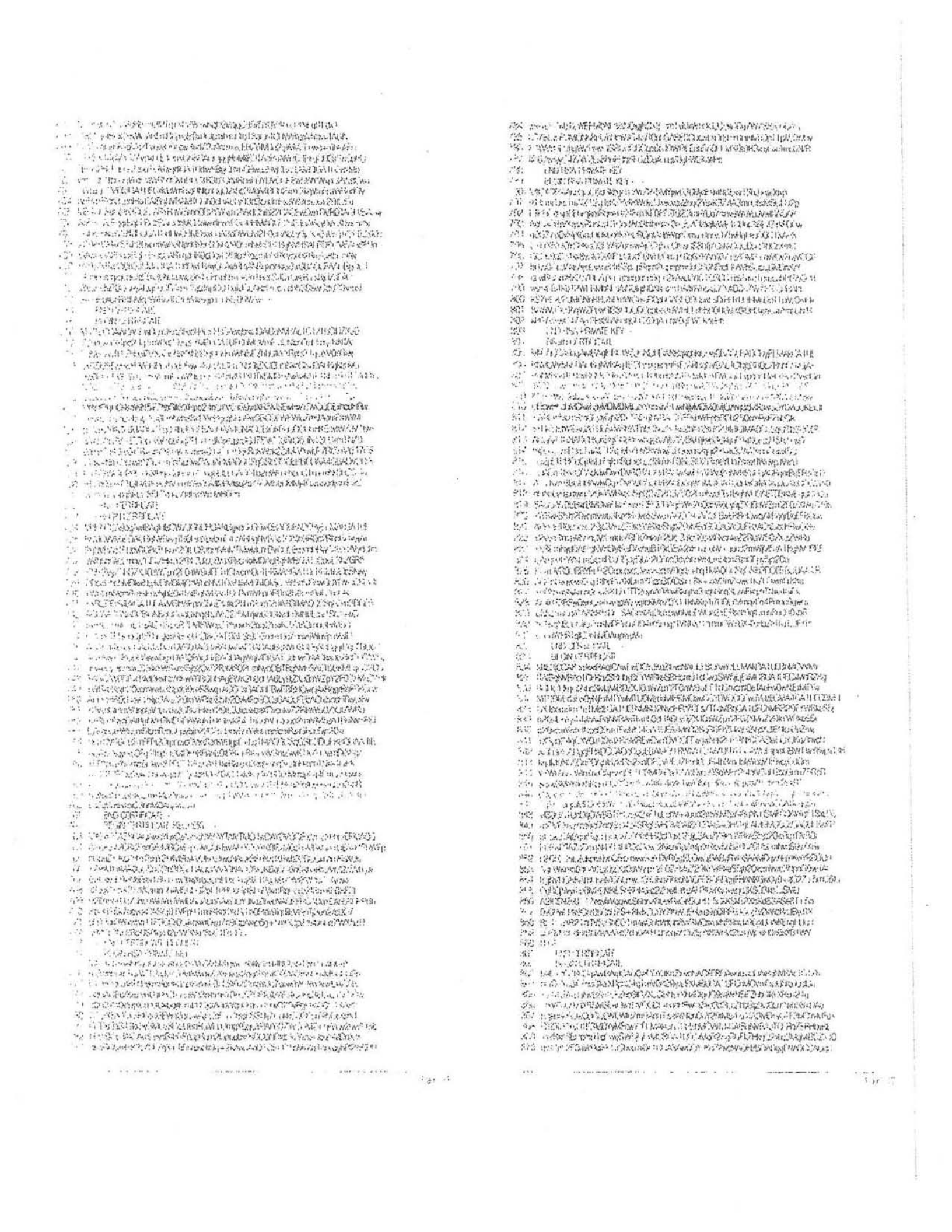
By: [redacted]

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

Attachment A







ATTACHMENT B

Lavabit uses 2048-bit Secure Socket Layer (SSL) certificates purchased from GoDaddy to encrypt communication between users and its server. SSL encryption employs public-key cryptography, in which both the sender and receiver each have two mathematically linked keys: a "public" key and a "private" key. "Public" keys are published, but "private" keys are not. In this circumstance, a Lavabit customer uses Lavabit's published public key to initiate an encrypted email session with Lavabit over the internet. Lavabit's servers then decrypt this traffic using their private key. The only way to decrypt this traffic is through the usage of this private key. A SSL certificate is another name for a published public key.

To obtain a SSL certificate from GoDaddy, a user needs to first generate a 2048-bit private key on his/her computer. Depending on the operating system and web server used, there are multiple ways to generate a private key. One of the more popular methods is to use a freely available command-line tool called OpenSSL. This generation also creates a certificate signing request file. The user sends this file to the SSL generation authority (e.g. GoDaddy) and GoDaddy then sends back the SSL certificate. The private key is not sent to GoDaddy and should be retained by the user. This private key is stored on the user's web server to permit decryption of internet traffic, as described above. The FBI's collection system that will be installed to implement the PR/TT also requires the private key to be stored to decrypt Lavabit email and internet traffic. This decrypted traffic will then be filtered for the target email address specified in the PR/TT order.

Depending on how exactly the private key was first generated by the user, it itself may be encrypted and protected by a password supplied by the user. This additional level of security is useful if, for example, a backup copy of the private key is stored on a CD. If that CD was lost or stolen, the private key would not be compromised because a password would be required to access it. However, the user that generated the private key would have supplied it at generation time and would thus have knowledge of it. The OpenSSL tool described above is capable of decrypting encrypted private keys and converting the keys to a non-encrypted format with a simple, well-documented command. The FBI's collection system and most web servers requires the key to be stored in a non-encrypted format.

A 2048-bit key is composed of 512 characters. The standard practice of exchanging private SSL keys between entities is to use some electronic medium (*e.g.*, CD or secure internet exchange). SSL keys are rarely, if ever, exchanged verbally or through print medium due to their long length and possibility of human error. Mr. Levison has previously stated that Lavabit actually uses five separate public/private key pairs, one for each type of mail protocol used by Lavabit.

PEM format is an industry-standard file format for digitally representing SSL keys. PEM files can easily be created using the OpenSSL tool described above. The preferred medium for receiving these keys would be on a CD.