Case Nos. 13-4625, 13-4626

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

IN RE: UNDER SEAL

UNITED STATES OF AMERICA

Plaintiff-Appellee,

v.

UNDER SEAL 1; UNDER SEAL 2,

Parties-In-Interest-Appellants

On Appeal from the United States District Court
for the Eastern District of Virginia
The Honorable Claude M. Hinton
Case Nos. 13-SW-00522-CMH-1; 13-DM-00022-DMH-1

BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF APPELLANT

Kurt Opsahl
kurt@eff.org
Jennifer Lynch
Hanni Fakhoury
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 436-9333

Counsel for Amicus Curiae
ELECTRONIC FRONTIER FOUNDATION

DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, amicus curiae Electronic Frontier Foundation states that it does not have a parent corporation, and that no publicly held corporation owns 10% or more of the stock of amicus.

Dated: October 24, 2013

Respectfully submitted,

/s/ Kurt Opsahl

Kurt Opsahl
Jennifer Lynch
Hanni Fakhoury
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333

Counsel for Amicus Curiae
ELECTRONIC FRONTIER FOUNDATION

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

Federal Statutes

Federal Rules

Constitutional Provisions

Other Authorities

STATEMENT OF INTEREST

The Electronic Frontier Foundation ("EFF") is a member-supported civil liberties organization working to protect free speech and privacy rights in the online world. With more than 24,000 dues-paying members nationwide, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age. As part of its mission, EFF has often served as counsel or *amicus* in cases involving digital searches and seizures, and expectations of privacy in electronic communications. *See, e.g., City of Ontario v. Quon*, 560 U.S. 746 (2010); *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010); *In re Search Warrant*, 71 A.3d 1158 (Vt. 2012).

Pursuant to Federal Rule of Appellate Procedure 29(c)(5), no one, except for undersigned counsel, has authored the brief in whole or in part, or contributed money towards the preparation of this brief. Neither Counsel for appellant Lavabit nor appellee the United States of America oppose the filing of this brief.

INTRODUCTION

Encrypted online communications form the backbone of the modern Internet. Without an encrypted connection, people would be at risk when they manage finances over the Web, purchase books online, transfer medical information between doctors or send and receive private communications.

To help enable the Internet to become an engine of free expression, innovation and commerce, in the 1990s the pioneering browser company Netscape introduced a protocol with two keys; a public key that anyone can use to encrypt communications to a service provider and a private key that only the service provider could use to decrypt the messages. The new security of this encrypted "Hypertext Transfer Protocol Secure" (HTTPS) allowed ecommerce to thrive and helped bring about the information economy.

The private key is the service provider's crown jewel, opening the door to every user's online interactions with the website. The security depends on the secrecy of the key—once it is compromised, the security model is shattered. What happened here demonstrates that this is not merely hypothetical, but real. By forcing Lavabit to turn over its private keys, the government not only disrupted the security model on which the Internet depends, it also violated the Fourth Amendment.

Lavabit has a reasonable expectation of privacy in its private key—both to protect its own communications and to protect the communications of its 400,000 customers. The government interfered with Lavabit's possessory interest in the key, in the process destroying its business and threatening to expose the private communications of its customers. The warrant, which the government ultimately obtained after attempting to seize the key with less stringent process, had no

limitations or protections for these innocent customers, casually destroying their privacy as collateral damage. Seeking Lavabit's private key to access the communications of one customer fails the minimization and particularity requirements of the Fourth Amendment and turns the warrant at issue here into a general warrant—no different than a warrant to search all houses in a city to find the papers of one suspect.

Nor was the government empowered to side-step the Fourth Amendment's requirements through a grand jury subpoena. Such subpoenas contain none of the protections of a warrant. All searches and seizures must be reasonable, yet the grand jury subpoena issued here was unreasonable because it violated the expectations of Lavabit and its users and oppressive because compliance with the subpoena was fatal to Lavabit's business.

Accordingly, this Court should reverse the district court's order.

ARGUMENT

I. Permitting the Government to Obtain a Private Encryption Key Compromises the Security of All Internet Users.

Relying on several different disclosure orders, the government has sought to obtain a private encryption key from Lavabit. This is like trying to hit a nail with a wrecking ball; disclosing the private encryption key will not only allow the government to access the information of the single Lavabit customer who is the target of its investigation, it will allow the government to access all of Lavabit's

400,000 customers' communications, Lavabit's own communications, and will, most importantly, compromise the security of the HTTPS protocol, on which the growth of innovation, expression, commerce and business on the Internet depends.

