RECORD NO. 13-4625(L); 13-4626

In The

United States Court Of Appeals

For The Fourth Circuit

In re: GRAND JURY PROCEEDINGS,

UNITED STATES OF AMERICA,

Plaintiff – Appellee

v.

UNDER SEAL,

Party-in-Interest – Appellant.

**ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
AT ALEXANDRIA**

BRIEF OF APPELLANT

Jesse R. Binnall
BRONLEY & BINNALL, PLLC
10387 Main Street
Suite 201
Fairfax, VA 22030
(703) 647-5926

Counsel for Party in Interest-Appellant

Ian Samuel
ATTORNEY AT LAW
290 W. 12th Street
Apt. 3B
New York, NY 10014
(917) 803-8609

Counsel for Party in Interest-Appellant

Marcia Hofmann
LAW OFFICE OF MARCIA HOFMANN
25 Taylor Street
San Francisco, CA 94102
(415) 830-6664

Counsel for Party in Interest-Appellant

David Warrington
Laurin Mills
LECLAIRRYAN
2318 Mill Road
Suite 1100
Alexandria, VA 22314
(703) 647-5926

Counsel for Party in Interest-Appellant

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is **not** required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. 13-4625 Caption: In re: UNDER SEAL, UNITED STATES OF AMERICA v. UNDER SEAL

Pursuant to FRAP 26.1 and Local Rule 26.1,

UNDER SEAL
(name of party/amicus)

who is Party-in-Interest- Appellant, makes the following disclosure:
(appellant/appellee/amicus)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☑ NO
If yes, identify all parent corporations, including grandparent and great-grandparent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(b))? ☐YES ☑NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐YES ☑NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐YES ☑NO
If yes, identify any trustee and the members of any creditors' committee:

Signature: /s/ Jesse R. Binnall Date: 10/10/2013

Counsel for: Party-in-Interest-Appellant

CERTIFICATE OF SERVICE

****

I certify that on October 10, 2013 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

James Trump
Assistant United States Attorney
United States Attorney's Office
Justin W. Williams U.S. Attorney's Building
2100 Jamieson Avenue
Alexandria, VA 22314

Michael Ben'Ary
United States Attorney's Building
2100 Jamieson Avenue
Alexandria, VA 22314

/s/ Jesse R. Binnall
(signature)

October 10, 2013
(date)

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases:

Statues:

Rule:

Other Authority:

JURISDICTION

Lavabit is an e-mail service provider, and this case arises out of a criminal investigation into one of its customers. In the course of that investigation, Lavabit was ordered to disclose the company's private encryption keys, which it refused to do. The district court held Lavabit in contempt on August 5, 2013. App. 132-133. The district court had jurisdiction under 28 U.S.C. § 1331. This appeal was timely noted. App. 134-135, 136-137, 138-139. This court has jurisdiction because the contempt order is a "final decision of [a] district court[] of the United States." 28 U.S.C. §1291.[1]

---

[1] A "final decision" generally "ends the litigation on the merits and leaves nothing for the court to do but execute the judgment." *United States* v. *Myers*, 593 F.3d 338, 344 (4th Cir. 2010) (quoting *Catlin* v. *United States*, 324 U.S. 229, 233 (1945)). The usual rule is therefore that "a party to litigation may not immediately appeal a civil contempt order." *Myers*, 593 F.3d., at 344. "A civil-contempt order may be immediately appealed by a nonparty," however, and is treated under those circumstances as a final decision for purposes of §1291. *Id.* at 344 n.9.

The contempt order issued here is of that latter type. Lavabit is not a target or a subject of the government's investigation. The government's criminal investigation is into one of Lavabit's *customers*—neither Lavabit nor its owner, Mr. Levison, is charged with or suspected of any crime. When a disinterested third party such as Lavabit is commanded to produce evidence but "disobey[s] and is committed for contempt," the "situation becomes so severed from the main proceeding as to permit an appeal." *Cobbledick* v. *United States*, 309 U.S. 323, 328 (1940). To disallow an appeal in those circumstances "would forever preclude review," and the Supreme Court has therefore explicitly approved whatever "interruption of the trial or of the investigation" may result from a full appellate airing of the third-party witness' claim. *Ibid.* To "defy a disclosure order and incur court-imposed sanctions" is a "long-recognized option" for securing immediate appellate review, which is precisely what Lavabit did. *Mohawk Indus.* v. *Carpenter*, 558 U.S. 100, 111 (2009). See also, *e.g.*, *In re Grand Jury Subpoena (T-112)*, 597 F.3d 189, 191 (4th Cir. 2010) (resolving, on the merits, an appeal of "a district court decision holding [appellants] in civil contempt" after they refused to comply with grand jury subpoenas *duces tecum*).

STATEMENT OF THE ISSUES

Whether the government may seize a business' private encryption keys, which would enable covert surveillance of all of that business' customers, when neither the business nor the overwhelming majority of its customers are suspected of any wrongdoing.

STATEMENT OF THE CASE

Appellants moved to quash several orders requiring the disclosure of certain private encryption keys to the government. The district court denied that motion. After appellants did not provide the encryption keys in electronic format, the district court found appellants in contempt, and imposed a fine of $5,000 per day until appellants did so. This appeal followed.

