IN THE
UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

Nos. 13-4625(L); 13-4626

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

v.

UNDER SEAL 1; UNDER SEAL 2,

Parties-In-Interest-Appellants.

Appeal from the United States District Court
for the Eastern District of Virginia at Alexandria
The Honorable Claude M. Hilton, Senior District Judge

BRIEF OF THE UNITED STATES

DANA J. BOENTE
ACTING United States Attorney

MICHAEL BEN'ARY
ANDREW PETERSON
JAMES L. TRUMP

United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314
(703) 299-3700

MYTHILI RAMAN
ACTING ASSISTANT ATTORNEY
GENERAL, CRIMINAL DIVISION

NATHAN JUDISH
JOSH GOLDFOOT
BENJAMIN FITZPATRICK
BRANDON VAN GRACK

U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES AND RULES

OTHER AUTHORITIES

IN THE
UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

Nos. 13-4625; 13-4626

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

v.

UNDER SEAL 1; UNDER SEAL 2,

Parties-In-Interest-Appellants.

Appeal from the United States District Court
for the Eastern District of Virginia at Alexandria
The Honorable Claude M. Hilton, Senior District Judge

BRIEF OF THE UNITED STATES

ISSUES PRESENTED

By marketing "secure" services, may an electronic communications service provider ignore (A) a statute compelling the provider to furnish "all" information needed for the installation and operation of a pen register/trap-and-trace device, and (B) a warrant issued by a neutral magistrate compelling the production of information used to decrypt a user's communications?

Was it plain error for a district court to use civil sanctions to compel the production of information needed to decrypt communications that were the subject of lawful court orders?

STATEMENT OF THE CASE AND FACTS

Lavabit LLC is an electronic communications service provider located in Dallas, Texas (*see* http://lavabit.com/). Ladar Levison is its sole owner and operator. Lavabit provides email services for its customers.

In June 2013, the Federal Bureau of Investigation determined that the target of an ongoing investigation in the Eastern District of Virginia was using Lavabit's email service. On June 8, 2013, the FBI served a grand jury subpoena on Lavabit through Ladar Levison for billing and subscriber information pertaining to the target's email account. J.A. 152-54. On June 10, 2013, the United States obtained an order pursuant to 18 U.S.C. § 2703(d) directing Lavabit LLC to provide, within ten days, additional records and information about the target's email account. J.A.

1-4. Mr. Levison received that order on June 11, 2013. J.A. 15. Mr. Levison responded by mail, which was not received by the government until June 27, 2013. *Id.*

On June 28, 2013, the United States applied for and obtained a pen register and trap and trace order (pen/trap order) for the target's Lavabit email account. J.A. 10-12. The pen/trap order, issued by the Honorable Theresa Buchanan, United States Magistrate Judge for the Eastern District of Virginia, authorized the government to (1) capture all "non-content" dialing, routing, addressing, and signaling information sent to or from a specific account, and (2) record the date and time of the initiation and receipt of such transmissions, to record the duration of the transmissions, and record user log-in data from that specific account, all for a period of sixty days. J.A. 10-11. The order further directed Lavabit to furnish the FBI, "forthwith, all information, facilities, and technical assistance necessary to accomplish the installation and use of the pen/trap device." J.A. 11. The order required that the government "take reasonable steps to ensure that the monitoring equipment is not used to capture any" content-related information. *Id.* The pen/trap order and accompanying application was sealed pursuant to 18 U.S.C. § 3123(d). *Id.*

On June 28, 2013, FBI special agents met Mr. Levison at his residence in Dallas, Texas, and discussed with him the pen/trap order entered earlier that day.

J.A. 15. Mr. Levison told the agents that he would not comply with the pen/trap order and wanted to speak to an attorney. *Id.* It was unclear to the agents whether Mr. Levison would not comply with the order because it was too difficult, technically not feasible, or simply not consistent with his business practice of providing encrypted email service for his customers. *Id.*

Shortly thereafter on June 28, upon the motion of the government, Magistrate Judge Buchanan issued an Order Compelling Compliance Forthwith. J.A. 8-9. The magistrate judge directed Lavabit to comply with the pen/trap order and, specifically, to provide the FBI with unencrypted data as well as any information, facilities, or technical assistance needed to provide the FBI with unencrypted data. *Id.* Finally, the order indicated that non-compliance would subject Lavabit "to any penalty in the power of the Court, including the possibility of criminal contempt of Court." J.A. 9.

Despite this order, Lavabit did not comply. Between June 28 and July 9, 2013, the FBI made numerous attempts, without success, to speak with Mr. Levison to discuss the pen/trap order. J.A. 16. On July 9, 2013, pursuant to the government's motion, the Honorable Claude M. Hilton, United States District Judge for the Eastern District of Virginia, ordered Mr. Levison to appear before the court on July 16, 2013, to show cause why Lavabit failed to comply with the pen/trap and compliance orders and why the court should not hold Lavabit and Mr. Levison in contempt. J.A. 21-22.

The following day, the government discussed by conference call the pen/trap order and related issues with Mr. Levison and his attorney.[1] J.A. 33-34. Mr. Levison's concerns focused primarily on how the pen/trap device would be installed on the Lavabit system, what data would be captured by the device, and what data would be viewed and preserved by the government. *Id.* The FBI explained to Mr. Levison that the pen/trap device could be installed with minimal impact to the Lavabit system, and the agents told Mr. Levison that they would meet with him when they were ready to install the device and discuss with him any of the technical details regarding the installation and use of the device. As for the data collected by the device, the agents assured Mr. Levison that the only data that the agents would obtain and review is that which is stated in the order – *i.e.*, user log-in information and the date, time, and duration of the email transmissions for the target account – and nothing more. *Id.* Mr. Levison appeared to acknowledge that the successful installation and use of the pen/trap device would require access to Lavabit's server and the encryption keys used by Lavabit's customers to encrypt

[1] Mr. Levison was represented intermittently during the course of proceedings in the district court.

their email communications. Mr. Levison did not indicate whether he would allow the FBI to install the pen/trap device or provide the encryption keys. *Id.*

On July 11, 2013, the United States Attorney's Office issued a subpoena for Mr. Levison to testify before the grand jury in the Eastern District of Virginia on July 16, 2013. J.A. 23-24. The grand jury subpoena also commanded Mr. Levison to bring to the grand jury the Lavabit encryption keys and any other information necessary to accomplish the installation and use of the pen/trap device pursuant to the pen/trap order. *Id.* The FBI attempted to serve the subpoena on Mr. Levison at his residence. After knocking on his door, FBI special agents witnessed Mr. Levison leave the rear of his apartment, get in his car, and drive away. Later in the evening, the FBI successfully served Mr. Levison with the subpoena. J.A. 82.

On July 13, 2013, Mr. Levison sent an email to the prosecutors 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 [sic] automatically if any problems appeared.

J.A. 83. Mr. Levison's email again confirmed that Lavabit was capable of providing the means for the FBI to install the pen/trap device and obtain the requested information in an unencrypted form. The Assistant United States Attorney replied to Mr. Levison's email 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. *Id.*

On July 16, 2013, the district judge issued a search warrant to Lavabit for (1) "[a]ll information necessary to decrypt communications sent to or from the [target email account], including encryption keys and SSL keys" and (2) "[a]ll information necessary to decrypt data stored in or otherwise associated" with the targeted Lavabit account. J.A. 25-29. A non-disclosure order issued pursuant to 18 U.S.C. § 2705(b) accompanied the warrant. J.A. 32. The search warrant and accompanying materials were further sealed by the court pursuant to a Local Rule 49(B). J.A. 31.

