13-4625(L); 13-4626

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 *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION AND ACLU OF VIRGINIA IN SUPPORT OF PARTY-IN-INTEREST—APPELLANT'S APPEAL SEEKING REVERSAL

Alexander A. Abdo
Brian M. Hauss
Catherine Crump
Nathan F. Wessler
Ben Wizner
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500

Rebecca K. Glenberg
American Civil Liberties Union
of Virginia Foundation, Inc.
530 E. Main Street, Suite 310
Richmond, VA 23219
(804) 644-8080

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Regulations

INTEREST OF *AMICI CURIAE*[1]

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with more than 500,000 members dedicated to the principles of liberty and equality embodied in the Constitution and this nation's civil rights laws. The American Civil Liberties Union of Virginia is the ACLU's Virginia affiliate. Since its founding in 1920, the ACLU has frequently appeared before the Supreme Court and this Court, both as direct counsel and as *amicus curiae*, in numerous cases implicating Americans' right to privacy. The ACLU and its members have long been concerned about the impact of new technologies on the right to privacy. The ACLU is particularly concerned with protecting the lawful use of encryption technologies, which are essential to safeguarding the confidentiality of the communications of dissidents, human rights activists, and journalists.

STATEMENT OF FACTS

Lavabit was a secure email service provider. In connection with a criminal investigation into one of Lavabit's customers, government agents obtained a court

[1] The parties have consented to the submission of this brief. Pursuant to Federal Rule of Appellate Procedure 29(c)(5), counsel for *amici curiae* states that no counsel for a party authored this brief in whole or in part, and no person other than *amici curiae*, their members, or their counsel made a monetary contribution to its preparation or submission.

order authorizing the installation of a pen/trap device on Lavabit's servers.[2] The government intended to use the pen/trap device to monitor information associated with the communications of the target of the investigation, such as the "to" and "from" information for email messages sent by the target Lavabit customer. Because all communications between Lavabit's servers and its customers are encrypted, however, the technological method of interception selected by the government could not decrypt, identify, and isolate the data of the particular user targeted by the investigation without also intercepting and scanning the data of Lavabit's 400,000 other users. To accomplish that feat, the government obtained further court orders—including a grand jury subpoena and a Stored Communications Act-authorized search warrant—requiring Lavabit to disclose its private encryption keys. The court denied Lavabit's motion to quash the warrant and the grand jury subpoena, and ordered Lavabit to produce the keys. When the company failed to do so by the stipulated deadline, the court held it in contempt. Although Lavabit ultimately provided its private encryption keys to the

[2] A pen/trap device is a combined pen register and trap and trace device. A pen register is a "device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C. § 3127(3). A trap and trace device is a "device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." *Id.* § 3127(4).

government, its founder decided to shutter the company shortly thereafter, believing that the company could not in good faith hold itself out as operating a secure email service while knowing that its private keys had been divulged.

SUMMARY OF ARGUMENT

Lavabit used Secure Sockets Layer (SSL), an industry-standard encryption technology used by major organizations and companies, from American Express to Google, to protect their users' communications against numerous cyber security threats. SSL technology protects the confidentiality of communications, secures data from tampering, and provides authentication by preventing other parties from impersonating service providers to their users. The protection offered by SSL technology depends on the continued secrecy of the service provider's private encryption keys, which enable the authorized recipients of a particular communication to access the communication's contents. In addition to the use of SSL encryption for all its communications, Lavabit also encrypted each user's stored email messages with a unique private key, which was itself encrypted and directly accessible only to the user. Through the use of these encryption technologies, Lavabit was able to better protect its customers' sensitive information from hacking, theft, and other threats.

Lavabit was under no legal obligation to design its secure email service in a manner that readily facilitated government surveillance. Whereas telephone

companies are statutorily required to construct networks in a way that allows them to facilitate government surveillance efforts, Congress has explicitly refrained from requiring electronic communication service providers like Lavabit to design their services in a way that enables the government to easily access their users' data. In accordance with Congress's decision to allow electronic communication service providers to prioritize cyber security, Lavabit designed a system that was highly resistant to cyber attacks, so long as the company maintained the secrecy of its SSL private encryption keys.

The district court's contempt holding should be reversed because the underlying orders requiring Lavabit to disclose its private keys imposed an unreasonable burden on the company. Although innocent third parties have a duty to assist law enforcement agents in their investigations, they also have a right not to be compelled "to render assistance without limitation regardless of the burden involved." *United States v. New York Tel. Co.*, 434 U.S. 159, 171 (1977). Balancing these interests, the Supreme Court has held that the courts may not impose unreasonable burdens in ordering third parties to assist in government investigations. *Id.* at 172.