STATEMENT OF FACTS

A. Lavabit's Email Service

Lavabit was a small business that provided secure email to its paying customers. It did so in a marketplace crowded with large, low-cost email providers, such as Gmail and Yahoo! Mail. But Lavabit's service was unique because its technical design offered its paying customers an unparalleled degree of security and privacy. Unlike companies such as Google, which "profile[] user's inboxes for targeted advertising," or AT&T,

---

In the alternative, if this Court concludes that it does not have jurisdiction under §1291, then it should treat this appeal as a petition for mandamus. See *Mohawk Indus.*, 558 U.S. at 111.

which had allowed "the government to tap phone calls without a court warrant," Lavabit developed an email service that "prevent[ed] everyone, including [Lavabit], from reading the e-mail of the people that use it." *Security Through Asymmetric Encryption*, http://lavabit.com/secure.html (archived version, January 15, 2013; available at http://web.archive.org).[2] And there was a substantial market for this service. At its height, Lavabit had more than 400,000 users. App. 67, 70, 104.

The details of Lavabit's secure email service are technically complex, but the general concepts are not. Lavabit relied on two forms of security to protect its paying customers' privacy. First, customers' email was encrypted before it was stored on Lavabit's servers, which prevented anyone from reading the customer's stored messages without the customer's password—including Lavabit. Second, Lavabit used an industry-standard security measure to ensure that all communications between Lavabit's email servers and its customers were encrypted in transit, so that when a customer was actually in the process of sending and receiving communications from Lavabit's servers, a third party would be unable to observe that information as it traveled over the Internet. It is the second type of privacy protection that is chiefly at issue in this appeal.

[2] In response to the government's conduct in this case, Lavabit ceased operations, and its website has been taken offline. An archived version of the company's site is referenced in this brief for the sake of exposition about the nature of Lavabit's service.

Lavabit's communications with its customers were protected using what is known as SSL encryption.[3] This is a form of encryption in which the message is encoded with one key but decoded with a different key. Customers encrypted their communications to Lavabit's servers using the company's public SSL keys, which (as the name suggests) are known to all. But once those communications reached Lavabit, they could only be decrypted using the company's private keys, which were closely guarded secrets and known only to the company. (For the sake of brevity, we will refer to those latter types of keys as the company's private keys.) Due to the nature of SSL public-key encryption, Lavabit's private keys were used to decrypt all customer communications. They were also used by the company for other purposes: for example, to securely sign communications or software distributed by the company, such that a customer could be sure that a given communication or piece of software really did originate with Lavabit.

In other words, Lavabit's private keys were the company's cryptographic crown jewels: master keys with which anyone could intercept and listen in on the company's communications with any and all of its customers. As one court has noted, "in the absence of a secured communication protocol such as SSL, Internet communications are similar to the 'party line' style of telephone communications, as any person could

[3] The SSL protocol is "widely considered to be the standard method for conducting secured communications via the Internet." *Stambler v. RSA Sec., Inc.*, No. Civ.A. 01-0065-SLR, 2003 WL 22749855, at *2 (D. Del. Nov. 14, 2003).

'listen in' on the communications between individuals." *Stambler*, 2003 WL 22749855, at *2 n.1. To say that such keys are closely guarded secrets is an understatement. If a business has reason to suspect that its private keys have been compromised, that business is generally obligated to inform the certifying authorities that signed the keys,[4] as well as its business partners and customers.[5] The information is especially sensitive in Lavabit's case, because its entire business model relied on providing secure email services.

B. The Government's Investigation Into Lavabit's Customer

This case arises out of an investigation into one of Lavabit's customers.[6]

[redacted]

[4] In fact, after the government's conduct in this case became public, the authority responsible for issuing Lavabit's cryptographic keys promptly revoked them—that is, informed the public that those keys were invalid and could no longer be trusted or used. See Kashmir Hill, GoDaddy Pulls Lavabit's Security Creds Because the FBI Got Ahold of Its Encryption Keys, Forbes, Oct. 9, 2013, http://www.forbes.com/sites/kashmirhill/2013/10/09/godaddy-pulls-lavabits-security-creds-because-the-government-got-ahold-of-its-encryption-keys/ (noting that "industry policies" require exactly this).

[5] The majority of states have laws that require companies to report security breaches that expose consumers' personal information. Texas, for example, requires companies to notify state residents when their unencrypted sensitive personal information is reasonably believed to have been acquired by an unauthorized person. Tex. Bus. & Comm. Code Ann. §§ 521.002 & 521.053. This reporting requirement extends to situations in which encrypted data has been acquired when the unauthorized person accessing the data has the key to decrypt it. Tex. Bus. & Comm. Code Ann. § 521.053.

[6] The customer's identity remains under seal.

[redacted]. Lavabit was then served with a grand jury subpoena to produce billing and subscriber information about the target customer's account. App. 23, 25-28. Lavabit provided this information to the government. App. 80. This was in accord with the company's privacy policy, which notified users that Lavabit would disclose information related "to an *individual* user" to the government, if the company were "legally compelled" to do so. *Privacy Policy*, http://lavabit.com/privacy_policy.html (archived version, January 15, 2013; available at http://web.archive.org) (emphasis added). Indeed, one of the purposes of limiting the secure email service to Lavabit's paying customers was to provide a paper trail to identify that customer, should the account be used for unlawful purposes. See *Security Through Asymmetric Encryption*, http://lavabit.com/secure.html (archived version, January 15, 2013; available at http://web.archive.org).