Mr. Levison, without counsel, appeared as directed before the district court on July 16, 2013. Mr. Levison made an oral motion to unseal the proceedings and related filings. J.A. 40. The government objected, and the district court denied Mr. Levison's motion. J.A. 30. Mr. Levison subsequently indicated to the court that he would permit the FBI to place a pen/trap device on his server. J.A. 48. The government requested that the district court further order Mr. Levison to provide his encryption or Secure Sockets Layer (SSL) keys, explaining that placing a pen/trap device on Lavabit's server would only provide encrypted information and 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. J.A. 33-37. The court determined that the government's request for the SSL keys was premature because Mr. Levison had offered to place the pen/trap device on his server and the court's order for a show cause hearing was based on the failure to comply with the pen/trap order. J.A. 44-46. 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. J.A. 51.

On July 25, 2013, Mr. Levison, through counsel, filed two motions – a Motion for Unsealing of Sealed Court Records and a Motion to Quash Subpoena and Search Warrant. J.A. 54-65, 66-75. In these motions, Mr. Levison confirmed that providing the SSL keys to the government would provide the data required under the pen/trap order in an unencrypted form. J.A. 59, 72. Lavabit refused, however, to provide the encryption keys. To provide the government with sufficient time to respond to the newly filed motions, the hearing was rescheduled for August 1, 2013.

Prior to the August 1 hearing, and after discussions with Mr. Levison, the FBI installed a pen/trap device to capture the information sought by the pen/trap order. Without the encryption keys, however, the pen register was not able to identify and capture data related to all of the emails sent to and from the target account as well as other information authorized for collection under the pen/trap order. *See* J.A. 105, 131.

At the hearing on August 1, 2013, the district court denied both of Lavabit's motions and directed Lavabit to provide the government with the encryption keys necessary for the operation of the pen/trap order by 5 p.m. on August 2, 2013. J.A. 118-19.

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 SSL keys[2] needed to operate the pen/trap device. This printout, in what appears to be 4-point type, consists of 11 columns of largely illegible characters. J.A. 125-30.

At approximately 3:30 p.m. EDT (2:30 p.m. CDT), an Assistant United States Attorney contacted counsel for Lavabit and Mr. Levison and informed him that the hard copy format for receipt of the encryption keys was unworkable, and the government would need the keys produced in electronic format. *Id.* Lavabit's 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. *Id.*

On August 4, 2013, the Assistant United States Attorney sent an email to counsel for Lavabit and Mr. Levison stating that the government expected to receive an electronic version of the encryption keys by 10:00 a.m. CDT on Monday, August 5, 2013. *Id.* The email indicated that the keys were to be produced in PEM format, an industry standard file format for representing SSL

[2] Throughout this brief, the government will refer to "SSL keys." Based on the government's knowledge, Lavabit had a separate SSL key for different application-layer protocols offered by the service, but the key was the same for every user of each particular protocol. Because any particular user might use every protocol offered by Lavabit, all of the SSL keys were necessary to decrypt one particular user's communications.

keys. The email further stated that the preferred medium for receipt of these keys would be a CD hand-delivered to the Dallas office of the FBI, a location with which Mr. Levison was familiar. *Id.* The Assistant United States Attorney informed counsel for Lavabit LLC and Mr. Levison that the government would seek an order imposing sanctions if Mr. Levison did not produce the encryption keys in electronic format by Monday morning. *Id.*

The government did not receive the electronic keys as requested. J.A. 122. Because Lavabit had only produced unusable information as of the August 2 deadline, the government then moved for sanctions. The government's request for sanctions explained what had transpired since the court's order directing the production of the keys, including Lavabit's production of incomprehensible information and failure to provide the information in a usable electronic format. The government requested that Lavabit and Mr. Levison be directed to produce the encryption keys in electronic format by noon (CDT) on August 5, 2013, and for sanctions in the amount of $5000 per day beginning August 5, 2013, and continuing each day in the same amount, until Lavabit and Mr. Levison complied with the district court's orders. J.A. 120-31.

On August 5, 2013, the district court, adopting the reasons stated in the government's motion, granted the motion for sanctions and imposed a fine of $5000 per day on both Mr. Levison and Lavabit, beginning August 5, 2013, until the encryption keys were produced in electronic format. J.A. 132-33. It is this order Lavabit and Mr. Levison now appeal.[3]

On August 7, 2013, at approximately 11:00 a.m. CDT, Mr. Levison left at the FBI's office in Dallas, Texas, a disk containing the encryption keys necessary to obtain the data sought by the pen/trap order.

That same day, Mr. Levison shut down Lavabit's operations, including its email service. In a statement posted on his web page, and subsequently in numerous interviews with the media, Mr. Levison alerted all of Lavabit's users, including the target of the investigation, that Lavabit was engaged in litigation with the government and that, rather than comply with the court's orders, he decided to shut down his business. *See* http://lavabit.com (last accessed Nov. 7, 2013).

SUMMARY OF ARGUMENT

Lavabit appeals a contempt order from the district court. But instead of attempting to justify Lavabit's contemptuous conduct, Lavabit instead launches a host of new challenges to the underlying orders. Almost none of these challenges were presented to the district court. Lavabit forfeited these new arguments, and this Court should not consider them.

[3] Lavabit also filed a notice of appeal regarding the district court's order denying Lavabit's motion to unseal the record in this matter. As the district court later unsealed substantial portions of the record and Lavabit raises no arguments regarding sealing in its brief, any challenge to the sealing order is forfeited.

Moreover, the pen/trap order and the search warrant issued by the district court were plainly lawful. The information used by Lavabit to encrypt communications on its systems, what has been referred to as SSL or encryption keys, was both necessary to the installation and operation of a lawfully ordered pen register/trap and trace device as well as subject to disclosure pursuant to 18 U.S.C. § 2703. As such, it was within the district court's power to compel the production of those keys. Just as a business cannot prevent the execution of a search warrant by locking its front gate, an electronic communications service provider cannot thwart court-ordered electronic surveillance by refusing to provide necessary information about its systems. That other information not subject to the warrant was encrypted using the same set of keys is irrelevant; the only user data the court permitted the government to obtain was the data described in the pen/trap order and the search warrant. All other data would be filtered electronically, without reaching any human eye. Finally, Lavabit's belief that the orders here compelled a disclosure that was inconsistent with Lavabit's "business model" makes no difference. Marketing a business as "secure" does not give one license to ignore a District Court of the United States.

ARGUMENT

I. BECAUSE LAVABIT FORFEITED NEARLY ALL THE ARGUMENTS IN ITS BRIEF BY FAILING TO RAISE THEM BELOW, THE STANDARD OF REVIEW IS PLAIN ERROR AT BEST.

A. Issues Not Before the Court

Below, Lavabit challenged a grand jury subpoena (which was later withdrawn) and a search warrant that both commanded Lavabit to produce its encryption keys. Initially, though Lavabit discusses at length the propriety of the government's use of a grand jury subpoena to obtain encryption keys, the grand jury subpoena is not before the Court. As Lavabit's brief before the district court noted in a footnote, the subpoena was withdrawn. J.A. 67. Mr. Levison never appeared before the grand jury, and the district court's August 1 order does not list the grand jury subpoena as a basis for the compelled production of the encryption keys. J.A. 118-19. Because it was Mr. Levison's failure to comply with the August 1 order that formed the basis of the district court's sanctions order, *see* J.A. 132-33, Mr. Levison's failure to comply with the withdrawn subpoena was not a basis for the district court's contempt finding. Thus, the validity of the subpoena is not on appeal.

Second, the statutory validity of neither the June 28 pen/trap order nor the search warrant should be considered on appeal. Lavabit made no argument regarding the pen/trap order or the pen/trap statute before the district court. In fact, Lavabit never asked the district court to quash the pen/trap order. Because the contempt order was based on Lavabit's failure to comply with *both* the pen/trap order and the warrant, J.A. 119 & 132, Lavabit's failure to challenge the pen/trap order below is sufficient, standing alone, to support the sanctions imposed by the district court.