A. A Private Key Protects the Communications and Other Security-Sensitive Information of All Users of a Service.

Private encryption keys like the one sought by the government in this case form the backbone for the industry-standard HTTPS protocol that secures communications online. HTTPS relies on the mathematics of asymmetric cryptography to encrypt communications between a user's computer and computers controlled by the service provider. While these computer-to-computer communications protected with encryption may include the content of user communications like email and chat, they encompass a much wider data set and often include many other types of sensitive information, such as passwords that users enter to log into services, security tokens in URLs used as authentication or access control mechanisms, or sensitive banking transaction or credit card information. Asymmetric cryptography secures communications using two keys—a "public key," which is held by a service provider and is made widely available, and a "private key," which is kept secret.[1] These keys can be represented by a

[1] For more on the technology, *see* Public-key Cryptography, Wikipedia, http://en.wikipedia.org/wiki/Public-key_cryptography (last visited Oct. 23, 2013).

string of alphanumeric characters, and the data of the private key is often stored in a small digital file under the control of the service provider.

The security of the HTTPS protocol relies on private keys being kept private and secure by the service provider, and providers take this security very seriously. As the key is thought generally to be too difficult to guess or "crack" even by parties with tremendous computational resources,[2] the security of the key hinges on whether another party is able to obtain a copy of it.

In industry-standard deployments of HTTPS, a single private key is used to secure the communications of all users of a service.[3] For example, Facebook has a

[2] The fact that keys cannot be uncovered with a brute force attack by even very powerful attackers may seem unintuitive, but this is widely believed to be the case based on how the mathematics of asymmetric cryptography work. Whether a key can be brute force attacked in this fashion depends on the key length, and there have been no demonstrated successful recoveries of RSA 1024 bit keys. Still, out of a theoretical concern that this key length may not be long enough to guard against attackers with tremendous resources, service providers have already begun to phase these out in favor of 2048 bit keys. Lavabit uses a 2048 bit key, thought to be uncrackable for the foreseeable future.

[3] The validity period is governed by entities known as "Certificate Authorities," and the validity is established via a mechanism known as "digital certificates." Certificate authorities typically only give out these certificates for validity periods of at least one year. For example, Facebook's certificate is valid from April 11th, 2013 until March 5th, 2016. This information is available by looking at the certificate presented when visiting "facebook.com." For a view into the policies of Verisign, a Certificate Authority, regarding certificate lifespan, *see* https://securitycenter.verisign.com/contents_VRSN_US/HTML/pop_validityPeriod.htm (last visited Oct. 23, 2013).

single private key that protects the communications of over 1.26 billion users.[4] When a private key has been discovered or disclosed to another party, all users' past and future communications are compromised for the duration that the key was active.[5] In the case of Facebook, having the private key used by the company would give unfettered access to the personal information of almost 20% of all of the human beings on the planet obtained through the Facebook site for three years.[6]

Moreover, a private key not only protects the electronic communications of a given communication service. It also protects passwords, credit card information, and other sensitive information like a user's search engine query terms. Many people re-use passwords,[7] so access to one site's key will allow access to all users' passwords on the site, which in turn can lead to access to many other online services.

---

[4] *See* The Faces of Facebook, http://app.thefacesoffacebook.com/ (last visited Oct. 23, 2013) (estimating the current number of Facebook users).

[5] Some deployments of HTTPS use a technology called Perfect Forward Secrecy ("PFS"). For HTTPS deployments that use PFS, the key can only be used to read future communications, and cannot retroactively be used to decrypt past sessions for users that have been collected. PFS is rarely used in practice. For a discussion of PFS, *see* Forward Security: Perfect Forward Secrecy, Wikipedia, http://en.wikipedia.org/wiki/Forward_secrecy#Perfect_Forward_Secrecy (last visited Oct. 23, 2013).

[6] *See* U.S. and World Population Clock, http://www.census.gov/popclock/ (last visited Oct. 23, 2013) (providing an estimate of current world population).

[7] *See, e.g.*, Ted Samson, *Study Finds High Rate of Password Reuse Among Users*, InfoWorld (Feb. 10, 2011), http://www.infoworld.com/t/data-security/study-finds-high-rate-password-reuse-among-users-188 (last visited Oct. 23, 2013).

B. The Public Key Infrastructure System Protects Encrypted Internet Communications Regardless of How Private Keys Are Compromised.

Given the tremendous importance of private keys, there is complex infrastructure in place to govern their use and revocation, known as public key infrastructure (or "PKI").[8] The PKI system is designed in part to minimize the chances that users' communications will be compromised through the turning over of a private key. Critical entities, known as Certificate Authorities, issue and manage security credentials for Internet companies. Their role in part is to ensure that private keys remain only in the hands of the intended recipients. To protect their users, browsers verify that a Certificate Authority has vouched for a given website before loading a secure page on that website.