The government then sought an order, which we will refer to as the "Pen Trap Order," pursuant to 18 U.S.C. §§3121–3127. This order authorized the installation of a device (called a pen-trap device) on Lavabit's servers, which would monitor all non-content (or "metadata") information sent between Lavabit and the target customer—that is, routing and addressing information, as well as the date and time of the customer's communications, but not the content of the customer's emails. App. 10-12. As detailed above, however, communications between Lavabit's email servers and its secure-email customers are encrypted. This means the government would not be able to determine which customer the company was communicating with at any given time

or what was being said. Lavabit told the government as much. App. 132. Though Lavabit could and did provide the customer's billing and subscriber information, the nature of its business and the technical design of its system prevented it from being able to do more.

In response, the government orally commanded Lavabit to turn over the company's private keys to the government. That would have allowed the government to decrypt and intercept *all* encrypted communications that were sent between Lavabit and its customers, examine those communications to determine which connections were with the target customer, and then gather the non-content data that the Pen-Trap Order authorized. Of course, it would also (as detailed above) allow a great deal more: it would enable the government to monitor the metadata, passwords, credit card information *and content* of all communications between Lavabit and all of its customers, or even masquerade as the company if it chose to do so. Moreover, the government forbade Lavabit from telling anyone that it had compromised its security in this way: not its customers, not its business partners, and not the relevant cryptographic authorities. The government insisted that all of those parties be affirmatively misled into believing that the system remained secure against exactly the kind of secret monitoring that the government was proposing to do. See App. 1-2, 11-12, [redacted]

Lavabit refused to comply with this demand for many reasons—not the least of which was that neither the Pen-Trap Order nor a subsequent "compliance order" (issued the same day) required the company to do so. See App. 8-9, 10-12. In response to Lavabit's refusal, the government secured an order commanding the company's owner, Mr. Levison, to personally appear in a district court over a thousand miles away from his home and explain his refusal to produce this information. App. 13-14. The government then secured a grand jury subpoena, which explicitly commanded Mr. Levison to appear before the grand jury and bring with him Lavabit's private keys. App. 23.

Before Mr. Levison's appearance, and in response to the government's blizzard of dubious court orders, Lavabit proposed a compromise: the company could itself record the non-content information related to the target of the government investigation—that is, Lavabit could record and turn over the target's "login and subsequent logout date and time, the IP address used to connect," and "non-content headers … from any future emails sent or received using the subject account." App. 83. Lavabit proposed to turn the logged information over at the conclusion of the court-ordered surveillance period or to provide it on a daily basis. App. 83. This solution—though more than Lavabit thought the law obligated it to do, and one with which the company felt profound discomfort—would have given the government the information to which it was entitled without requiring the company to turn over its private keys, thereby protecting the privacy of its other customers.

The government refused, on the basis that Lavabit's proposed solution would not have given it "real-time access" to the target customer's data. App. 83. After refusing Lavabit's compromise, and betraying a well-grounded skepticism about the legal basis for its prior demands, the government secured a warrant under the Stored Communications Act, which again commanded Lavabit to hand over its private keys, while again gagging Lavabit from telling anyone that the government had done so. App. 118-119, [redacted] The government did this while Mr. Levison was traveling from Dallas to Virginia to appear, *pro se*, in district court, to "show cause" for his prior refusal of the government's demands. App. 39-40.

At that appearance, Mr. Levison made it clear that he had no objection to the government's lawful installation of the pen-trap device—only to the provision of his company's private keys, "because that would compromise all of the secure communications in and out of my network." App. 42, 48. The district court, satisfied with that much for the moment (and aware of Mr. Levison's status as a then-unrepresented litigant), scheduled another hearing to determine the propriety of providing the private keys. App. 47, 50-51. Very shortly after the hearing, the government served Lavabit with the Stored Communications Act warrant.

Lavabit moved to quash all of the court orders requiring it to turn over its private encryption keys. App. 66, 73. Lavabit argued that requiring it to turn over those keys was inconsistent with the Fourth Amendment, that the keys were not material to the government's investigation, and that providing them in response to a

subpoena would be unduly burdensome and oppressive. Following a hearing, the district court denied Lavabit's motion and gave the company 24 hours to turn over the keys. App. 116, 118-119. After Lavabit did not provide the keys in electronic format within that time, the district court held Lavabit in civil contempt, commanding it to pay $5,000 per day until it provided the keys in electronic form. App. 132, 133.

Faced with what it regarded as a decision "to become complicit in crimes against the American people or walk away from nearly ten years of hard work," Lavabit provided its private keys to the government—but also shut down its service entirely, believing that it could not operate the service in good faith while the government had the ability to secretly spy on the very customers who had paid Lavabit to secure them against just that. Lavabit, http://lavabit.com/ (accessed September 24, 2013) ("This experience has taught me one very important lesson: without congressional action or a strong judicial precedent, I would *strongly* recommend against anyone trusting their private data to a company with physical ties to the United States."). The government would still be able to use Lavabit's private keys to decrypt and access data that it had already intercepted (including customers' usernames, passwords, and the contents of their emails), but Lavabit was forbidden from communicating this security breach to its customers or business partners.

This appeal timely followed. App. 134-135, 136-137, 138-139.

SUMMARY OF ARGUMENT

The orders requiring Lavabit to produce its private keys were unlawful. In district court, the government relied on what can charitably be described as a mélange of theories; at turns, the government argued that it was entitled to Lavabit's private keys by virtue of the Pen Register Statute, the Stored Communications Act, and a grand jury subpoena. Each of those theories is completely without merit. The district court's order of contempt should be vacated and this case remanded for further proceedings consistent with that conclusion.