Third, though Lavabit did ask to quash the search warrant, Lavabit argued before the district court that the search warrant failed to meet the standards for court orders under 18 U.S.C. § 2703(d) (which refers to the standards for issuing an order described in 18 U.S.C. § 2703(c)(1)(C)), but never mentioned the warrant provisions of the Stored Communications Act, *see* 18 U.S.C. § 2703(c)(1)(A). "It is the general rule, of course, that a federal appellate court does not consider an issue not passed upon below." *Singleton v. Wulff*, 428 U.S. 106, 120 (1976); *Holland v. Big River Minerals Corp.*, 181 F.3d 597, 605 (4th Cir. 1999).

B. The Standard of Review

In its pleading before the district court, Lavabit made three arguments: (1) the search warrant was a general warrant because it did not sufficiently limit an investigating officer's discretion to view other users' information, J.A. 67; (2) the subpoena and warrant sought information that was not material to the government's investigation, J.A. 70; and (3) compliance with the subpoena was unduly burdensome, J.A. 71.

Lavabit's first two claims were attacks on the warrant under the Fourth Amendment and 18 U.S.C. § 2703(d) (which was not the basis for the warrant). The review of legal issues involved in those determinations is *de novo*, but the district court's factual determinations are reviewed under a "highly deferential" standard of review, *Simmons v. Poe*, 47 F.3d 1370, 1378 (4th Cir. 1995), and may be overturned only if clearly erroneous, *see United States v. Rusher*, 966 F.2d 868, 873 (4th Cir. 1992). *See also United States v. Wellman*, 663 F.2d 224, 228 (4th Cir. 2011) ("[A] judicial officer's determination of probable cause customarily is accorded 'great deference' by reviewing courts."). The district court's rejection of Lavabit's argument that production of its encryption keys would be unduly burdensome is only reviewable as an abuse of discretion. *See In re Grand Jury Subpoena*, 646 F.3d 159, 164 (4th Cir. 2011).

These standards only apply where a litigant has preserved such claims by raising them before the district court. Yet Lavabit's appellate brief contains numerous arguments Lavabit failed to raise before the court below. In the Fourth Circuit, claims not raised below are forfeited unless the party raising them can identify one of two exceptional circumstances: (1) plain error, or (2) a fundamental miscarriage of justice. *See Volvo Const. Equip. N. Am., Inc. v. CLM*

Equip. Co., 386 F.3d 581, 603 (4th Cir. 2004); *Muth v. United States*, 1 F.3d 246, 250 (4th Cir. 1993); *see also United States v. One 1971 Mercedes Benz 2-Door Coupe,* 542 F.2d 912, 914 (4th Cir. 1976) (noting issues not presented to the district court may only be considered on appeal in "exceptional circumstances"). Neither is present here.

Lavabit's newly raised arguments do not identify any error committed by the district court, let alone plain error. To commit plain error, a court must commit error that is "obvious or clear" under current law. *See United States v. Brack*, 651 F.3d 388, 392 (4th Cir. 2011); *see also United States v. Olano*, 507 U.S. 725, 731-32 (1993) (defining plain error for the purposes of Federal Rule of Criminal Procedure 52(b)). Lavabit itself has stated that the issues raised in its brief are issues "of first impression." Lavabit Br. at 30. When an issue has *never been raised before by anyone in any court*, it is not an "obvious" or "clear" violation of an existing legal rule. "An error is clear or obvious 'when settled law of the Supreme Court or this circuit establishes that an error has occurred.'" *United States v. Reid*, 523 F.3d 310, 316 (4th Cir. 2008) (quoting *United States v. Promise*, 255 F.3d 150, 160 (4th Cir. 2001) (en banc)). *See also United States v. King*, 628 F.3d 693, 700 (4th Cir. 2011) ("An error qualifies as 'plain' only if it contravenes 'the settled law of the Supreme Court or this circuit.'").

Moreover, it was not error for the district court to ignore legal theories that Lavabit did not raise when enforcing the pen/trap order and search warrant. To identify error at all, Lavabit must show that the district court's failure to *sua sponte* consider the issues Lavabit has only now come around to litigating was error. But courts generally ignore issues not raised by parties in litigation. Though courts sometimes raise issues *sua sponte*, the choice (unless the issue is jurisdictional) is discretionary. *See, e.g.*, *Clodfelter v. Republic of Sudan*, 720 F.3d 199, 207-08 (4th Cir. 2013) (noting that decision to consider *res judicata* defense not raised by a party is discretionary). Where, as here, a court acts within its lawful discretion, it does not commit error, and certainly not error that is plain.

Neither the issuance of the pen/trap order and search warrant nor the sanctioning of Lavabit constituted a "fundamental miscarriage of justice." A fundamental miscarriage of justice is normally reserved for extreme situations, such as the wrongful conviction of an innocent person. *See United States v. MacDonald*, 641 F.3d 596, 610 (4th Cir. 2011). Indeed, the government has found no reported case where a court's enforcement of its own lawful orders was considered a "fundamental miscarriage of justice." Nor would any miscarriage of justice result from the court's refusal to consider Lavabit's forfeited claims. Because Lavabit has now complied with the warrant and disclosed the keys, the only practical issue at stake in this appeal is Lavabit and Mr. Levison's liability for the $5000 per day assessment imposed by the district court. As Lavabit has identified no exceptional circumstances justifying this Court's consideration of its newly raised legal arguments, the Court should reject them. *See Agra Gill & Duffus, Inc. v. Benson*, 920 F.2d 1173, 1176 (4th Cir. 1990).

Lavabit's reliance on facts outside the record to support its new claims is an additional reason to reject them. The primary rationale of the rule against litigating issues first on appeal is that parties must be able to present evidence to support their arguments before the district court. *See Singleton*, 428 U.S. at 120 (noting that refusal to review arguments not previously raised is "essential in order that parties may have the opportunity to offer all the evidence they believe relevant to the issues." (internal quotation marks and citation omitted)). Lavabit's newly raised arguments are fact-intensive: For instance, as part of its argument that the search warrant was not lawful, Lavabit argues that "Lavabit's private keys are not connected with criminal activity in the slightest." Lavabit Br. 22. That is a factual assertion unsupported by the record. Lavabit also now challenges whether there was sufficient probable cause to support the warrant. *Id.* at 22. Whether there are sufficient facts to determine probable cause is by definition a fact-specific inquiry. *See United States v. Williams*, 974 F.2d 480, 481 (4th Cir. 1992). Courts should be especially cautious to rule on weighty matters where they lack the benefit of a completely developed record or the consideration of the judge below. *See United*

States v. Ramos-Cruz, 667 F.3d 487, 500 (4th Cir. 2012) (declining to consider new evidence for the first time on appeal). Thus, this Court should decline to review Lavabit's forfeited statutory and constitutional claims, and limit appellate review to those claims raised below.

II. THE DISTRICT COURT PROPERLY ORDERED LAVABIT TO DISCLOSE ITS ENCRYPTION KEYS PURSUANT TO THE PEN/TRAP STATUTE.

Lavabit never moved in the district court to quash the pen/trap order, and never argued the government lacked statutory authority for that order; thus, these arguments were forfeited.