Companies are sometimes under contractual obligations with Certificate Authorities to not disclose their private key,[9] and those authorities are charged with immediately revoking a key when there is any evidence of a security breach. There is no exception for government access, and as soon as it became public that

[8] For a more detailed discussion of PKI, *see* Public Key Infrastructure, Wikipedia, http://en.wikipedia.org/wiki/Public-key_infrastructure (last visited Oct. 23, 2013).

[9] For an example of how Certificate Authorities can put companies under an obligation to notify, *see* Trustis HMRC Set Certificate Service: Obligations of Subscribers, Trustis-Set, http://www.trustis.com/pki/HMRCSET/policy/pds.html (last visited Oct. 23, 2013) ("Immediately notify the Registration Authority of a suspected or known compromise of Certificate security in accordance with the procedures laid down in the Trustis HMRC SET Issuing Authority Certificate Policy.").

Lavabit's key had been compromised through the disclosure order issued in this case, the Certificate Authority GoDaddy revoked the company's key.[10] Once a Certificate Authority has revoked a company's key, its secure site becomes effectively unavailable to users, sharply impacting its ability to conduct commerce on the Internet.

C. Because Security of the HTTPS Protocol Is Critical to the Growth of the Internet, Breach of a Private Key is Catastrophic Security Event.

HTTPS is used by service providers of all sorts, from banks and social networks to email providers, to protect everything from passwords and credit card information to the content of user communications. Part of the advantage of HTTPS is that users do not need any sort of special or technical knowledge to benefit from this encryption; people who browse the Internet routinely and automatically use the HTTPS protocol and may sometimes notice visual indicators in their browsers that signify that a particular connection is secure.[11]

The security of the HTTPS protocol is of vital importance for the protection of users and the growth of commerce and business on the Internet. Industries such

---

[10] *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/.

[11] For a description of what these indicators look like in the Chrome browser, for example, *see* Google Chrome Website Settings, https://support.google.com/chrome/answer/95617?hl=en (last visited Oct. 23, 2013).

as health care, which have been slow to rely on the Internet given security risks, are beginning to view the Internet as a place where secure transactions can occur.[12] Security experts and technologists have therefore highlighted how critical it is to avoid the chilling effect that would result from the diminished security of HTTPS.[13]

For all of these reasons, the breach of a private key compromises the security of the HTTPS protocol as a whole and should be considered a catastrophic security event, one that has the potential to have a profound effect on not only the security of HTTPS, but on the United States economy as well.

Service providers with an interest in protecting users will choose legal jurisdictions based in part on statutory or case-law-developed rules governing lawful access to key material. This may push such providers to move their businesses to jurisdictions that afford more protections for privacy and security.

---

[12] The rise of the health care industry using online security mechanisms is a multifaceted topic. But, for example, proposed standards for distributing Electronic Health Records use an Internet-based open authentication protocol that relies on HTTPS. *See, e.g.*, Adrian Gropper, *The Dog's OAuth*, The Healthcare Blog, (Jan. 18, 2010) http://thehealthcareblog.com/blog/2010/01/18/the-dogs-oauth/.

[13] *See Technologists' Comment to the Director of National Intelligence Review Group on Intelligence and Communications Technology* (Oct. 4, 2013) https://www.eff.org/files/2013/10/05/nsa-review-panel-tech-comment.pdf ("This comes at a critical time in the evolution of Internet security: new industries like health care are just starting to put more trust into the security of online systems. It would be disastrous if the NSA's efforts undermined this growing trust in online security.").

Moreover, if it becomes clear that the government can routinely access private keys, HTTPS will be considered much less secure, and new security mechanisms will be developed to ensure that bulk access to user communications is not possible.

Thus, given the importance of private keys to the security infrastructure of the Internet, and the power that comes with access to these keys, ensuring that there are strong protections against compelled disclosure of private keys is critical to the security of HTTPS. The Fourth Amendment to the U.S. Constitution provides one such protection, but as explained below, both the search warrant and the subpoena used to obtain Lavabit's private key fell outside constitutional boundaries of what the Fourth Amendment permits.

II. The Orders Authorizing Disclosure of the Private Key Violate the Fourth Amendment.

Lavabit is in the unusual position of defending against the disclosure of a single "document"—its private encryption key—via a "blizzard" of different court orders. Appellant's Opening Brief ("AOB") at 8. But neither the search warrant, nor the pen/trap order, nor the subpoena issued to Lavabit could compel disclosure of the key consistent with the Fourth Amendment.