First, the government is bereft of any statutory authority to command the production of Lavabit's private keys. The Pen Register 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*. Moreover, providing private keys is not "unobtrusive," as the statute requires, and results in interference with Lavabit's services, which the statute forbids. Nor does the Stored Communications Act authorize the government to seize a company's private keys. It permits seizure of the contents of an electronic communication (which private keys are not), or information pertaining *to a subscriber* (which private keys are also, by definition, not). And at any rate it does not authorize the government to impose undue burdens on the innocent target business, which the government's course of conduct here surely did.

Second, the Fourth Amendment independently prohibited what the government did here. The Fourth Amendment requires a warrant to be founded on probable cause that a search will uncover fruits, instrumentalities, or evidence of a crime. But Lavabit's private keys are none of those things: they are lawful to possess and use, they were known only to Lavabit and never used by the company to commit a crime, and they do not prove that any crime occurred. In addition, the government's proposal to examine the correspondence of all of Lavabit's customers as it searched for information about its target was both beyond the scope of the probable cause it demonstrated and inconsistent with the Fourth Amendment's particularity requirement, and it completely undermines Lavabit's lawful business model. General rummaging through all of an innocent business' communications with all of its customers is at the very core of what the Fourth Amendment prohibits.

Finally, the grand jury subpoena was oppressive, unduly burdensome, and ought to have been quashed. Compliance with the subpoena inflicted grave harm on Lavabit. It was required either to cease operations entirely or perpetrate a massive commercial fraud on its customers and business partners, by lying to them about the security of services that were purchased *because* of their security. While the grand jury's investigative powers are broad, courts have never hesitated to quash subpoenas that intrude so gravely on the interests of innocent people. To commercially ruin a third-party small business using a grand jury subpoena is *per se* oppressive—indeed is close to the Platonic ideal of an unreasonable demand that

ought to have been promptly quashed, especially in light of Lavabit's ability to provide the government with the information to which it was entitled by other, far less intrusive, means.

ARGUMENT

Standard of Review

A district court's legal conclusions are reviewed de novo. *United States v. Mehta*, 594 F.3d 227, 281 (4th Cir. 2010). A district court's refusal to modify or quash a subpoena is reviewed for abuse of discretion. *In re Grand Jury Subpoena John Doe, No. 05GJ1318*, 584 F.3d 175, 182 (4th Cir. 2009).

Discussion of the Issues

An "individual appealing a contempt order" may challenge both "whether contempt was proper" and the propriety of "the order alleged to have been violated" (so long as "earlier appellate review" of that underlying order was unavailable). *United States* v. *Myers*, 593 F.3d 338, 344 (4th Cir. 2010). See also *United States* v. *Ryan*, 402 U.S. 530, 532 (1971) (when a discovery order is "unduly burdensome or otherwise unlawful," its target may "refuse to comply and litigate those questions in the event that contempt or similar proceedings are brought against him"). Earlier appellate review was not available here, and Lavabit is therefore pursuing this appeal to challenge the underlying disclosure orders.

A. The Government Has No Statutory Authority To Command the Production of Lavabit's Private Keys

1. The Pen Register Statute Does Not Authorize Seizing Private Keys

The government argued initially that Lavabit was required to produce its encryption keys by virtue of the Pen-Trap Order and a follow-on compliance order. App. 8-9, 11. Specifically, Lavabit was commanded to provide the government all technical assistance necessary to accomplish the installation and use of the pen-trap device. App. 8. But those orders were lawful only to the extent they were statutorily authorized. And the enabling statute, the Pen Register Statute, only requires third parties to "furnish … all information, facilities, and technical assistance necessary to accomplish *the installation* of the pen register *unobtrusively*," once the government is "authorized to install and use a pen register," so that there is "a minimum of interference with the services" that the third party provides to the target of the investigation. 18 U.S.C. §3124(a) (emphasis added). See also 18 U.S.C. §3124(b) (setting forth an identical standard for the installation of a trap-and-trace device). A service provider might thus be required, for example, to tell the government which cables carry the relevant communications, so that the government can attach the device correctly.

The plain language of §3124(a) requires only that a third party provide information that is necessary to the "installation" of a pen-trap device. And Congress further limited the government's power to demand third-party assistance

to only that information which would be required to make the installation of a pen register "unobtrusive[]," such that the target of the investigation would not detect any "interference" with the service—thereby, perhaps, alerting the target to the investigation. Encryption keys are not necessary to install the device unobtrusively, and are not needed to avoid interference with the service. (That is amply demonstrated here, because the government successfully installed the pen-trap device before obtaining Lavabit's private keys.)

What the government has argued is, in essence, that an innocent third party must provide whatever information might hypothetically be needed to make the government's use of a pen-trap device *effective*—but that is not what the statute says.[7] Congress commanded assistance with the installation of a pen register

[7] Nor is Lavabit under any general obligation to operate an email service that is easy to wiretap. Congress has explicitly carved out email service providers from that sort of statutory obligation, which does exist for other businesses. The Communications Assistance for Law Enforcement Act requires most telecommunications carriers to ensure their equipment, facilities, and services are capable of intercepting users' communications and accessing call-identifying information for law enforcement purposes. 47 U.S.C. §1002(a). But Congress chose not to extend this requirement to providers of "information services," including email service providers. *Id.* at §1002(b)(2); §1001(6)(B)(iii) (definition of "information services" includes "electronic messaging services"). Thus, Lavabit has no legal obligation to design its facilities or services to accommodate law enforcement.