Nonetheless, the Pen Register and Trap and Trace Device statute, 18 U.S.C. §§ 3121-3127 ("Pen/Trap statute") authorized the court orders requiring Lavabit to disclose its encryption keys. Those orders were proper because the Pen/Trap statute mandates that providers assist with installation and use of a pen/trap device when such assistance is directed by a court. *See* 18 U.S.C. § 3124. Section 3124 contains separate assistance provisions for pen registers and trap and trace devices. *See* 18 U.S.C. § 3124(a) (pen registers); 18 U.S.C. § 3124(b) (trap and trace devices). Lavabit incorrectly asserts that these two provisions set forth "identical standard[s]" and argues, for the first time on appeal, that the provisions only require assistance with "installation" of a pen/trap device. Lavabit Br. at 14. But Lavabit has fundamentally misread the statute. Both provisions support the district court orders requiring Lavabit to disclose its encryption keys, and what is more the assistance provision for trap and trace devices is even broader than the assistance provision for pen registers. In particular, the pen-register provision of § 3124(a) requires assistance with "installation" of a pen register, while the trap-and-trace-device provision of § 3124(b) requires assistance "including installation and operation" of the device. 18 U.S.C. § 3124. This statutory language is fatal to Lavabit's argument that the district court lacked statutory authority to compel Lavabit to disclose its keys.

A. Statutory Background

The Pen/Trap statute provides two related mechanisms for law enforcement to obtain non-content information regarding a user's communications: pen registers and trap and trace devices. A "pen register" is defined as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted … ." 18 U.S.C. § 3127(3).[4] A "trap and trace device" is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing,

[4] This definition further excludes contents of communications and devices or processes used for billing or cost accounting.

addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication … ." 18 U.S.C. § 3127(4).[5]

Based on these definitions, the Pen/Trap statute "unambiguously authorize[s] the use of pen registers and trap and trace devices on e-mail accounts." *In re Application*, 416 F. Supp. 2d 13, 14 (D.D.C. 2006); *see also United States v. Forrester*, 512 F.3d 500, 509-11 (9th Cir. 2008) (rejecting Fourth Amendment challenge to pen register on email and Internet activity). For example, a trap and trace device on a web-based email account (such as the targeted Lavabit account in this case) captures the Internet Protocol addresses from which a user accesses his email account[6] and the "from" information on email sent to the account, because this information helps identify the source of communications to the account. A pen register on a web-based email account captures the "to" information on email sent from the account, because "to" information is addressing information transmitted by the provider. Thus, when the United States obtained a pen/trap order on the targeted Lavabit email account, it obtained authority to use both a pen register and a trap and trace device.

[5] This definition further excludes contents of communications.

[6] This IP address information can be particularly valuable to law enforcement in locating a fugitive. If law enforcement can discover in real-time the IP address used by a fugitive, it may be able to locate and apprehend the fugitive.

The Pen/Trap statute mandates that providers assist with installation and use of both a pen register and a trap and trace device when such assistance is directed by a court. *See* 18 U.S.C. § 3124(a) & (b). Although both provisions have broad scope, the trap-and-trace provision is broader than the pen register provision.[7] In particular, the trap-and-trace assistance provision states that, upon the request of an officer authorized to receive the results of a trap and trace device, a service provider:

> shall install such device forthwith on the appropriate line or other facility and shall furnish such investigative or law enforcement officer *all additional information, facilities and technical assistance including installation and operation of the device* unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the

[7] The distinction between the assistance requirements for pen registers and trap and trace devices has historical roots. When the Pen/Trap statute was enacted in 1986, pen/traps were implemented only on telephones. *See* Electronic Communications Privacy Act of 1986 § 301, Pub. L. No 99-508, 100 Stat 1848 (creating the Pen/Trap statute and defining "pen register" using telephone-specific language); S. Rep. No. 99-541, at 10 (1986). At that time, providers had to do more work to implement a trap and trace device than a pen register. *See In re Application*, 616 F.2d 1122, 1127 (9th Cir. 1980) ("In the case of the pen register, the device may be physically operated by law enforcement officers after limited assistance from the telephone company … . Tracing through ESS facilities, on the other hand, because it is entirely automated, must be activated by the programing of a computer by a technician of the telephone company."). When the definitions of "pen register" and "trap and trace device" were broadened to reach Internet communications in 2001, the assistance provisions of § 3124 remained unchanged. USA Patriot Act § 216, Pub. L. No. 107-56, 115 Stat 272 (2001). Regardless, given the broad statutory definitions of "pen register" and "trap and trace device," both assistance provisions require providers to assist with the implementation of pen/trap orders on the Internet.

> installation and use is to take place, if such installation and assistance is directed by a court order as provided in § 3123(b)(2) of this title.

18 U.S.C. § 3124(b) (emphasis added). The pen-register assistance provision section provides that upon request of a law enforcement agency authorized to use a pen register, a service provider:

> shall furnish such investigative or law enforcement officer forthwith *all information, facilities, and technical assistance necessary to accomplish the installation of the pen register* unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in § 3123(b)(2) of this title.

18 U.S.C. § 3124(a) (emphasis added).

B. The District Court Orders Demanding Lavabit's Encryption Keys Were Lawful, as This Information Was Necessary to the Installation and Operation of the Pen/Trap Device.

When the government obtained a pen/trap order on the targeted Lavabit account, the issuing judge ordered Lavabit to assist with "installation and use" of the pen/trap device, and the court subsequently issued two additional orders requiring assistance from Lavabit, including disclosure of its encryption keys. J.A. 8-9, 11-12, 118-19. Both the pen-register assistance provision of § 3124(a) and the trap-and trace-device assistance provision of § 3124(b) supported these orders.

Under the plain language of § 3124(b), the district court properly ordered Lavabit to provide its encryption keys to the United States: A provider must furnish "*all additional information*, facilities and technical assistance *including installation and operation*" of the trap-and-trace device. 18 U.S.C. § 3124(b) (emphasis added). Lavabit's encryption keys were information essential to the device's "installation and operation." Lavabit had not programmed its system to produce pen/trap information in response to a court order, and so Lavabit could not implement the order on its own without taking the time to write the necessary code. The government could implement the pen/trap device with its hardware and software, but that device needed Lavabit's encryption keys to function effectively. J.A. 131. Thus, under § 3124(b), the court properly ordered Lavabit to disclose its encryption keys, as the keys were "information" necessary for installation and operation of the device.

Lavabit mistakenly asserts that the Pen/Trap statute "requires only that a company provide the government with technical assistance in the *installation* of a pen/trap device; providing encryption keys does not aid in the device's installation at all, but rather in its *use*." Lavabit Br. at 11, 14-15 (emphasis in original). In fact, the actual language of § 3124(b) requires assistance with "all additional information … including installation *and operation*" (emphasis added). Thus, to the extent Lavabit argues that § 3124(b) is limited to the installation of a trap-and-trace device, Lavabit is wrong. Because § 3124(b) mandates assistance with installation and operation, the court properly ordered Lavabit to disclose its encryption keys.

Lavabit further argues that the statute only requires assistance with installing a device unobtrusively, rather than effectively. Lavabit Br. at 14-15. Not only would this interpretation make a mockery of the Pen/Trap statute's assistance provisions, but it is also inconsistent with the language of § 3124(b). Section 3124(b) requires a provider to furnish assistance "*including* installation and operation of the device unobtrusively and with a minimum of interference with the services" (emphasis added). Under this language, the provider's assistance is not limited to installation and operation, though it certainly includes those functions. This broad interpretation of the § 3124(b) assistance requirement is further supported by the heading of § 3124 itself: "Assistance in installation and *use* of a pen register or a trap and trace device" (emphasis added). *See Fla. Dep't of Revenue v. Piccadilly Cafeterias, Inc.*, 554 U.S. 33, 47 (2008) (stating that a section heading is a "tool[] available for the resolution of a doubt about the meaning of a statute"). Moreover, to install and operate the device unobtrusively, it must be installed and operated effectively. Thus, the court's order to Lavabit to disclose its keys was proper.