Here, the orders requiring Lavabit to disclose its private encryption keys fatally undermined the company's lawful business model, which depended heavily on the security provided by SSL encryption. Because that security in turn depended

on the total secrecy of the company's private encryption keys, their disclosure to the government (once publicly known) would have devastated the company's reputation as a secure email service provider. The orders were also unnecessary because Lavabit offered to create and install onto its servers a narrow, focused, pen-register-like surveillance system capable of providing the non-content information pertaining to the target of the government's investigation—an alternative procedure that would have fulfilled the government's surveillance needs without requiring the company to disclose its private keys. In light of these circumstances, the orders requiring Lavabit to turn over its private encryption keys were unreasonably burdensome.

ARGUMENT

I. LAVABIT USED LEGITIMATE ENCRYPTION TECHNOLOGIES TO PROTECT ITS CUSTOMERS AGAINST CYBER SECURITY THREATS.

The government has publicly expressed concern about the large number of cyber attacks that have plagued American businesses, critical infrastructure, and the government. Encryption technologies help address those threats by preventing unauthorized access to sensitive information. Without such technologies, private information traveling over the Internet would be completely open to interception. For this reason, encryption technologies are used by essentially everyone who uses the Internet. The particular type of encryption at issue here, SSL, is a widely used,

industry-standard technology built into every web browser and used by a large number of popular websites operated by organizations such as Google, American Express, and the federal government's own Health Insurance Marketplace. All of these entities depend on the secrecy of their SSL private encryption keys to ensure the security of users' communications.

Although Lavabit used industry-standard SSL encryption to protect the security of communications between the company and its customers, it also utilized other encryption technologies to make sure that even its own employees could not access the emails stored by its customers on the company's servers. Lavabit's additional encryption measures ensured that even individuals who managed to gain unauthorized access to the company's servers would face severe difficulties in trying to access customers' stored information. The additional encryption measures also made it difficult for Lavabit to facilitate government surveillance activities without either writing new code to provide a targeted method of access to the requested information, as Lavabit offered to do for the government here, or divulging the company's SSL private encryption keys.

A. Encryption Technology Protects Against Cyber Security Threats.

The government has invested much time and energy in convincing the public that cyber security threats are serious. Director of National Intelligence (DNI) James Clapper told the Senate this year that cyber attacks lead the national security

threats faced by the United States.[3] In recent years, foreign governments such as China have hacked into the computer systems of major U.S. companies, including technology firms and defense contractors, stealing intellectual property and classified documents.[4] But cyber threats are not limited to state actors. As then FBI Director Robert Mueller observed earlier this year, "criminals are constantly discovering and exploiting vulnerabilities in our software and our networks."[5] These cyber threats "put all sectors of our country at risk, from government and private networks to critical infrastructures."[6] Private email accounts, in particular,

---

[3] Luis Martinez, *Intel Heads Now Fear Cyber Attack More Than Terror*, ABC News (March 13, 2013), http://abcnews.go.com/Blotter/intel-heads-now-fear-cyber-attack-terror/story?id=18719593.

[4] *See, e.g.*, Edward Wong, *Hacking U.S. Secrets, China Pushes for Drones*, N.Y. Times, Sept. 20, 2013, http://www.nytimes.com/2013/09/21/world/asia/hacking-us-secrets-china-pushes-for-drones.html?_r=0; Ellen Nakashima, *Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies*, Wash. Post, May 27, 2013, http://articles.washingtonpost.com/2013-05-27/world/39554997_1_u-s-missile-defenses-weapons-combat-aircraft ("Designs for many of the nation's most sensitive advanced weapons systems have been compromised by Chinese hackers, according to a report prepared for the Pentagon and to officials from government and the defense industry.").

[5] Robert Mueller, Dir., Fed. Bureau of Investigation, Remarks at International Conference on Cyber Security 2013, Fordham University, Aug. 8, 2013, available at: http://www.fbi.gov/news/speeches/the-future-of-cyber-security-from-the-fbis-perspective.