Nor does Lavabit have any legal duty to retain records about its customers, as businesses in more highly regulated industries do. See, *e.g.*, the Bank Secrecy Act, 12 U.S.C. §1829(b) (imposing recordkeeping transactions on federally insured depository institutions).

device, not its use or operation—and when "interpreting a statute," there is "one, cardinal canon" that stands "before all others": Congress "says in a statute what it means and means in a statute what it says there." *Conn. Nat'l Bank v. Germain*, 503 U.S. 249, 253–54 (1992). See also *Brown* v. *Waddell*, 50 F. 3d 285, 290–91 (4th Cir. 1995) (interpreting the pen register statute in line with its "plain textual meaning").

Moreover, reading §3124's broad language to authorize seizure of a company's private keys is inconsistent with the principle that Congress "does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions—it does not, one might say, hide elephants in mouseholes." *Whitman* v. *Am. Trucking Ass'n, Inc.*, 531 U.S. 457, 468 (2001). As discussed below, for a company built on secure email services to surrender its private keys to an untrusted third party is a truly dramatic act, akin to requiring a hotel to turn over a master key to all of its hotel rooms (or install clear glass doors on those rooms)—or, for that matter, commanding the City of Richmond to give the police a key to every house within the city limits. It is unthinkable that Congress would have given the government the authority to seize keys that would make it possible to intercept *all* of Lavabit's communications with *all* of its customers—communications that the

customers have been told *are private against exactly that kind of secret surveillance*—except in the clearest possible words.[8]

The Pen Register Statute does not come close. An anodyne mandate to provide information needed merely for the "unobtrusive installation" of a device will not do. If there is any doubt, this Court should construe the statute in light of the serious constitutional concerns discussed below, to give effect to the "principle of constitutional avoidance" that requires this Court to avoid constructions of statutes that raise colorable constitutional difficulties. *Norfolk S. Ry. Co.* v. *City of Alexandria*, 608 F.3d 150, 156–57 (4th Cir. 2010).

2. The Stored Communications Act Does Not Authorize Seizing Private Keys

Sensing (correctly) that the Pen Register Statute could not bear the weight of its demands for Lavabit's private keys, the government also secured a warrant for those keys pursuant to the Stored Communications Act, 18 U.S.C. §2703. App. 25-29. Even

[8] Moreover, the assistance demanded by the government here was neither "unobtrusive" nor accomplished with a "minimum of interference" with Lavabit's services. See 18 U.S.C. §3124(a). It eviscerated the basic purpose of the company: to provide an email service that protects the privacy and security of users' communications, which remains a legitimate objective in a free society.

Customers chose to use Lavabit's service because they wanted to protect their privacy, and Lavabit made public commitments to protect those interests and had contractual obligations to its customers to do so. The government's demand that Lavabit turn over its private keys gutted the entire premise the company was built on, and Lavabit would have lost its customers as a result of complying with it. Compare *Company* v. *United States*, No. 02-15635, 2009 WL 3957906, at **9-10 (9th Cir. Nov. 13, 2003) (if facilitating eavesdropping on customers would cause the company to be unable to operate, it is not accomplished with a "minimum of interference").

if that warrant had complied with the Fourth Amendment's Warrant and Particularity Clauses—which, as discussed below, it did not—the Stored Communications Act nonetheless did not authorize it.

§2703 permits a court to order the disclosure of two types of information. First, a court may order disclosure of "the contents of a wire or electronic communication." 18 U.S.C. §2703(a). But Lavabit's encryption keys are plainly not the "contents" of any "electronic communication." "Contents" are statutorily defined to mean "any information concerning the substance, import, or meaning of that communication." 18 U.S.C. §2510(8).[9] Encryption keys are not that; they are simply cryptographic tools (akin to a password) that convey neither meaning nor message. The government's purpose in seeking the encryption keys is to gain access to other data. And no educated speaker of English would describe a safe's "contents" as including the combination to that safe.

Nor were Lavabit's private keys an "electronic communication." An "electronic communication" is "any *transfer* of signs, signals, writing, images, sounds, data, or intelligence of any nature *transmitted* in whole or part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. §2510(12) (emphasis added). The entire point of Lavabit's private keys is

[9] The Stored Communications Act relies on the Wiretap Act's definitions. 18 U.S.C. §2711 ("As used in this chapter . . . the terms defined in section 2510 of this title have, respectively, the definitions given terms in that section[.]").

that they are *not* "transfer[red]" or "transmitted" to anyone, but rather held as closely guarded secrets by the company. §2703(a) therefore does not authorize the government to seize private encryption keys.

Alternatively, the government may seek "a record or other information pertaining to a subscriber." 18 U.S.C. §2703(c). Lavabit's private keys were undoubtedly "information," but by definition they do not "pertain[] to a subscriber." Lavabit's private keys are known to the company alone, and are not specific to any given customer. The information available under §2703(c) is "a subscriber's name, address, length of subscription, and other like data"—that is, data *about a subscriber*. *United States* v. *Appelbaum*, 707 F.3d 283, 287 (4th Cir. 2013). Lavabit's private encryption keys are just the opposite: they are information *about the company*. The government may therefore not seek private keys under §2703(c), either, and its warrant was invalid at the outset.

Even if Lavabit's private keys could generously be characterized as the contents of electronic communications or as pertaining to a subscriber, compliance with such an order must not "cause an undue burden" to the provider. 18 U.S.C. §2703(d). The warrant to disclose Lavabit's private keys, however, has imposed exactly that sort of burden on the company. Lavabit was forced to either (1) shut down, or (2) intentionally defraud its users about the security of its system, permanently harm its reputation should its deception be discovered, behave unethically by lying openly about its system's security, and violate universally-agreed-upon commercial practices within its industry.