A. Private Keys are Protected by the Fourth Amendment.

The Fourth Amendment protects people from "unreasonable searches and seizures" of their "persons, houses, papers and effects." U.S. Const. amend. IV. A

"Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001) (citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan J., concurring)).[14] A "seizure" for purposes of the Fourth Amendment occurs when "there is some meaningful interference with an individual's possessory interests in that property." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (citing *United States v. Chadwick*, 433 U.S. 1, 13, n. 8 (1977)). "Possession" means a person has "dominion and control" over the item. *United States v. Rusher*, 966 F.2d 868, 878 (4th Cir. 1992).

Here, both search and seizure are at issue. First, Lavabit has a reasonable expectation of privacy in the key itself. The private key was effectively a password—albeit a long, difficult to remember one—that had the potential to unlock the contents of all of its users' electronic communications. Lavabit treated the key as private and took great steps to prevent its disclosure. Society expects and relies on the fact that service providers will protect their private keys to ensure the security of the HTTPS protocol. The Public Key Infrastructure system was set up in part to manage and enforce this.

[14] The U.S. Supreme Court has recently revived the pre-*Katz* focus on physical intrusion onto private property as another way in which the government can violate the Fourth Amendment. *See Florida v. Jardines*, 133 S. Ct. 1409 (2013); *United States v. Jones*, 132 S. Ct. 945 (2012). But as the Court recently explained in *Jones*, these holdings complement, but do not displace *Katz's* foundational approach that looks at expectations of privacy. *Jones*, 132 S. Ct. at 952.

Moreover, the government's attempt to obtain the key interfered with Lavabit's possessory interest in it. Since no one knew the key but Lavabit, and since the key enabled it to have exclusive dominion and control over the files and communications effectively "locked" by the private key, the government's efforts to obtain the key interfered with Lavabit's exclusive "dominion and control" over the key. Lavabit would no longer be the only one able to decrypt the communications and have control and access to the communications on its servers. Thus, when the government obtained the key, it constituted a "seizure" under the Fourth Amendment.

B. Lavabit's Customers Have an Expectation of Privacy in their Communications, and Lavabit Can Assert that Privacy Interest on their Behalf.

The Fourth Amendment extends to protect not only to the private key and its seizure, but also to the information the private key unlocked: an enormous database of Lavabit's customer's email communications. Passwords are "affirmatively intended to exclude" others from the place to be searched, *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001), and here, the place unlocked by the password contained one of the most treasured pieces of private information: details of a person's electronic communications.[15] The Fourth Amendment protects these

[15] The government here sought the SSL private key to get routing information about the suspect's electronic communications and not the communications themselves. *See* AOB at 6. While the government has argued in other contexts

communications no less than the contents of letters sent through the mail. *See Ex parte Jackson*, 96 U.S. 727, 733 (1877); *see also United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (expectation of privacy in the contents of emails) ("*Warshak II*"); *United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div.*, 407 U.S. 297, 313 (1972) (Fourth Amendment protects "conversational privacy").

Lavabit itself can assert its customers' privacy interest in the electronic communications they have locked away on Lavabit's servers. *See United States v. Perez*, 689 F.2d 1336, 1338 (9th Cir. 1982) (per curiam) (a person or entity can have a "legitimate expectation of privacy in a place or object he does not own") (citing *United States v. Reyes*, 595 F.2d 275, 278 (5th Cir. 1979)). Determining an expectation of privacy requires examining the person's "interest in and control of the area searched" as well as its "efforts to ensure that privacy and society's willingness to recognize his expectation as reasonable." *United States v. Horowitz*, 806 F.2d 1222, 1225 (4th Cir. 1986) (citing *Rakas v. Illinois*, 439 U.S. 128 (1978)).

Here, Lavabit not only had control of the area to be searched—its servers—but it also had an "interest" in that area. It had a business interest because its entire

---

that this routing information is not protected by the Fourth Amendment since it is information turned over to a third party, *see e.g., United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008), the fact that it sought a search warrant here means that it should be deemed to waive this argument in this case. *See Steagald v. United States*, 451 U.S. 204, 209 (1981) (government can "lose its right to raise factual issues" about whether a Fourth Amendment expectation of privacy exists "when it has made contrary assertions in the courts below").

business model was predicated on the extraordinary steps it took to safeguard its customers' data—steps far more aggressive than more mainstream commercial email providers. The effort Lavabit took to safeguard its customers' privacy allows it to assert the privacy interests of its customers. *See, e.g., United States v. Golden Valley Elec. Ass'n*, 689 F.3d 1108, 1116 (9th Cir. 2012) ("Depending on the circumstances or the type of information, a company's guarantee to its customers that it will safeguard the privacy of their records might suffice to justify resisting an administrative subpoena" as being unconstitutional under the Fourth Amendment).