[6] David Hall, *The Morning Ledger: Cybersecurity Risks Rising*, CFO Journal (Mar. 13, 2013, 6:56 AM), http://blogs.wsj.com/cfo/2013/03/13/the-morning-ledger-cybersecurity-risks-rising/ (quoting remarks by JamesClapper, Dir. Of Nat'l Intelligence).

are a popular target among hackers.[7]

Encryption helps minimize the risk of cyber attacks, in part by mitigating the harm that attackers can cause if they do break into a system.[8] By converting information from its original form to a scrambled form that can be decoded only through the use of a predetermined key, encryption prevents unauthorized individuals with access to the scrambled version of a sensitive communication (such as a password, bank account number, or private email message) from ascertaining its actual contents. *Junger v. Daley*, 209 F.3d 481, 482 (6th Cir. 2000). In the absence of encryption technologies, "Internet communications are similar to the 'party line' style of telephone communications, as any person could 'listen in' on the communications between individuals." *Stambler v. RSA Sec., Inc.*, No. Civ.A. 01-0065-SLR, 2003 WL 22749855, at *2 n.1 (D. Del. Nov. 14, 2003). It would require little effort for even an unsophisticated hacker to intercept an individual's unencrypted emails, financial information, or medical records as they passed over the Internet.

---

[7] Tom Jackman, *Password Hackers Are Slippery to Collar*, Wash. Post, Sept. 7, 2009, http://articles.washingtonpost.com/2009-09-07/news/36883566_1_e-mail-password-sarah-palin-law-professor.

[8] *See* Shawn Henry, Exec. Assistant Dir., Fed. Bureau of Investigation, Remarks at the Information Systems Security Association, Oct. 20, 2011, available at: http://www.fbi.gov/news/speeches/responding-to-the-cyber-threat ("Managing the consequences of a cyber attack entails minimizing the harm that results when an adversary does break into a system. An example would be encrypting data so the hacker can't read it.").

B. Lavabit Employed A Widely Used, Industry-Standard Encryption Technology To Protect Its Communications With Its Customers.

The encryption technology that Lavabit used to protect communications between its servers and its customers is a widely used, industry-standard encryption technology, known by three largely interchangeable terms: SSL (Secure Sockets Layer), HTTPS (Hypertext Transfer Protocol Secure), and TLS (Transport Layer Security).[9] For clarity, this brief refers to these technologies as SSL. "SSL provides security by establishing a secure channel for communications between a web browser and the web server; that is, SSL ensures that the messages passed between the client web browser and the web server are encrypted." *Disney Enters., Inc. v. Rea*, No. 1:12cv687 (LMB/TRJ), 2013 WL 1619686, at *9 (E.D. Va. Apr. 11, 2013). To accomplish this, SSL utilizes a two-key asymmetric encryption method, consisting of a public key and a private key. *Stambler*, 2003 WL 22749855, at *2 n.2. A certificate authority certifies the website's public key, which enables visitors to that site to trust that they are in fact visiting a website run

[9] These are, in fact, three separate technical protocols, all of which aim to deliver the security properties of communications integrity, confidentiality, and authentication. *See generally* Alan Freier, Philip Karlton & Paul Kocher, *The Secure Sockets Layer (SSL) Protocol Version 3.0*, Internet Engineering Task Force Request for Comment 6101, August 2011, http://tools.ietf.org/html/rfc6101; Tim Dierks & Eric Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.2*, Internet Engineering Task Force Request for Comment 5246, August 2008, http://tools.ietf.org/html/rfc5246; Eric Rescorla, *HTTP Over TLS*, Internet Engineering Task Force Request for Comment 2818, May 2000, http://tools.ietf.org/html/rfc2818. The technical differences between these protocols are not relevant to the issues in this case.

by the organization named in the certificate.[10] The public key is published online and shared with visitors to the website, permitting them to encrypt their communications with the website. *Stambler*, 2003 WL 22749855, at *2 n.2. The website, using its unique private key, may then decrypt communications encoded by users with the public key. *Id.*[11]

Because only the website operator knows its private key, users can rest assured that anyone else who intercepts their communications with the website will be unable to read the encrypted information. This process, however, depends on the secrecy of the website's private key. For this reason, companies like Microsoft, Google, and Facebook have stated that they have never shared their SSL private encryption keys with the government and would vigorously challenge any government order requiring them to do so.[12] And the website certificates themselves are, as a standard policy, revoked (i.e., publicly identified as untrustworthy) by the issuing certificate authority whenever it becomes apparent that private encryption keys have been lost, stolen, or disclosed to an unauthorized

---

[10] *See generally* Steven Roosa & Stephen Schultze, *Trust Darknet: Control and Compromise in the Internet's Certificate Authority Model*, 17 IEEE Internet Computing 18, 18 (2013), available at: http://www.computer.org/csdl/mags/ic/2013/03/mic2013030018.pdf.

[11] *See generally Public-key cryptography*, Wikipedia (last updated Oct. 23, 2013), http://en.wikipedia.org/wiki/Public-key_cryptography.