The pen-register assistance provision of § 3124(a) also justified the district court's order. That provision requires a provider to furnish "forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register." Lavabit's encryption keys were information necessary to accomplish the installation of the pen register. A pen register is by definition a device or process that "records or *decodes* dialing, routing, addressing, or signaling information." 18 U.S.C. § 3127(3) (emphasis added). Without Lavabit's encryption keys, the government would be unable to decode the addressing information of communications of the targeted account. Indeed, without Lavabit's encryption keys, the pen register device would be unable to identify communications from the targeted account. A device that cannot decode dialing, routing, addressing, or signaling information is simply not a pen register; thus, without Lavabit's encryption keys, no pen register could be installed on the targeted account at all.

Lavabit, without citing a single source, interprets "installation" of a pen register to end when the device is set in position; it argues that a provider "might" be required "to tell the government which cables carry the relevant communications, so that the government can attach the device correctly." Lavabit Br. at 14. But the definition of "installation" is not so limited. *See, e.g.*, Webster's Third New International Dictionary 1171 (1961) (defining "installation" as "the setting up or placing in position for service or use"); American Heritage Dictionary of the English Language (3d ed. 1992) (defining "install" as "to set in position and connect or adjust for use"); Webster's II New Riverside University Dictionary (1988) (defining "install" as "to set in position or adjust for use"). Without Lavabit's encryption keys, the pen register on the targeted account could never be adjusted for use, so it would not be installed.

The logical extension of Lavabit's narrow interpretation of "installation" would allow a company to thwart any pen/trap order. Under Lavabit's interpretation of "installation," a landlord, custodian, or service provider would exhaust the duty to assist in "installation" by merely telling an officer the location of a telephone wire. The person would be under no obligation to unlock the front door or permit access to the telephone wiring closet or to identify the type of system or hardware used to transmit the relevant communications. Such a narrow interpretation of "installation" would make installing a pen/trap device impossible, even in the pre-Internet age. Thus, the district court properly ordered Lavabit to disclose its encryption keys under § 3124(a).

Lavabit asserts that interpreting § 3124 to require it to disclose its keys is inconsistent with congressional intent, but its assertion is based on neither statutory text nor legislative history. *See* Lavabit Br. at 16-17 ("It is unthinkable that Congress would have given the government the authority to seize keys[.]"). Indeed, Lavabit cites no evidence from the statute or its legislative history in support of its novel position that providers must assist in the placement of pen/trap devices but nothing else. To the contrary, when Congress enacted § 3124, it explained that a provider would be required to provide assistance "necessary to effectuate the pen register order." S. Rep. No. 99-541, at 48 (1986). It would be truly odd that Congress, when enacting a statute for the purpose of codifying government surveillance of electronic communications, intended to deny the government the authority to obtain information to which a provider has access merely because the information is encrypted during the transmission between a user and the provider.

Lavabit also argues that the language in the statute requiring installation be "unobtrusive" limits the assistance the communications provider must offer to the government, such that *only* assistance that is unobtrusive may be provided. Lavabit Br. at 14-15.[8] This argument makes no sense. A pen/trap device that does not function may well be "unobtrusive," but providers are not allowed to limit their assistance to helping the government install ineffective devices. Moreover, the statute anticipates that it may be impossible to install a device with no interference at all. Both §§ 3124(a) and (b) state that a provider must provide assistance to accomplish the installation of a pen/trap device "unobtrusively *and with a*

[8] In the summary of argument, Lavabit states that the compelled production of the keys was obtrusive in that it disrupted Lavabit's service. Lavabit Br. at 11. That is not the argument made in the substance of the brief. That argument is also wrong – the production of the keys and the use of the pen/trap device would have been entirely invisible to Lavabit's customers.

minimum of interference … ." Thus, there is no basis to conclude that the language in the Pen/Trap statute designed to avoid tipping off targets of lawful criminal investigation prohibits the orders issued by the district court here.

Lavabit claims that requiring the disclosure of its keys was "a truly dramatic act," Lavabit Br. at 16, but providers can avoid disclosing their encryption keys simply by configuring their systems to implement pen/trap orders without government assistance. The record demonstrates that Lavabit could easily have done so: Lavabit stated that it could add code to implement the pen/trap order in twenty to forty hours. J.A. 112. Yet Lavabit chose not to do so, even during the five-week period between Lavabit's receipt of the pen/trap order and its shutdown. Lavabit was entitled to design its system as it pleased.[9] But having refused to add code to implement a lawful pen/trap order, Lavabit could not then refuse to cooperate with the government in implementing the order. In essence, Lavabit is

[9] The Communications Assistance for Law Enforcement Act ("CALEA"), 47 U.S.C. § 1002, does not apply to Lavabit, but the provider assistance obligations of the Pen/Trap statute are independent of CALEA. Moreover, when Congress enacted CALEA, it understood that existing provider-assistance provisions required a provider like Lavabit to decrypt communications. Both the House and Senate reports for CALEA stated that "telecommunications carriers have no responsibility to decrypt encrypted communications that are the subject of court-ordered wiretaps, *unless the carrier provided the encryption and can decrypt it*." H.R. Rep. No. 103-827(I), at 24 (1994); S. Rep. No. 103-402, at 24 (1994) (emphasis added). These reports explained that this obligation to decrypt was based on the Wiretap Act's provider assistance provision, 18 U.S.C. § 2518(4). *See id.* That provision is similar to the assistance provisions in § 3124 of the Pen/Trap statute.

claiming that private businesses have the authority to nullify the Pen/Trap statute simply by offering SSL encryption services that any service provider can purchase for a modest sum.

Lavabit also misstates the significance of key disclosure on communications to and from other Lavabit accounts. The pen/trap order only authorized access to the targeted account. Had the government been able to implement the pen/trap order effectively, that order, as well as other statutes such as the Wiretap Act and the Pen/Trap statute, would have prevented access to other Lavabit users' accounts using the encryption key. As the government stated to the district court, "[a]ll we're going to look at and all we're going to keep is what is called for under the pen register order." J.A. 114. The district court properly ordered Lavabit to disclose its encryption keys under the Pen/Trap statute, and Lavabit's challenge to the district court orders should be rejected.

III. THE SEARCH WARRANT ISSUED BY THE DISTRICT COURT LAWFULLY COMPELLED LAVABIT TO PRODUCE ITS ENCRYPTION KEYS TO THE GOVERNMENT.

Lavabit argues for the first time on appeal that the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq*, does not authorize a district court to issue a search warrant for private encryption keys. Even if it were not forfeited, this argument is both beside the point and incorrect. Lavabit's argument is beside the point because, even if the warrant were invalid, the pen/trap order independently required Lavabit to produce the encryption keys.[10] As argued above, Lavabit never asked the district court to quash the pen/trap order and the pen/trap order lawfully commands Lavabit to produce information identical to that described in the search warrant. Lavabit's argument is incorrect because the search warrant is valid. The SCA authorizes the government to obtain a warrant compelling disclosure of "information pertaining to a subscriber," 18 U.S.C. § 2703(c), and the keys specified in the warrant fall within that category.

A. The Search Warrant Was Properly Issued Under The Stored Communications Act.

In the event the Court reaches Lavabit's forfeited SCA claim, the Court should reject it. Contrary to Lavabit's contention, the SCA authorizes the government to obtain a warrant compelling disclosure of information – such as the key at issue here – as long as it "pertain[s] to a subscriber to or customer of" the electronic communication service by obtaining a warrant under the Federal Rules of Criminal Procedure or a "court order for such disclosure under subsection (d) of this section." 18 U.S.C. § 2703(c)(1)(A) and (B).

[10] Lavabit complains of a "flurry" of orders, Lavabit Br. at 28, and argues that the government's decision to issue the warrant was a concession that the pen/trap order by itself was inadequate, *id.* at 17. It was no such thing. As the record reflects, the government supplemented its pen/trap order with additional process only after Lavabit refused to obey prior court orders. This attempt to resolve the dispute and move forward with the investigation without requiring additional court intervention was not a concession.