C. Because the Search Warrant Contained No Limiting Principles, It Was an Illegal "General Warrant."

Warrantless searches and seizures are "*per se* unreasonable under the Fourth Amendment" unless they fall within a few specific exceptions, none of which apply here. *Coolidge v. New Hampshire*, 403 U.S. 443, 454-55 (1971) (quoting *Katz*, 389 U.S. at 357)). Indeed, the government must have recognized the Fourth Amendment interests here when it ultimately decided to seek a warrant after initially trying to use a subpoena to obtain the private key. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 562-63 (1978) ("[S]earch warrants are more difficult to obtain than subpoenas. . . . Where, in the real world, subpoenas would suffice, it can be expected that they will be employed [instead of warrants] by the rational

prosecutor."). Yet the mere existence of the warrant does not end the constitutional inquiry.

The Fourth Amendment requires a warrant "particularly describe[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. This requirement ensures that "those searches that are deemed necessary are as limited as possible," as the evil of unrestrained searches "is not that of intrusion *per se*, but of a general, exploratory rummaging" in a protected space. *Coolidge*, 403 U.S. at 467 (emphasis added). Another function of the particularity requirement is to "ensure[] that the search will be carefully tailored to its justifications." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). That is done by ensuring "nothing is left to the discretion of the officer executing the warrant" in determining what information can be taken under the warrant. *Marron v. United States*, 275 U.S. 192, 196 (1927); *see also United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010).

When it comes to the use of electronic surveillance to intrude into conversational privacy, the Supreme Court has held that "Fourth Amendment safeguards" *must* be applied. *U.S. Dist. Court for E. Dist. of Mich.,* 407 U.S. at 313; *see also Berger v. New York*, 388 U.S. 41, 58 (1967) ("indiscriminate use of electronic devices . . . must be carefully circumscribed so as to prevent unauthorized invasions of the sanctity of a man's home and the privacies of life.")

(citations and quotations omitted). Courts are authorized to impose *ex ante* conditions on the execution of a search warrant in order to avoid the risk of a "general warrant" inherent in broad electronic searches. *See, e.g.*, *In re Appeal of Application for Search Warrant*, 71 A.3d 1158, 1172 (Vt. 2012); *United States v. Comprehensive Drug Testing*, 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (per curiam).

Courts may also assess the reasonableness of how the government conducts an electronic search after the search has occurred. *See United States v. Christie*, 717 F.3d 1156, 1167 (10th Cir. 2013) ("even if courts do not specify particular search protocols up front in the warrant application process, they retain the flexibility to assess the reasonableness of the search protocols the government actually employed in its search after the fact.").

Moreover, courts have routinely invalidated warrants whose "description . . . of the place to be searched is so vague that it fails reasonably to alert executing officers to the limits of their search authority." *United States v. Clark*, 638 F.3d 89, 94 (2d Cir. 2011); *see also Davis v. Gracey*, 111 F.3d 1472, 1479 (10th Cir. 1997) (warrants are invalid "where the language of the warrants authorized the seizure of virtually every document that one might expect to find in a . . . company's office, including those with no connection to the criminal activity providing the probable cause for the search") (internal quotation omitted); *United*

States v. Kow, 58 F.3d 423, 427 (9th Cir. 1995) (same where warrant "contained no limitations on what documents within each category could be seized or suggested how they related to specific criminal activity").

Judged under this standard, the warrant here fails the Fourth Amendment's particularity requirement. It contained nothing to limit the government's collection of information about each and every one of Lavabit's users. The warrant itself, of course, was focused on only one Lavabit customer. But the warrant commanded surrender of any information "necessary to decrypt communications sent to or from the Lavabit e-mail account . . . including encryption keys and SSL keys." App. 118-19.[16] Seizure of the private key would permit the government to obtain the information about the suspect. However, it would also permit the government to obtain the same information on all of Lavabit's customers, exposing them, in the process, to the potential of recurring government surveillance for as long as the key was valid in the future and as long as it had been valid in the past.

The government's oblique promise to only use the private key to decrypt records pertaining to the target[17] is not a valid limitation on the warrant. Just as the

[16] "App." refers to the appendix filed in connection with Lavabit's opening brief.

[17] In the government's opposition to Lavabit's motion to quash the subpoena and invalidate the search warrant, it asserted federal laws would limit its authority to collect data on other Lavabit users. Resp. of the U.S. in Opp'n to Lavabit's Mot. to Quash Subpoena and Mot. to [*sic*] for Unsealing of Sealed Ct. Rs. at 13-14, *In re Application of the U.S. Authorizing the Use of a Pen Register/Trap and Trace Device on an Elec. Mail Account*, No. 1:13-EC-297 (E.D. Va. July 31, 2013).