[12] Declan McCullagh, *Feds Put Heat on Web Firms for Master Encryption Keys*, CNET (July 24, 2013, 4:00 AM), http://news.cnet.com/8301-13578_3-57595202-38/feds-put-heat-on-web-firms-for-master-encryption-keys/.

party, including the government. Indeed, that is precisely what happened in this case: Lavabit's certificate authority, GoDaddy, revoked the certificate for the company's website as soon as media reports revealed that Lavabit had provided the government its private encryption keys in compliance with the court's orders.[13]

SSL is "widely considered to be the standard method for conducting secured communications via the Internet." *Stambler*, 2003 WL 22749855, at *2. Support for it is built into the web browser software used by hundreds of millions of consumers. And the technology is enabled by default by major financial institutions;[14] popular communications services, such as Google Mail,[15] Facebook,[16] and Twitter;[17] and even federal agencies, including the Central

[13] *See* Kashmir Hill, *GoDaddy Pulls Lavabit's Security Creds Because the FBI Got Ahold of Its Encryption Keys*, Forbes (Oct. 9, 2013, 8:01 PM), http://www.forbes.com/sites/kashmirhill/2013/10/09/godaddy-pulls-lavabits-security-creds-because-the-government-got-ahold-of-its-encryption-keys/.

[14] *See, e.g.*, *Security and Support FAQs*, Bank of America, https://www.bankofamerica.com/onlinebanking/online-banking-security-faqs.go (last visited Oct. 21, 2013); *Online Security: Enforcing Safe Online Banking Practices*, Chase, https://www.chase.com/resources/online-banking-security#!chase-online-security:enforcing-safe-online-banking-practices (last visited Oct. 21, 2013); *Security Center: Online Protection*, American Express, https://www.americanexpress.com/us/content/fraud-protection-center/online-protection.html (last visited Oct. 21, 2013).

[15] Sam Schillace, *Default HTTPS Access for Gmail*, Official Gmail Blog (Jan. 12, 2010), http://gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html (explaining that "using https helps protect data from being snooped by third parties" and stating that "turning https on for everyone was the right thing to do").

[16] *Secure Browsing by Default*, Facebook (July 31, 2013), http://www.facebook.com/notes/facebook-engineering/secure-browsing-by-

Intelligence Agency,[18] the federal government's Affordable Care Act Health Insurance Marketplace,[19] and parts of the PACER system run by the Administrative Office of the U.S. Courts.[20] Google's decision to enable SSL by default for its email service in 2010 resulted in public praise from the Federal Bureau of Investigation's General Counsel,[21] while the slow speed of SSL

---

default/10151590414803920 ("Turning on https by default is a dream come true, and something Facebook's . . . teams have worked on for years. We're really happy with how much of Facebook's traffic is now encrypted.").

[17] *Securing Your Twitter Experience with HTTPS*, Twitter Blogs (Feb. 13, 2012), https://blog.twitter.com/2012/securing-your-twitter-experience-with-https ("HTTPS is one of the best ways to keep your account safe.").

[18] Press Release, Central Intelligence Agency, *Statement on CIA Website Enhancement*, July 17, 2006, available at: https://www.cia.gov/news-information/press-releases-statements/press-release-archive-2006/statement-on-cia-website-enhancement.html ("We believe the inconveniences of implementing SSL for the entire website will be offset by increased visitor confidence that they are, in fact, connected to the CIA website and that their visits are secure and confidential.").

[19] Max Eddy, *Beware of Fake Obamacare Insurance Marketplace Sites*, SecurityWatch, PC Magazine (Oct. 3, 2013), http://securitywatch.pcmag.com/security/316473-beware-of-fake-obamacare-insurance-marketplace-sites.

[20] *Register for a PACER (Case Search) Account*, PACER, https://www.pacer.gov/psco/cgi-bin/regform.pl (last accessed Oct. 21, 2013) ("Note: We protect the security of your information during transmission using Secure Sockets Layer (SSL) software.").

[21] Valerie Caproni, Statement Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*, Hearing, Feb. 17, 2011 (Serial 112-59), available at: http://judiciary.house.gov/hearings/printers/112th/112-59_64581.PDF ("Google, for the last 9 months, has been encrypting all gmail. So as it travels on the Internet, it is encrypted. We think that is great.").

adoption by other major technology companies led to public criticism from both a Federal Trade Commission Commissioner and a U.S. Senator.[22] The adoption of SSL by default by several major email and social networking services has been praised by Federal Trade Commission Chairwoman Edith Ramirez as an example of companies "lift[ing] the burden of privacy protection off the shoulders of consumers."[23] And the technology has been recommended by numerous federal agencies with cyber security expertise, including the National Security Agency,[24] the Federal Communications Commission,[25] the Federal Trade Commission,[26] and the Department of Homeland Security.[27]

---

[22] *See* Commissioner Pamela Jones Harbour, Remarks Before Third Federal Trade Commission Exploring Privacy Roundtable in Washington, D.C., Mar. 17, 2010, available at: http://www.ftc.gov/speeches/harbour/100317privacyroundtable.pdf); Press Release, Senator Charles E. Schumer, *Schumer: Wireless Network Connections at Coffee Houses and Bookstores Allow Easy Access to Hackers; Allows Them to Steal Private Information on Users of Popular Websites Like Twitter, Yahoo, and Amazon* (Feb. 28, 2011), available at: http://www.schumer.senate.gov/record.cfm?id=331455 ("It's my hope that the major sites will immediately put in place secure HTTPS web addresses.").