Here, the government obtained a warrant. The warrant described the "property to be searched" as "information associated with [redacted] that is stored at premises controlled by Lavabit, LLC." J.A. 26. The warrant described the "particular things to be seized" in relevant part as:

> 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]

J.A. 27.

Lavabit argues that this information "do[es] not 'pertain[] to a subscriber.'" Lavabit Br. at 19. Whether the information described in the warrant pertains to a subscriber is a fact-intensive question. The result of Lavabit's failure to raise the issue below is that neither party had the opportunity to present evidence about whether the affidavit supported the warrant or established statutory authority to issue the warrant. *Volvo,* 386 F.3d at 603; *see also Sims v. Apfel,* 530 U.S. 103, 109 (2000) (requiring arguments to be presented first to the district court is "essential in order that litigants may not be surprised on appeal by final decision there of issues upon which they have had no opportunity to introduce evidence." (quoting *Hormel v. Helvering*, 312 U.S. 552, 556 (1941))).

Nonetheless, Lavabit appears to argue that a key could *never*, under any circumstances, pertain to a subscriber. This argument is wrong. Lavabit argues that the keys are "known to the company alone." Lavabit Br. at 19. But the statute authorizes the government to seek information that "pertains" to a customer, even if that information is not known to the customer. For instance, the statute authorizes the production of a list of Internet Protocol addresses that the subscriber used to connect to the service—information that the subscriber might not know. *See In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d),* 830 F. Supp. 2d 114, 120 (E.D. Va. 2011) ("A human user may not know the specific IP address assigned to his network connection …"). *See also In re Applications*, 509 F. Supp. 2d 76, 79-80 (D. Mass. 2007) (holding that historical cell tower data pertains to a subscriber). Lavabit also argues that the keys "are not specific to any given customer." Lavabit Br. at 19. But the statute describes information that "pertain[s] to a subscriber to or customer," not information that is "specific" to a "given" subscriber or customer. For example, § 2703(c) permits the government to acquire "telephone connection records," 18 U.S.C. § 2703(c)(2)(C), which will often contain telephone numbers of other customers and subscribers, and thus not be "specific" to one "given" subscriber or customer.

Finally, Lavabit relies on this Court's decision in *In re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d)*, 707 F.3d 283, 287 (4th Cir. 2013) (cited in Lavabit's Brief as *United States v. Appelbaum*), in arguing that § 2703(c) is limited to information about the subscriber, such as his "name, address, length of subscription, and other like data." Lavabit Br. at 19. But the scope of § 2703 was not before this Court in that case. Even so, when this Court described the breadth of the statute, the Court made clear that its list of records subject to § 2703 was illustrative, not exhaustive. *Id.* at 287 ("To obtain records of stored electronic communications, *such as* a subscriber's name, address, length of subscription, and other like data….") (emphasis added). More to the point, the decision in *In re Application* emphasized that the SCA was designed to "protect legitimate law enforcement needs" by "providing an avenue for law enforcement entities to compel a provider of electronic communication services to disclose the contents and records of electronic communications." *Id*. That design would be utterly frustrated if the statute were construed not to authorize warrants – despite a finding of probable cause by a neutral magistrate – to obtain information necessary to decrypt the relevant contents and records.

The search warrant was also lawfully issued under the Fourth Amendment because it sought to obtain property involved in crime. Lavabit argues that under the Fourth Amendment a search warrant may be used to obtain only the "fruits, instrumentalities, or evidence of crime," Lavabit Br. at 22, and that the private key did not fall into those categories, *id*. at 22-23 (citing *Zurcher v. Stanford Daily*, 436 U.S. 547, 554, 558 (1978)). But *Zurcher* did not hold that "fruits, instrumentalities, or evidence of a crime" are the only permissible objects of a search warrant. For instance, in *Warden v. Hayden*, the Supreme Court explained that "probable cause must be examined in terms of cause to believe that the evidence sought will aid in a particular *apprehension* or conviction." 387 U.S. 294, 307 (1967) (emphasis added). *See also In re Smartphone Geolocation Data Application*, --- F. Supp. 2d ---, 2013 WL 5583711, at *3 (E.D.N.Y. May 1, 2013) (holding that a warrant may issue for "information that reasonably could facilitate capture of the defendant"). Thus, so long as the government can demonstrate probable cause to believe that the compelled production of an encryption key will aid in the apprehension of a suspect or a conviction, the compelled production of an encryption key does not violate the Fourth Amendment. *See, e.g.*, *United States v. Thompson*, 495 F.2d 165, 169 (D.C. 1974) (holding apartment keys were lawfully seized as instrumentalities of narcotics distribution); *cf. Messerschmidt v. Millender*, 565 US ---, 126 S.Ct 1235, 1248 (2012) (rejecting argument that gang paraphernalia was not "evidence of crime" because such paraphernalia may establish motive, provide the foundation for additional charges, or be relevant to the impeachment of a witness at trial).

Regardless, as with Lavabit's SCA argument, Lavabit did not raise the issue of whether there was probable cause to support the warrant before the district court and that argument is therefore forfeited. To the extent that Lavabit is now arguing that a private key can *never* be the subject of a search warrant because such a key is not "fruits, instrumentalities, or evidence of crime," Lavabit Br. at 22, Lavabit is wrong. Magistrate judges routinely issue warrants that permit officers to copy encryption keys that permit the examination of other data that is seized as evidence. *See United States v. Scarfo*, 180 F. Supp. 2d 572, 574 (D.N.J. 2001) (two warrants authorized installation of keystroke loggers "in order to decipher the passphrase to the encrypted file, thereby gaining entry to the file"); *United States v. Sutton*, No. 5:08-CR-40, 2009 WL 481411, at *2 (M.D. Ga. Feb. 25, 2009) (warrant authorizing seizure of "encryption codes" that were "required to access computer programs or data"); *United States v. Simpson*, No. 3:09-CR-249, 2011 WL 721912, at *2 (N.D. Tex. Mar. 2, 2011) (warrant authorized seizure of encryption devices and passwords); U.S. Dep't Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence* (3d ed. 2009) at 249 (suggesting warrant language that would permit the seizure of "encryption keys, and other access devices that may be necessary to access" a seized hard drive). An encryption key could easily be used to encrypt a criminal communication, to encrypt evidence of a crime, or to encrypt the fruits of a crime. And a warrant may name any premises where such things are found — even if the premises are owned by someone other than the suspect or a private business such as Lavabit. *See Zurcher*, 436 U.S. at 554.

B. The Warrant Did Not Impose an Unreasonable Burden on Lavabit.

Lavabit argues that, even if valid, the search warrant was invalid because it imposed an undue burden on Lavabit. Lavabit Br. at 19-20. But the § 2703(d) "undue burden" standard only applies to "court orders" issued pursuant to 18 U.S.C. § 2703(c)(1)(B), not to search warrants issued pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c)(1)(A). However, as amicus American Civil Liberties Union correctly argues, "the Supreme Court has held that the courts may not impose unreasonable burdens in ordering third parties to assist in government investigations." ACLU Br. at 4 (citing *United States v. N.Y. Tel. Co*., 434 U.S. 159, 171 (1977)). The Supreme Court in *New York Telephone* upheld a court order requiring a service provider to assist with implementation of a pen register. The Supreme Court held that the order was not unduly burdensome because it "provided that the Company be fully reimbursed at prevailing rates, and compliance with it required minimal effort on the part of the Company and no disruption to its operations." *Id.* at 175. Even if Lavabit's erroneous invocation of the § 2703(d) standard was recast as a constitutional "unreasonable burden" claim, under that precedent the claim would fail.