Supreme Court "would not uphold an unconstitutional statute merely because the Government promised to use it responsibly," *United States v. Stevens*, 559 U.S. 460, 480 (2010),[18] this Court should not uphold an unconstitutional search warrant merely because the government promised it would only view information about the target and no one else. Accordingly, the Stored Communications Act warrant was invalid under the Fourth Amendment.

D. The Fourth Amendment Protects Private Keys from Disclosure Pursuant to a Grand Jury Subpoena.

As an intermediate position before obtaining a search warrant for Lavabit's private key, the government served Lavabit with a grand jury subpoena commanding it to disclose the key.[19] The subpoena also fails under the Fourth

[18] A better limitation to avoid a general warrant would have been explicit minimization instructions in the warrant, similar to that suggested in Judge Kozinski's concurring opinion in *Comprehensive Drug Testing*. *See* 621 F.3d at 1180 (Kosinzki, J., concurring). Those requirements are (1) the government must waive the "plain view" rule, and agree to only use evidence of the crime or crimes that led to obtaining the warrant; (2) the government must wall off the forensic experts who use the key to decrypt communications from the agents investigating the case; (3) the government must use a reasonable search protocol to designate what information the forensic experts can give to the investigating agents; and (4) the government must destroy or return non-responsive data. *Id.*; *see also In re Search Warrant*, 71 A.3d at 1170 (*ex ante* conditions like those in *Comprehensive Drug Testing* "acceptable mechanisms for ensuring the particularity of a search"). But as explained in more detail below, the government should have worked harder with Lavabit to obtain the records it requested before resorting to the extraordinary step of attempting to obtain the private key.

[19] The government initially obtained a Pen Trap Order, which it contended required Lavabit to turn over its private key. AOB at 6-7, 14. Lavabit has already

Amendment because the subpoena power cannot grant the government authority to compel disclosure of Lavabit's most "closely guarded secrets." AOB at 5.

This case presents an unprecedented use of the subpoena power. The government here claims that, with a mere subpoena, it can compel a disclosure that would in one fell swoop destroy Lavabit's business and expose the communications of every single one of its users to government scrutiny. Were this true, there would be no limiting principle preventing the government from undermining the security of any website that relies on public key encryption—from Facebook to Google to Bank of America to Amazon—all with a single subpoena.

However, the government cannot constitutionally exercise the subpoena power in this way. By invading the legitimate privacy interest of Lavabit and its customers and by effectively destroying Lavabit's legitimate business model when it complied with the subpoena, the subpoena was unreasonably burdensome and violated the Fourth Amendment.

1. *The Invasion of Privacy Wrought by Disclosure of a Private Key Precludes Use of a Grand Jury Subpoena.*

Despite the importance and breadth of the subpoena power, the Fourth Amendment necessarily limits it. *See In re Subpoena Duces Tecum*, 228 F.3d 341, 347 (4th Cir. 2000) (citing *Hale v. Henkel,* 201 U.S. 43, 76 (1906)). In fact, the

---

thoroughly discussed why this Order did not give the government the authority to compel disclosure of the key, AOB at 14-17, and *amicus* joins this argument.

Supreme Court has found that a grand jury is "*without power* to invade a legitimate privacy interest protected by the Fourth Amendment." *United States v. Calandra*, 414 U.S. 338, 346 (1974) (emphasis added); *In re Subpoena Duces Tecum*, 228 F.3d at 349. Compelling the disclosure in this case would invade Lavabit's own expectation of privacy in its key as well its users' in their communications. *See Warshak II,* 631 F.3d at 288. The district court's denial of Lavabit's motion to quash was mistaken because it failed to take into account the serious invasion of privacy wrought by the subpoena. *See Calandra*, 414 U.S. at 346 (where a subpoena is unreasonable and invades a constitutionally protected expectation of privacy, "[j]udicial supervision is properly exercised in such cases to prevent the wrong before it occurs").

Here, as explained in more detail above, Lavabit itself has an expectation of privacy in the item sought for disclosure, the private key. Yet, the subpoena would not just require production of the key but would also directly enable an unlimited search of the communications of hundreds of thousands of Lavabit's users.