[23] Commissioner Edith Ramirez, Remarks at Privacy by Design Conference, *Privacy by Design and the New Privacy Framework of the U.S. Federal Trade Commission* 3, June 13, 2013, available at: http://www.ftc.gov/speeches/ramirez/120613privacydesign.pdf.

[24] *See, e.g.*, Enter. Applications Div. of the Sys. and Network Analysis Ctr., Nat'l Sec. Agency, *Guidelines for Implementation of REST* 14, available at: http://www.nsa.gov/ia/_files/support/guidelines_implementation_rest.pdf ("Encryption should always be used to transfer data or sensitive information.").

[25] *See* Federal Communications Commission, *Cyber Security Planning Guide* WS-4, available at:

Indeed, SSL encryption is so effective that it is often required by law or industry regulation. The State of Massachusetts, for example, requires that companies use encryption to protect "all transmitted records and files containing personal information that will travel across public networks, and . . . all data containing personal information to be transmitted wirelessly." 201 Mass. Code Regs. 17.04(3); *see also*, *e.g.*, Nev. Rev. Stat. § 603A.215(2); Minn. Stat. § 62J.55(a). And major credit card companies—including VISA, Mastercard, and American Express—have established industry standards that require merchants and other companies to use SSL to protect credit card information as it is transmitted over the Internet.[28] Thus, there can be little doubt that Lavabit was acting in accord

---

http://www.dhs.gov/sites/default/files/publications/FCC%20Cybersecurity%20Planning%20Guide_1.pdf.

[26] *See* Federal Trade Commission, *Tips for Using Public Wi-Fi Networks*, OnGuardOnline.gov (Sept. 2011), http://www.onguardonline.gov/articles/0014-tips-using-public-wi-fi-networks.

[27] *See* Department of Homeland Security, *Protecting Your Personal Information with Secure Passwords* (May 8, 2013, 1:44 PM), http://www.dhs.gov/blog/2013/05/08/protecting-your-personal-information-secure-passwords (encouraging consumers to make sure that the webpages where they submit account information are encrypted).

[28] *See About Us*, PCI Security Standards Council, https://www.pcisecuritystandards.org/organization_info/index.php (last visited Oct. 21, 2013); PCI Security Standards Council, *Payment Card Industry Data Security Standard: Requirements and Security Assessment Procedures v.2.0* 35 (Oct. 2010), available at: https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf.

with industry-wide best practices and procedures when it adopted SSL encryption for its secure email service.

C. Lavabit Also Employed Additional Encryption Technology To Ensure The Security Of Its Customers' Sensitive Information.

The SSL technology used by Lavabit was just one component of the company's secure email service. In addition to encrypting communications between subscribers and the company's servers with SSL, the company also used a different encryption technology to encrypt emails that were stored on the company's servers. The encrypted messages stored on Lavabit's servers could be decrypted only through the use of a unique private key, which was different for every user. That private key was itself encrypted and could be decoded only when the end-user entered his or her password.[29] Lavabit's servers had brief access to the passwords, private encryption keys, and the unencrypted copies of emails while interacting with users' computers, but the passwords and unencrypted data were quickly wiped from the memory of Lavabit's servers as soon as any transaction was completed.[30]

Although the SSL encryption used by Lavabit is an industry-standard technology, the encryption of stored emails with unique encryption keys for each

[29] *See* Dan Goodin, *How Might the Feds Have Snooped on Lavabit*, Ars Technica (Aug. 25, 2013, 8:00 PM), http://arstechnica.com/tech-policy/2013/08/how-might-the-feds-have-snooped-on-lavabit/.
[30] *Id.*

user is not common among major email service providers, such as Google. That is because Google and other email service providers derive advertising revenue from their ability to scan customers' emails. As Vint Cerf, Google's Chief Internet Evangelist, explained, "[w]e couldn't run our system if everything in it were encrypted because then we wouldn't know which ads to show you. So [our service] was designed around a particular business model."[31] Whereas Google's use of SSL encryption effectively protects the communications as they are transmitted to and from the company's servers, anyone inside the company—including Google's employees and hackers that have penetrated the company's security defenses—has the ability to access sensitive customer data stored on the company's servers.[32] By contrast, even Lavabit's own employees could not read the information stored on