Both the government and the district court upheld the obligation not to impose an undue burden on Lavabit. Lavabit argues that the subpoena and search warrant put Lavabit to "an existential crisis," denying Lavabit the ability to "*exist* as an honest company," and giving it no choice but to cease operations. Lavabit Br. at 29. But Lavabit's own privacy policy stated that Lavabit was willing to comply with court orders, so there was no dishonesty in complying with the orders of the district court. J.A. at 91. And Lavabit never warned the district court that its orders put Lavabit to an "existential crisis." In its Motion to Quash, Lavabit did not argue that it would have to cease operations if the district court denied its motion. At most, Lavabit asserted its business "could be destroyed if it is required to produce" the key, J.A. at 71-72, though Lavabit intimated the *coup de grâce* would come from loss of customer trust, rather than be self-inflicted within days of the district court's decision.

Instead, Lavabit's arguments to the district court identified a different, less burdensome way to comply with the district court's orders. As alternative relief, Lavabit asked the district court that it "be given an opportunity to revoke the current encryption key and reissue a new encryption key," and be compensated for the expense of doing so. J.A. 73. In other words, Lavabit did not, when it filed its motion, assess the burden as being so great that Lavabit would have to go out of business immediately. Rather, Lavabit sensibly proposed that, should it lose the motion it quash, it would turn over its key, and then obtain a new private key once the court-ordered pen/trap was complete. Doing so would have restored Lavabit to exactly the position it was in before it received any order from the government:

Lavabit, alone, would have the only copy of Lavabit's private key. The Government, in response, agreed that "once court-ordered surveillance is complete, Lavabit will be free to change its SSL keys," pointed out that a new private key might cost $100, and suggested that Lavabit would be entitled to compensation for that expense. J.A. 91.

Nothing in the search warrant required Lavabit to shut down. Nor was Lavabit ever under an obligation to "intentionally defraud its users about the security of the system." Lavabit Br. at 19. A provider does not defraud its users by both promising security and complying with lawful court orders. Lavabit publicly advised its users that Lavabit would comply with valid legal process. J.A. 91. Users who expected otherwise were not defrauded; at worst, they had the unreasonable belief that Lavabit was entitled to ignore court orders.

Lavabit argues that the warrant was unreasonable because it interfered with Lavabit's "business model," Br. at 12, but the Fourth Amendment does not provide special protection for business models based on a refusal to cooperate with lawful criminal investigations. For example, a bank that refused to comply with lawful subpoenas could no doubt build a lucrative business from customers seeking to avoid governmental scrutiny. The Fourth Amendment, however, does not protect a business model that conflicts with "the longstanding principle that the public has a right to every man's evidence." *Branzburg v. Hayes*, 408 U.S. 665, 688 (1972) (internal quotation marks and ellipses omitted). Lawful process that disrupts such a business model does not impose an unreasonable burden.

Finally, Lavabit also argues that the burdens imposed on it were unreasonable because Lavabit offered to implement the pen/trap itself, with its own software, making it unnecessary for the government to obtain the private key. Lavabit Br. at 8, 20. To be sure, in most cases, when government agents serve a provider with a pen/trap order, they are happy to let the provider use its own equipment and software to implement the order. Lavabit also had that option on June 28, the day it was served with the pen/trap order. But Lavabit did not implement its own pen/trap. Eight days later, on July 6, Lavabit still had not implemented its own pen/trap, giving the government's agent the non-sequitur reply that "we don't record this data." J.A. 81. Twelve days after receiving the pen/trap order, Lavabit participated in a conference call with the government, and had consulted with counsel, but otherwise had done nothing to implement the pen/trap. J.A. 82. The next day, FBI agents attempted to serve Lavabit's proprietor, Mr. Levison, with a subpoena, but, after knocking on his door, witnessed him exit his apartment, get in his car, and drive away. J.A. 82.

The "offer" to implement the pen/trap finally came on July 13, 2013, fifteen days after service of the pen/trap order. That offer fell well short of what the court had ordered Lavabit to do: For an advance payment of $2000, Lavabit offered to provide all of the data "at the conclusion of the 60 day period." Levison offered to provide the data "intermittently during the collection period but only as my schedule allows." If the government wanted more frequent production, Lavabit demanded a flat figure of $1500. J.A. 83. Thus, fifteen days after receiving the order, Lavabit revealed it had not even begun to comply, and only offered to produce data intermittently at best. At the August 1 hearing, thirty-four days after the pen/trap order had been served, Lavabit's counsel represented that Lavabit's work on implementing its own pen/trap still had not begun. J.A. 112. Counsel offered that once Lavabit began work on writing the necessary computer code, it would take "a week to a week and a half" before it would be ready, "although I would be willing to talk to my client to see if we can get that expedited." J.A. 112.

It was not error for the district court to order production of Lavabit's private keys despite this "offer." The offer came after almost a quarter of the allotted time for the pen/trap order had evaporated, perhaps along with crucial investigative opportunities. Lavabit requested compensation without offering any basis to evaluate whether that compensation was reasonable, in exchange for doing less than what the pen/trap order required. Lavabit made this offer just three days after its proprietor avoided agents attempting to serve process. Thirty-four days into the order, Lavabit still had done no work to implement its own solution, and Lavabit's counsel conceded that the proposed pace of work was not "expedited." From all this, the district court was entitled to conclude that Lavabit was either incapable of implementing its own pen/trap, or simply unwilling.

IV. THE FOURTH AMENDMENT DOES NOT PROHIBIT OBTAINING ENCRYPTION KEYS FOR THE PURPOSE OF DECRYPTING COMMUNICATIONS THAT THE GOVERNMENT IS LAWFULLY AUTHORIZED TO COLLECT.

Lavabit's final argument is that the requirement to produce the encryption keys violated the Fourth Amendment because, with the keys, the government would have the ability (though not the authority) to review other Lavabit users' data. Lavabit's argument, in essence, is that since it would be theoretically possible for the government to use Lavabit's encryption keys to decrypt and read the contents of electronic communications of all of Lavabit's users, any warrant requiring Lavabit to disclose the encryption keys is unreasonable under the Fourth Amendment. This argument is wrong.

First, there is no doubt that the warrant was sufficiently particular. "The 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 warrant's specification easily met that standard: it asked for information necessary to decrypt the communications of one Lavabit user. When Lavabit finally complied with the warrant, it had no difficulty identifying the exact data called for by the warrant.

The warrant, then, was not defective for describing the data to be produced in a vague, broad fashion.

Second, the search warrant did not authorize "rummag[ing]" through the communications of all Lavabit users. Lavabit Br. at 21-24, 27. Nor, for that matter, did the government "propos[e] to examine the correspondence of all of Lavabit's customers," *id.* at 12, seek to "gain unfettered access to all—*all*—of the data," *id.* at 21, or to "expose and search through the content and non-content data of all [Lavabit] users," *id.* at 26. Lavabit conflates information that would actually be seen by a human investigator with data that would momentarily pass through the pen/trap device's memory before a computer forever discarded it. *Id.* at 27. The only user data the government was permitted to see was the data described in the pen/trap order and the search warrant; all other data would be filtered out, electronically, without reaching any human eye. If certain data did not pertain to the one identified user, the government could not read it; if there were encryption keys used to encrypt information other than that particular account, the government could not use them.