As a result, the subpoena served on Lavabit falls far outside of traditional practice. The Supreme Court has suggested that where a subpoena is aimed at a document such as a personal diary, "[s]pecial problems of privacy" arise. *Fisher v. United States*, 425 U.S. 391, 401 n. 7 (1976) (citing *United States v. Bennett*, 409 F.2d 888, 897 (2d Cir. 1969)). That is because a diary, much like the private key at

issue here, is a paradigmatic example of a private paper subject to a legitimate expectation of privacy. *See Bennett*, 409 F.2d at 897; *Katz*, 389 U.S. at 361 (Harlan J., concurring). Obtaining the key with a subpoena would thus be akin to an "unlimited search," *Bennett*, 409 F.2d at 897, a use of the subpoena power that is disallowed under the Fourth Amendment. *See Calandra*, 414 U.S. at 346.

Since *Katz*, the Supreme Court has considered and rejected several Fourth Amendment challenges to subpoenas. *See, e.g., SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735 (1984); *United States v. Miller,* 425 U.S. 435 (1976). However, these cases are not controlling because they turn on the crucial fact that the individual challenging the subpoena was deemed to not have a legitimate expectation of privacy in the documents at issue because they were business records held by a third party.[20] *See Miller,* 425 U.S. at 446; *O'Brien,* 467 U.S. at 743; *Warshak v. United States*, 490 F.3d 455, 469 (6th Cir. 2007) *("Warshak I")* *vacated en banc on other grounds*, 532 F.3d 521 (6th Cir. 2008) (noting that the crucial inquiry in case of compelled disclosure of e-mails held by an ISP is whether "an e-mail user maintains a reasonable expectation of privacy in his e-mails *vis-a-vis* the party who is subject to compelled disclosure").

[20] A similar distinction underlies the holding in *United States v. Dionisio*, 410 U.S. 1 (1973), where the Court found that a grand jury could subpoena individuals to appear and provide voice exemplars since individuals have no reasonable expectation of privacy in the sound of their voices. *Dionisio* 410 U.S. at 3, 14.

By contrast, Lavabit and its customers have a legitimate expectation in the privacy of the key itself and in the information unlocked by the key respectively. This expectation of privacy is entitled to full Fourth Amendment protection, and therefore, the key cannot be obtained with a mere subpoena.

2. *The Subpoena Was Unreasonable Because it was Arbitrarily Excessive and Compliance Was Oppressive.*

In addition, the subpoena for Lavabit's private key violated the Fourth Amendment because of its burdensome (and in fact fatal) effect on Lavabit's e-mail service.

The Fourth Amendment requires a subpoena to be "reasonable" and forbids subpoenas that are overbroad or "arbitrarily excessive." *In re Subpoena Duces Tecum*, 228 F.3d at 347, 349 (quoting *United States v. Morton Salt Co.*, 338 U.S. 632, 653 (1950)); *see also Oklahoma Press Publ'g Co. v. Walling*, 327 U.S. 186, 208 (1946) ("The gist of the protection is in the requirement, expressed in terms, that the disclosure sought shall not be unreasonable."). A subpoena is generally "reasonable" if it is "sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome." *In re Subpoena Duces Tecum*, 228 F.3d at 347 (quoting *See v. City of Seattle*, 387 U.S.

541, 544 (1967)) (internal quotations omitted).[21] "[W]hat is reasonable depends on context." *United States v. R. Enters., Inc.*, 498 U.S. 292, 299 (1991). The inquiry "cannot be reduced to a formula." *Walling*, 327 U.S. at 209. The district court's refusal to quash the subpoena at issue in this case was in error because the subpoena was arbitrarily excessive and unreasonably burdensome.

In a typical case, a subpoena might be judged arbitrarily excessive because it is "far too sweeping in its terms" or "not suitably specific and properly limited in its scope in respect to [its] breadth." *In re Subpoena Duces Tecum*, 228 F.3d at 349 (internal quotations omitted). For example, a request for thousands of documents with which it would be practically impossible to comply could be considered unreasonable. *Id.* at 350. However, because this inquiry is context-specific, even a narrow subpoena request can be unreasonable if it has an extreme effect on the recipient. Hence, a subpoena aimed at a company can be arbitrarily excessive when it "put[s] a stop to the business of that company." *Hale*, 201 U.S. at 77; *FCC v. Cohn*, 154 F. Supp. 899, 912-13 (S.D.N.Y. 1957) (finding that an administrative subpoena that required disclosure of trade secrets in a "highly competitive industry" would be fatal to challenger's business and therefore "unreasonable and oppressive").

[21] Similarly, Federal Rule of Criminal Procedure 17(c)(2) allows a court to "quash or modify the subpoena if compliance would be unreasonable or oppressive." Fed. R. Crim. P. 17(c)(2).