[31] Vint Cerf, Remarks, Sixth Annual Meeting of the Internet Governance Forum, *Global Trends to Watch: The Erosion of Privacy and Anonymity and The Need of Transparency of Government Access Requests*, Sept. 29, 2011, available at: http://www.intgovforum.org/cms/component/content/article/71-transcripts-/894-sop-workshop-160-global-trends-to-watch-the-erosion-of-privacy-and-anonymity-and-the-need-of-transparency-of-government-access-requests.

[32] Indeed, Google has fired engineers who misused their access to the company's servers in order to read the communications of Google customers. *See* Ryan Tate, *David Barksdale Wasn't Google's First Spying Engineer*, Gawker (Sept. 15, 2010, 2:41 PM), http://gawker.com/5638874/david-barksdale-wasnt-googles-first-spying-engineer. And the Los Angeles Police Department refused to use Google's "cloud" based email services, specifically because they were concerned about Google employees having access to sensitive police emails. Jaikumar Vijayan, *Los Angeles Drop Plans to Move to Google Apps*, TechWorld (Dec. 27, 2011, 12:11 PM), http://news.techworld.com/data-centre/3326744/los-angeles-police-drop-plans-move-google-apps/.

the company's servers, because the company did not have access to the passwords and unique private keys necessary to decrypt the messages.

Lavabit's use of multiple encryption layers protected its users' communications against all but the most virulent of cyber attacks. Even if someone were to break into Lavabit's servers, she would have a much harder time accessing stored customer information.[33] It also made it exceedingly difficult for the company to facilitate government surveillance efforts without either modifying the company's computer code to offer a targeted method for accessing the requested information—an offer the government rejected in this case—or disclosing the private keys upon which the security of *all* Lavabit's customer communications depended.

II. LAVABIT HAD NO OBLIGATION TO PROVIDE AN EMAIL SERVICE THAT IS EASY TO SURVEIL.

Although Lavabit could have designed its email service to more readily facilitate government surveillance, the company was under no obligation to do so.[34] Whereas Congress has required telecommunications carriers, such as

[33] Goodin, *supra* n.29.

[34] Indeed, several companies and organizations sell or distribute communications software that is far less amenable to government surveillance requests than Lavabit's system was. *See, e.g.*, Ryan Gallagher, *Instead of "Dead Dropping," Petraeus and Broadwell Should Have Used These Email Security Tricks*, Slate (Nov. 13, 2012, 4:14 PM), http://www.slate.com/blogs/future_tense/2012/11/13/petraeus_and_broadwell_sho

telephone companies, to build surveillance capabilities into their networks that enable the government to intercept users' communications and related metadata in real time, it has explicitly refrained from extending this requirement to email service providers.

When Congress enacted the Communications Assistance for Law Enforcement Act ("CALEA") in 2004, it required "telecommunications carriers" to ensure that their equipment, facilities, and services are capable of "enabling the government . . . to intercept" users' communications and access users' call-identifying information. 47 U.S.C. § 1002(a). In other words, CALEA required telecommunications carriers to construct technological "backdoors" enabling law enforcement agencies to intercept, in real time, callers' communications and metadata. CALEA also, however, specifically exempted "information services," including "electronic messaging services" like Lavabit, from this requirement. *Id.* §§ 1002(b)(2), 1001(6)(B)(iii). The exclusion of "information services" was intended to address privacy concerns,[35] and was achieved with the agreement of

---

uld_have_used_pgp_encryption_and_tor_not_dead.html (describing effectiveness of Pretty Good Privacy (PGP) encryption and The Onion Router (Tor) anonymity tool).

[35] H.R. Rep. No. 103-827, at 18 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3498 ("It is also important from a privacy standpoint to recognize that the scope of the legislation has been greatly narrowed. . . . [E]xcluded from coverage are all information services, such as Internet service providers or services such as Prodigy and America-On-Line.").

the FBI.[36] The House Committee Report explained that Congress was rejecting "[e]arlier digital telephony proposals [that] covered all providers of electronic communications services" because "[t]hat broad approach was not practical. Nor was it justified to meet any law enforcement need."[37]

Recently, federal law enforcement officials have begun to seek amendments to CALEA requiring "all services that enable communications — including encrypted e-mail transmitters like BlackBerry . . . — to be technically capable of complying if served with a wiretap order."[38] Although the FBI has sought such changes to CALEA in recent sessions of Congress,[39] Congress has refused to expand the statute's reach. The FBI's proposals have met resistance in Congress, as well as from the business community, because of concerns that "legislatively

---

[36] Louis J. Freeh, Dir., Fed. Bureau of Investigation, Statement Before the Subcomm. on Telecomms. & Fin. of the H. Comm. on Energy & Commerce, *Wiretapping Access*, Hearing, Sept. 13, 1994, 1994 WL 497163 ("The language of the legislation reflects reasonableness in every provision. For example, the coverage of the legislation focuses on common carriers . . . . [I]nformation services are excluded.").