It is difficult to imagine what would qualify as an undue burden if that does not—especially in light of Lavabit's proposal to provide the government with the information it requested with no loss of general customer privacy. This Court has emphasized that the Stored Communications Act was enacted to "minimiz[e] intrusions on the privacy of system users" and protect the "business needs of electronic communications system providers." *Appelbaum*, 707 F.3d, at 287. The government's course of conduct in this case, however, seems practically calculated to run roughshod over both of those purposes. The burden it imposed on Lavabit was as plainly undue as it was unjust.

B. The Fourth Amendment Forbids the Seizure of Lavabit's Private Keys and the Government's Subsequent Access of Customer Communications Data

Even if the government had the statutory authority to seize Lavabit's private keys, the Fourth Amendment independently prohibits the government from doing so. Moreover, the serious constitutional difficulties with the government's course of conduct provides an additional reason not to read the statutes to authorize what was done here, so long as there is any plausible alternative construction.

The Fourth Amendment permits warrants to issue only upon probable cause that the fruits, instrumentalities, or evidence of a crime will be found. See *Zurcher* v. *Stanford Daily*, 436 U.S. 547, 549–50 (1978). Lavabit's private keys are none of those things. They are lawful, innocent business secrets—like Coca-Cola's secret formula. The government surely could not demand that Coca-Cola turn *that* over without some

showing that the formula was the fruit, instrumentality, or evidence of a crime. The principle is the same here: A business' most closely guarded secrets may not be ransacked simply to gather a small amount of information about someone suspected of wrongdoing.

Moreover, the government proposed to use Lavabit's private keys to gain unfettered access to all—*all*—of the data traveling between Lavabit's servers and its customers. After all, explained the government, only then could it know which data involved the target of its investigation. But the Fourth Amendment insists that a warrant name *particular* things to be searched; a warrant that permits open-ended rummaging through all of Lavabit's communications data is simply a modern-day writ of assistance, the sort of general warrant that the Fourth Amendment was ratified to forbid. The government might as well have demanded that a hotel install glass doors on all of its rooms so it could see what the occupant of one of those rooms was up to.

1. Lavabit's Private Keys Were Not the Fruits, Instrumentalities, or Evidence of Any Crime

The government proposed to examine and copy Lavabit's most sensitive, closely guarded records—its private keys—despite the fact that those keys were not contraband, were not the fruits of any crime, were not used to commit any crime, and were not evidence of any crime. Rather, the government obtained a warrant to search and seize Lavabit's property simply because it believed that the information would be helpful to know as it conducted its investigation of someone else.

The Fourth Amendment's Warrant Clause forbids any warrant to issue but upon "probable cause." By probable cause, the Supreme Court has repeatedly explained, what is meant is a reason to believe that the "fruits, instrumentalities, or evidence of crime" will be found in the place to be searched. *Zurcher* v. *Stanford Daily*, 436 U.S. 547, 550 (1978). In other words, a "valid warrant" is one issued to search property "at which there is probable cause to believe that fruits, instrumentalities, or evidence of a crime will be found." *Id.*, 554. This rule is universally accepted and oft-repeated; this Court has frequently stated that "probable cause to search" depends on the existence of "facts and circumstances" that would "warrant a man of reasonable prudence in the belief that *contraband or evidence of a crime* will be found" in a particular place. *United States* v. *Doyle*, 650 F.3d 460, 471 (4th Cir. 2011) (emphasis added). While the issuing magistrate is of course entitled to make a "common sense determination" about the existence of probable cause, he must be evaluating the probability that "*contraband or evidence of a crime* will be found in a particular place." *United States* v. *Grossman*, 400 F.3d 212, 217 (4th Cir. 2005) (emphasis added).

By those lights, this is a very easy case. Lavabit's private keys are not connected with criminal activity in the slightest—the government has never accused Lavabit of being a co-conspirator, for example. The target of the government's investigation *never* had access to those private keys. Nor did anyone, in fact, other than Lavabit. Given that Lavabit is not suspected or accused of any crime, it is quite impossible for information known only to Lavabit to be evidence that a crime has occurred. The

government will not introduce Lavabit's private keys in its case against its target, and it will not use Lavabit's private keys to impeach its target at trial. Lavabit's private keys are not the fruit of any crime, and no one has ever used them to commit any crime. Under those circumstances, absent any connection between the private keys and a crime, the "conclusion[] necessary to the issuance of the warrant" was totally absent. *Zurcher*, 436 U.S., at 557 n.6 (quoting, with approval, Comment, 28 U. Chi. L. Rev. 664, 687 (1961)).

To be sure, the Fourth Amendment does not require that "the owner or possessor of the premises to be searched [be] himself reasonably suspected of complicity in the crime being investigated." *Zurcher*, 436 U.S., at 550. *Zurcher* permitted a search of a newspaper for evidence of a third party's crimes, and so if the government had probable cause to believe that the target of its investigation had left unencrypted emails detailing his crimes on Lavabit's servers (for example), a valid search warrant could permit the government to obtain them. What the government seized from Lavabit, however, was not information about its target or the target's crimes, but information *about Lavabit*.

If the Fourth Amendment permits the government to seize information that is not the fruit, instrumentality, or evidence of a crime, but that would simply be useful in apprehending the suspect, there is no practical limit on the government's gaze. It could demand the production of all manner of innocent information from all types of innocent people—no matter how intrusive or burdensome—so long as that

information might plausibly assist in its investigation. (Perhaps the government could demand to read the diaries of a suspect's friends, to learn what he was up to on certain days.) The government's warrant was therefore invalid as unsupported by probable cause, and Lavabit should not have been held in contempt for disobeying it.