Here, as Lavabit has explained, the subpoena had a fatal effect on Lavabit's business. AOB at 28-29. Its business model was so predicated on protecting its client's confidences that, by being forced to disclose its private key, it was also forced to shut its business down. This was not a choice undertaken lightly. Given the Public Key Infrastructure system described above, disclosure of Lavabit's private key was likely to be the death of its business even if Lavabit decided to keep operating. As explained above, once a private key is disclosed to a third party, it is industry standard to revoke the site's security certificate. And that is exactly what happened to Lavabit,[22] effectively shutting down the service.

Faced with an oppressive, unreasonable subpoena for its private key, Lavabit presented the government with a less burdensome alternative by offering to narrow the information to be disclosed pursuant to the subpoena to only that pertaining to the target. *Cf. In re Subpoena Duces Tecum*, 228 F.3d at 349 ("[B]efore a court will conclude that a subpoena is 'arbitrarily excessive,' it may expect the person served 'to have made reasonable efforts . . . to obtain reasonable conditions' from the government." (quoting *Morton Salt,* 338 U.S. at 653)). Lavabit also offered to provide this on a continuing basis, either daily or at the end of the authorized surveillance period. This would have given the government the records it sought

[22] *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/.

on the specific target of the investigation without compromising the security of all of its users. *See* AOB at 8; App. 83. It also would have preserved Lavabit's business model. It would have required Lavabit to spend time and money reconfiguring its computer architecture, but Lavabit offered to do this anyway, provided the government reimbursed the company for its costs.

However, this offer was not good enough for the government, which wanted real-time access to the information, did not think Lavabit's proposed expenses were reasonable, and most crucially, was concerned that the proposal would require it to "trust" Lavabit to turn over information. App. at 83. But none of these are valid grounds for rejecting Lavabit's "reasonable efforts" to obtain less-intrusive subpoena conditions before resorting to the constitutionally unreasonable step of requiring it to turn over the private key. *See In re Subpoena Duces Tecum*, 228 F.3d at 351.

The government's desire for information Lavabit could not provide was not enough to justify a subpoena for the private key. Nor does the government's contention that Lavabit's claimed expenses were unreasonable have any bearing on the constitutional analysis of the subpoena.[23] And, of course, the government's

[23] In any case, the government could have negotiated the price of compliance with Lavabit, as it does with other providers who it must reimburse for its technical assistance in aiding government investigations. *See, e.g.,* 18 U.S.C. § 2706 (government must reimburse provider who discloses electronic communication records); 18 U.S.C. § 3124(c) (government must reimburse provider for technical

need to "trust" that the recipient of a subpoena is complying is inherent in all subpoenas, particularly those requiring the production of paper records.

Above all, the government's unwillingness to consider less burdensome alternatives to the subpoena and the effect it had on Lavabit's e-mail service shows that the subpoena was an arbitrarily excessive means to get at information on a single user. The use of such a "nuclear option" cannot possibly be considered reasonable for the purposes of the Fourth Amendment.

CONCLUSION

Disclosure of a private key threatens the fundamental premise of HTTPS and the security of the Internet. Ultimately it is up to the Courts to impose strict safeguards to preserve the constitutional expectation of privacy in Internet communications, determine that less intrusive alternatives are attempted first and ensure that compliance with a law enforcement request does not mean the death of a business.

Because the government's efforts to obtain Lavabit's private key violated the Fourth Amendment, this Court should reverse the lower court's decision finding Lavabit in contempt of court.

---

assistance in installing a pen register or trap and trace device); 47 U.S.C. § 1008(a) (authorizing reimbursement of "reasonable costs" spent by providers to modify their equipment to be capable of wiretapping); *see also Verizon, AT&T get most bucks from feds for wiretaps,* CBS News (July 11, 2013) http://www.cbsnews.com/8301-201_162-57593273/ (noting different prices different service providers charge the government for wiretaps).

Dated: October 24, 2013

Respectfully submitted,

/s/ Kurt Opsahl

Kurt Opsahl
Jennifer Lynch
Hanni Fakhoury
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Counsel for Amicus Curiae
ELECTRONIC FRONTIER FOUNDATION

**CERTIFICATE OF COMPLIANCE
WITH TYPE-VOLUME LIMITATION,
TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS
PURSUANT TO FED. R. APP. P. 32(a)(7)(C)**

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of Amicus Curiae In Support Of Party-of-Interest-Appellant complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6,573 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

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 proportionally spaced typeface using Microsoft Word 2011, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: October 24, 2013

/s/ Kurt Opsahl
Kurt Opsahl

Counsel for Amicus Curiae
ELECTRONIC FRONTIER FOUNDATION

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Fourth Circuit by using the appellate CM/ECF system on October 24, 2013.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: October 24, 2013

/s/ Kurt Opsahl
Kurt Opsahl

Counsel for Amicus Curiae
ELECTRONIC FRONTIER FOUNDATION