[37] H.R. Rep. No. 103-827, at 18.

[38] *See* Charlie Savage, *U.S. Tries to Make it Easier to Wiretap the Internet*, N.Y. Times, Sept. 27, 2010, http://www.nytimes.com/2010/09/27/us/27wiretap.html.

[39] *See* Caproni, *supra* n.21; Charlie Savage, *U.S. Weighs Wide Overhaul of Wiretap Laws*, N.Y. Times, May 7, 2013, http://www.nytimes.com/2013/05/08/us/politics/obama-may-back-fbi-plan-to-wiretap-web-users.html; Ellen Nakashima, *Panel Seeks to Fine Tech Companies for Noncompliance with Wiretap Orders*, Wash. Post, Apr. 28, 2013, http://articles.washingtonpost.com/2013-04-28/world/38885216_1_wiretap-proposal-companies.

forcing telecommunications providers to build back doors into systems will actually make us less safe and less secure. . . . [R]equiring back doors in all communications systems by law runs counter to how the Internet works and may make it impossible for some companies to offer their services."[40] Congress has had ample opportunity to compel email service providers to build standardized technological interception backdoors into their products and services for government surveillance purposes, but has chosen not to do so.

Congress's choice to allow electronic communication service providers to prioritize cyber security over ease of government access to subscriber data is amply supported by the cyber security concerns discussed in Section I.A. Indeed, technical experts have repeatedly opposed U.S. government legislative proposals to mandate the creation of interception capabilities in Internet systems, specifically because they weaken the security of those systems.[41] In contrast to the relative

[40] Rep. John Conyers, Statement Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*, Hearing, Feb. 17, 2011 (Serial 112-59). *Accord* Ben Adida, et al., *CALEA II: Risks of Wiretap Modifications to Endpoints*, Center for Democracy & Technology (May 17, 2013), available at: https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf.

[41] *See id.*; Susan Landau, Statement Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*, Hearing, Feb. 17, 2011 (Serial 112-59), available at: http://judiciary.house.gov/hearings/pdf/Landau02172011.pdf; Stephanie K. Pell, *Jonesing for a Privacy Mandate, Getting a Technology Fix – Doctrine to Follow*,

security of many email communications systems, telephone networks are not secure, and are therefore vulnerable to interception by criminals and foreign governments.[42] Moreover, so-called "lawful interception systems" in telephone and email services are often irresistible hacking targets.[43]

Consistent with Congress's decision to allow electronic communication service providers a free hand in prioritizing cyber security, Lavabit established a secure email service that made it extremely difficult for unauthorized entities to intercept or otherwise access users' communications and data. Only Lavabit's SSL

---

14 N.C. J. L. & Tech. 489, 533 (2013) ("[W]hen compromised, an encrypted communications system with a lawful interception back door is far more likely to result in the catastrophic loss of communications confidentiality than a system that never has access to the unencrypted communications of its users.").

[42] *See, e.g.*, Kim Zetter, *Hacker Spoofs Cell Phone Tower to Intercept Calls*, Wired (July 31, 2010, 7:57 PM), http://www.wired.com/threatlevel/2010/07/intercepting-cell-phone-calls/ (describing a public demonstration by a security researcher in which he showed that he could trick nearby cell phones into using his own cellular tower rather than AT&T's network, which enabled him to intercept calls).

[43] *See* Ellen Nakashima, *Chinese Hackers who Breached Google Gained Access to Sensitive Data, U.S. Officials Say*, Wash. Post, May 20, 2013, http://articles.washingtonpost.com/2013-05-20/world/39385755_1_chinese-hackers-court-orders-fbi (revealing that Chinese hackers broke into the lawful interception systems of Google and Microsoft in 2009 in order to learn which Chinese agents U.S. law enforcement and intelligence agencies were monitoring); Vassilis Prevelakis & Diomidis Spinellis, *The Athens Affair: How Some Extremely Smart Hackers Pulled Off the Most Audacious Cell-Network Break-In Ever*, IEEE Spectrum (June 29, 2007, 2:07 PM), http://spectrum.ieee.org/telecom/security/the-athens-affair (describing the compromise of the lawful interception system of Vodafone Greece in 2004, allowing the attackers to secretly listen to the calls of the Greek prime minister, the defense and foreign affairs ministers, top military and law enforcement officials, and journalists).

private encryption keys could decipher intercepted communications between the company and its customers, and Lavabit accordingly treated those keys as its most closely guarded secrets.