2. The Government Violated the Fourth Amendment By Gaining Access to All Communications Data Traveling to and From Lavabit's Email Servers

Lavabit's private keys allowed the government access to data related to the target of the investigation. But it also gave the government access to *all* the data of Lavabit's 400,000 other customers—including the contents of unencrypted messages, and passwords that could be used to derive the keys necessary to decrypt customers' stored messages. As the government made clear, it would need to comb through all this information to identify the small amount of data relevant to its investigation. App.114. In short, the government proposed an open-ended rummaging through the correspondence of hundreds of thousands of people, to seize a small amount of information about one person suspected of a crime. Though the government may have thought the collateral damage to the privacy of hundreds of thousands of people outweighed by its investigative needs, its proposal contravenes the Fourth Amendment's prohibition against unreasonable searches and seizures, which exists "to safeguard the privacy and security of individuals against arbitrary invasions by government officials." *Camara v. Mun. Ct.,* 387 U.S. 523, 528 (1967).

The Fourth Amendment's text plainly prohibits unreasonable searches of the citizenry's "papers." See *Ex Parte Jackson*, 96 U.S. 727, 733 (1878). The contents of a telephone conversation are similarly protected from eavesdropping absent a warrant. See *Berger v. New York*, 388 U.S. 41 (1967); *Katz v. United States*, 389 U.S. 347 (1967). These protections apply analogously and equally to electronic correspondence as it travels to and from an email provider's servers. See *United States* v. *Warshak,* 631 F.3d 266, 288 (6th Cir. 2010).[10] As this Court has acknowledged in the context of the marital communications privilege, "emails today, in common experience, are confidential." *United States v. Hamilton*, 701 F.3d 404, 407 (4th Cir. 2012) (internal quotation marks omitted).

The Fourth Amendment therefore forbids the government to search the correspondence of Lavabit's customers in a manner that is unreasonable. But the government in this case had probable cause to suspect only one customer of a crime,

[10] This argument has been met with wide acceptance in the federal courts. See *In re Applications for Search Warrants for Info. Associated with Target Email Address,* Nos. 12–MJ–8119–DJW & 12–MJ–8191–DJW, 2012 WL 4383917, at *5 (D. Kan. Sept. 21, 2012) (holding that "an individual has a reasonable expectation of privacy in emails or faxes stored with, sent to, or received through an electronic communications service provider."); *United States v. Lucas,* 640 F.3d 168, 178 (6th Cir. 2011) ("individuals have a reasonable expectation of privacy in the content of emails stored, sent, or received through a commercial internet service provider."); *United States v. Ali,* 870 F. Supp. 2d 10, 40 n.39 (D.D.C. 2012) (same); *R.S. ex rel. S.S. v. Minnewaska Area Sch. Dist., No. 2149,* 894 F. Supp. 2d 1128, 1142 (D. Minn. 2012) ("one cannot distinguish a password-protected private Facebook message from other forms of private electronic correspondence," so user "had a reasonable expectation of privacy to her private Facebook information and messages").

and the warrant was not written to limit the scope of the search to data that the government had probable cause to search. Rather, it permitted the government to access and search a far broader range of data well beyond anything associated with the target of the investigation. See *United States* v. *Roche*, 614 F.2d 6, 7 (1st Cir. 1980) (invalidating a warrant that did not limit search to investigative target's documents concerning motor vehicle insurance, but authorized the broad seizure of documents related to all types of insurance). This Court has found that a warrant exceeded the scope of probable cause even when it authorized the seizure of legitimate documents from a company allegedly "permeated with fraud." *United States v. Oloyede*, 982 F.2d 133, 141 (4th Cir. 1992). The warrant here is far more dubious—Lavabit is a wholly innocent business, neither suspected nor accused of the slightest wrongdoing, and the government has nonetheless proposed to examine the correspondence of hundreds of thousands of its customers.

Just as the government cannot demand the master key to every room in a hotel based on probable cause to search for evidence of a particular guest's crime, see *United States v. Ritter*, 416 F.3d 256, 267 (3rd Cir. 2005) (once officers learn that a house believed to be a single residence is multi-occupancy, original warrant does not authorize search of entire building), the government cannot seize Lavabit's private keys to expose and search through the content and non-content data of all its users.

This is especially so because the Fourth Amendment requires that a warrant describe "the persons or things to be seized" with particularity. *Stanford v. Texas*, 379 U.S. 476, 511 (1965). This is to "prevent[] the seizure of one thing under a warrant

describing another." *Id.*, at 485-86 (quoting *Marron v. United States*, 275 U.S. 192, 196 (1927)). But the government's warrant here contemplated exactly that: examining the communications of every Lavabit customer, no matter how unconnected with the investigation. See also *United States v. Abrams*, 615 F.2d 541, 543 (1st Cir. 1980) (warrant permitting seizure of all Medicare and Medicaid records in an office, as well as some records of non-Medicare and non-Medicaid patients, did not comply with particularity requirement). See also *Voss v. Bergsgaard*, 774 F.2d 402, 406 (10th Cir. 1985) (a warrant that "simply authorizes the seizure of all files, whether or not relevant to a specified crime, is insufficiently particular").