Lavabit's use of a single lock to secure all its users communications does not mean the government's procurement of Lavabit's key for the purpose of inspecting one user's communications is overbroad. Lavabit used a single set of keys to encrypt all users' communications. Lavabit Br. at 4. Lavabit's analogy – that the government demanded the master key to every room in a hotel when it had authority to search only a single room – is based on a false premise. In Lavabit's analogy, there is a unique key to the room the government sought to search. Here, no such unique key existed – there was only a master key. That does not invalidate a lawful warrant to obtain such a key, physical or digital; indeed, the taking of keys pursuant to a lawful search for the purpose of opening other locked items is both well-established and routine. *See, e.g.*, *United States v. Herrera-Contreras*, 269 Fed. App'x 875, 2008 WL 656242, at *1 (11th Cir. Mar. 12, 2008) (holding that key seized during a lawful arrest could be used to unlock a closet in the course of executing a warrant); *United States v. Grossman*, 400 F.3d 212, 216-18 (4th Cir. 2005) (discussing seizure of a criminal suspect's keys as part of an effort to search various residences); *United States v. Horn*, 187 F.3d 781, 787-88 (8th Cir. 1999) (holding that warrant authorizing seizure of "any and all … keys … showing access to, or control of" a residence was not unconstitutionally overbroad); *United States v. Otobo*, 1993 WL 196053, at *3 (6th Cir. June 9, 1993) (per curiam) (unpublished); *United States v. Peagler*, 847 F.2d 756, 756 (11th Cir. 1988) (per curiam); *Thompson*, 495 F.2d at 169 (holding apartment keys were lawfully seized as instrumentalities of narcotics distribution).[11]

[11] Nor would the use of a pen/trap device to electronically scan traffic on Lavabit's network constitute an unconstitutional search or seizure. The use of a pen register device on an email account is not a search. *See Forrester*, 512 F.3d at 509.

Third, Lavabit's parade of hypotheticals regarding other possible unlawful actions the government might take with the fruits of a lawfully executed search warrant should not invalidate a warrant issued by a neutral magistrate based on probable cause. Statutes, such as the Wiretap Act, 18 U.S.C. § 2510 *et seq.*, and the Pen/Trap statute itself, 18 U.S.C. § 3121, strictly regulate the government's ability to conduct electronic surveillance. Were a government officer to do as Lavabit fears and "rummage" through other users' communications without authorization, that would be a crime. Conjecture that the government will execute a search warrant illegally is not grounds to invalidate a warrant. *See Dalia v. United States*, 441 U.S. 238, 257 (1979) ("Nothing in the language of the Constitution or in this Court's decisions interpreting that language suggests that …

Federal courts have refused to apply Fourth Amendment protection to envelope information. In *United States v. Huie*, the United States Court of Appeals for the Fifth Circuit held that United States Postal Service customers had no reasonable expectation to privacy in information placed on the outside of mailing envelopes. 593 F.2d 14, 15 (5th Cir. 1979). Applying the same rationale, the Supreme Court held that telephone users had no reasonable expectation of privacy in dialed telephone numbers, since dialing a telephone to connect a call reveals those numbers to the telephone service provider. *See Smith v. Maryland*, 442 U.S. 735, 742-44 (1978)("Given a pen register's limited capabilities, therefore, petitioner's argument that its installation and use constituted a 'search' necessarily rests upon a claim that he had a 'legitimate expectation of privacy' regarding the numbers he dialed on his phone. This claim must be rejected."). Several courts have used the same analysis in holding that non-content information disclosed to Internet service providers should not be afforded Fourth Amendment protections. *See, e.g.*, *Forrester*, 512 F.3d at 509-13; *Guest v. Leis*, 255 F.3d 325, 335-36 (6th Cir. 2001); *United States v. Hambrick*, 55 F. Supp. 2d 504, 508-09 (W.D. Va. 1999), *aff'd*, 225 F.2d 656 (4th Cir. August 3, 2000).

search warrants also must include a specification of the precise manner in which they are to be executed."); *see also United States v. Grubbs*, 547 U.S. 90, 97-98 (2006) (noting that Fourth Amendment's particularity requirement is limited to places to be searched and things to be seized). Lavabit's claim is even more speculative than the Defendant's claim rejected by the Supreme Court in *Dalia.* In *Dalia*, the Supreme Court rejected the argument that a warrant must contain restrictions on the manner of its execution to be consistent with the Fourth Amendment. *Id*. at 259. Lavabit's claim is that, regardless of how the actual search is conducted, to comply with the Fourth Amendment a warrant must also contain other, unidentified restrictions on future anticipated government action.

Taken to its logical extension, Lavabit's argument could be used to invalidate any investigative action taken by the government. Rogue agents might abuse any pen/trap device, for example, to illegally and surreptitiously collect data related to phone numbers or email accounts not listed in the authorizing order. The authority granted by a warrant to search a specific physical location for specific evidence could be exceeded by executing government agents. A law enforcement officer could use a search warrant to lawfully seize a weapon and later use the weapon in a crime. The possibilities are only limited by the imagination. Courts do not and should not invalidate warrants based on speculation; rather, whether a particular government act violates the Fourth Amendment requires actual facts –

not just the possibility for harm. *See Richards v. Wisconsin*, 520 U.S. 385, 395-96 (1997); *see also* Orin Kerr, "Ex Ante Regulation of Computer Search and Seizure," 96 Va. L. Rev. 1241, 1260-76 (2010) (discussing Supreme Court disapproval for evaluation of search warrants based on hypothetical government action). Here, where Lavabit's only claims of government overreaching are based on conjecture that federal agents will commit crimes, Lavabit's Fourth Amendment challenges to the search warrant and pen/trap order should be denied.

CONCLUSION

The United States has a compelling interest in the investigation and prosecution of crime. *See Va. Dep't of State Police v. Wash. Post*, 386 F.3d 567, 578 (4th Cir. 2004). Congress has passed numerous statutes, including the Stored Communications Act and the Pen/Trap statute, which further that interest by authorizing the collection of certain information from providers of electronic communication. Congress has ensured investigations stay true to those statutes by providing oversight by the courts. Here, Lavabit claims the right to ignore those courts and thwart such investigations simply by offering for sale, to the general public, encrypted email. Because there is no reason to treat a business that offers encrypted email services differently from any other business, this Court should affirm the district court's order for sanctions.

Respectfully submitted,

DANA J. BOENTE
ACTING United States Attorney

MICHAEL BEN'ARY
ANDREW PETERSON
JAMES L. TRUMP

United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314
(703) 299-3700

MYTHILI RAMAN
ACTING ASSISTANT ATTORNEY
GENERAL, CRIMINAL DIVISION

NATHAN JUDISH
JOSH GOLDFOOT
BENJAMIN FITZPATRICK
BRANDON VAN GRACK

U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

/s/ Andrew Peterson
ANDREW PETERSON
ASSISTANT UNITED STATES ATTORNEY
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314
(703) 299-3700

CERTIFICATE OF COMPLIANCE

Pursuant to this Court's order dated, I hereby certify that that this brief contains 11,685 words (excluding the parts of the brief exempted by Rule 32(a)(7)(B)(iii)) and has been prepared in a proportionally spaced, 14-point typeface using Microsoft Word 2010.

/s/ Andrew Peterson
Andrew Peterson

CERTIFICATE OF SERVICE

I hereby certify that on November 12, 2013, I filed the foregoing Brief of the United States of America with the Clerk of the Court using the CM/ECF system, which will send a Notice of Electronic Filing to the following registered users:

Jesse Ryan Binnall
Email: jbinnall@bblawonline.com
Bronley & Binnall, PLLC
10387 Main Street
Fairfax, VA 22030-0000

Marcia C. Hofmann
Email: marcia@marciahofmann.com
Law Office of Marcia Hofmann
25 Taylor Street
San Francisco, CA 94102

Laurin Howard Mills
Email: laurin.mills@leclairryan.com
Leclair Ryan, PC
2318 Mill Road
Alexandria, VA 22314-0000

Ian James Samuel
Email: isamuel@jonesday.com
290 West 12th Street
New York, NY 10014

David Alan Warrington, Esq.
Email: david.warrington@leclairryan.com
Leclair Ryan, PC
Suite 1100
2318 Mill Road
Alexandria, VA 22314-0000

/s/ Andrew Peterson
Andrew Peterson