The government's warrant here demanded "[a]ll information necessary to decrypt communications sent to or from the Lavabit email account [xxxxxxxxxx]@lavabit.com, including encryption keys and SSL keys," as well as "[a]ll information necessary to decrypt data stored in or otherwise associated with the Lavabit account [xxxxxxxxxx]@lavabit.com." App. 27. This demand for Lavabit's private keys, however, gave the government access to *all* content and non-content data sent and received by *all* of Lavabit's subscribers, not just the target of the investigation. While very little of this data was the object of the search, the government would rummage through all of it to identify the small amount relevant to the investigation. The indiscriminate sweep of the warrant as written was "constitutionally intolerable," rendering the warrant defective. *Stanford*, 379 U.S. at 486.

C. *A Grand Jury Subpoena Requiring a Company to Provide Its Private Encryption Keys is Unreasonable and Oppressive*

In between simply demanding Lavabit's private keys orally and securing a facially invalid warrant for those keys under the Stored Communications Act, the government also served Lavabit with a grand jury subpoena commanding the company to produce what it wanted. App. 23-24. That subpoena should have been quashed. Requiring Lavabit to provide its private keys is the very definition of an "unreasonable or oppressive" command. Fed. R. Crim. P. 17(c).

While there are "various ways in which a subpoena may be unreasonable or oppressive," classic examples are subpoenas that are "abusive or harassing," "excessively broad," or (perhaps most relevant here) those that "intrude[] gravely" on other "significant interests." *In re Grand Jury, John Doe No. GJ 2005-2*, 478 F.3d 581, 585 (4th Cir. 2007) (quoting *In re Grand Jury Matters*, 751 F.2d 13 (1st Cir. 1984)). When "compliance is likely to entail consequences" that are "more serious" than the mere "inconveniences" that may be occasioned by a typical overbroad record request, Rule 17(c) directs the court to quash or modify the subpoena.

We will not swell this brief with further restatements of the harm the government's request has caused Lavabit. Suffice to say that it was precisely the sort of abusive and destructive request that Rule 17(c) is meant to guard against. If it is not "abusive" to barrage a small businessman with a flurry of orders of this sort while he is forced to travel cross-country in response to the government's demands,

it is unclear what would be. And to comply with the government's subpoena would have either required Lavabit to perpetrate a fraud on its customer base or shut down entirely. That is the key point, and the resulting harm goes far beyond a mere inconvenient search for records. Just as requiring a hotel owner to install glass doors on all its hotel rooms would destroy the hotel's business, Lavabit *cannot exist* as an honest company if the government is entitled to take this sort of information in secret. Its relationship with its customers and business partners depends on an assurance that it will not secretly enable the government to monitor all of their communications at all times. If a mere grand jury subpoena can be used to get around that (in secret, no less), then no business—anywhere—can credibly offer its customers a secure email service.

"What is reasonable" for a grand jury subpoena "depends on the context." *United States* v. *R Enters., Inc.*, 498 U.S. 292, 299 (1991). The context here is admittedly an unusual one, but the principle is clear. If using a grand jury subpoena to put an honest small business to an existential crisis is not "oppressive," nothing is.

CONCLUSION

The district court's finding of contempt should be vacated because the underlying disclosure orders were unlawful. This Court should order the contempt fines assessed against Appellants be reversed and compel the government to turn over the SSL keys in its possession. This case should be remanded for further proceedings consistent with that conclusion.

STATEMENT OF ORAL ARGUMENT

Because this case presents important legal issues of first impression, oral argument is requested.

Dated: October 10, 2013

Respectfully submitted,
By: /s/ Jesse R. Binnall

Jesse R. Binnall
Bronley & Binnall, PLLC
10387 Main Street, Suite 201
Fairfax, Virginia 22030
(703) 647-5926
E-mail: jbinnall@bblawonline.com

Ian Samuel
290 W. 12th Street, Apt. 3B
New York, New York 10014
(917) 803-8609
ian@iansamuel.com

Marcia Hofmann
Law Office of Marcia Hofmann
25 Taylor Street
San Francisco, CA 94102
(415) 830-6664
marcia@marciahofmann.com

David Warrington
LeClairRyan
2318 Mill Road, Suite 1100
Alexandria, VA 22314
(703) 647-5926
David.Warrington@leclairryan.com

Laurin Mills
LeClairRyan
2318 Mill Road, Suite 1100
Alexandria, VA 22314
(703) 647-5903
Laurin.Mills@leclairryan.com

Counsel for Party-in-Interest – Appellant

CERTIFICATE OF COMPLIANCE WITH RULE 32(a)
Certificate of Compliance with Type-Volume Limitation, Typeface Requirements, and Type Style Requirements

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because:

   this brief contains 7,614 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because:

   this brief has been prepared in a proportional spaced typeface using Microsoft Word in 14 point Garamond.

By: /s/ Jesse R. Binnall
Jesse R. Binnall, Esq.

Dated: October 10, 2013

CERTIFICATE OF FILING AND SERVICE

I hereby certify that on October 10, 2013, I electronically filed the foregoing with the Clerk of Court using the CM/ECF System, which will send notice of such filing to the following registered CM/ECF users:

Michael P. Ben'Ary
James L. Trump
OFFICE OF THE
UNITED STATES ATTORNEY
2100 Jamieson Avenue
Alexandria, VA 22314
(703) 299-3700

Counsel for Appellee

The necessary filing and service were performed in accordance with the instructions given to me by counsel in this case.

By: /s/ Melissa A. Dockery
Melissa A. Dockery
GIBSON MOORE APPELLATE SERVICES, LLC
421 East Franklin Street, Suite 230
Richmond, VA 23219