III. THE COURT ORDERS COMPELLING LAVABIT TO DISCLOSE ITS PRIVATE KEYS WERE UNREASONABLY BURDENSOME.

The ACLU supports the arguments put forth by Lavabit in its merits brief. As an alternative to the grounds for reversal raised in Lavabit's brief, this Court could conclude that the orders requiring Lavabit to turn over its private keys were unreasonably burdensome, and therefore invalid.

"[T]he power of federal courts to impose duties upon third parties is not without limits; unreasonable burdens may not be imposed." *New York Tel. Co.*, 434 U.S. at 172; *see also United States v. Mountain States Tel. & Tel. Co.*, 616 F.2d 1122, 1132 (9th Cir. 1980) (affirming a district court's order compelling Mountain States to trace telephone calls by using electronic facilities within the company's exclusive control, on the ground that "the obligations imposed . . . were reasonable ones" (citing *New York Tel. Co.*, 434 U.S. at 172)); *The Company v. United States*, 349 F.3d 1132, 1148 (9th Cir. 2003) (holding that the Federal Wiretap Act prohibited a court order requiring a company to disrupt its emergency communication service so as to enable government surveillance) (Tallman, J.,

dissenting) ("Service disruption that is severe enough to result in serious adverse effects on a provider may be prohibited by the doctrine of undue burden.").[44]

In *New York Telephone*, the Supreme Court upheld a court order, issued under the auspices of Federal Rule of Criminal Procedure 41 and the All Writs Act, requiring a private telephone company to provide a telephone line for the installation of a pen register device. 434 U.S. at 164, 175–78. In so holding, the Court explained that the order at issue was justified because it "required minimal effort on the part of the Company and no disruption to its operations." *Id.* at 175. The Court observed that the company was a "highly regulated public utility" that "regularly employ[ed] [pen-register] devices without court order for the purposes of checking billing operations, detecting fraud, and preventing violations of law." *Id* at 174–75. Under such circumstances, the judicially compelled installation of a pen register device was "by no means offensive to [the company]." *Id* at 174.

Here, by contrast, the government demanded something that Lavabit would never have voluntarily provided to a customer or any other party, because doing so would have ruined the company. To be sure, turning over the private keys did not

[44] Although *New York Telephone* involved an order issued pursuant to Federal Rule of Criminal Procedure 41 and the All Writs Act, it has been suggested that the doctrine also applies to statutory orders compelling third-party service providers to assist in government surveillance efforts. *See The Company*, 349 F.3d at 1148 (Tallman, J., dissenting) (stating, in a Title III wiretap case, that the undue burden doctrine prohibits service disruption that is severe enough to have serious adverse effects on a provider (citing *New York Telephone*)).

cause any technical disruption to Lavabit's email service, but it completely undermined Lavabit's lawful business model, which was to provide a genuinely secure email service.[45]

Access to the private encryption keys would have enabled the government—and anyone else who obtained or stole the private keys from the government—to eavesdrop on all the data traveling to and from Lavabit's email servers, including: the contents of emails, email metadata, credit card numbers, the contents of all communications between Lavabit and its customers, and passwords that could be used to decrypt customers' stored email messages. Because SSL private encryption keys are also used to authenticate the identity of websites, access to the keys would also allow others to impersonate Lavabit in dealings with the company's customers.[46] Lavabit's concern that its encryption keys could be used for impersonation, Lavabit Br. at 7, is neither overblown nor theoretical. High-profile email providers have been the victims of impersonation attacks in the past—in

[45] *Security Through Asymmetric Encryption*, Lavabit, http://web.archive.org/web/20130115081000/http://lavabit.com/secure.html (archived Jan. 15, 2013).

[46] *See, e.g.*, *Man-in-the-Middle Attack*, Wikipedia, http://en.wikipedia.org/wiki/Man-in-the-middle_attack (describing a type of impersonation attack) (last updated Oct. 11, 2013).

2011, for example, hackers impersonated Google for the purpose of spying on its Iranian users.[47]

Lavabit could not have withstood the massive business disruption, loss of consumer confidence, and hemorrhaging of customers that would have likely resulted after the public learned that the company had been forced to divulge its private encryption keys.[48] The market for email services is highly competitive, and dominated by large companies that offer vast amounts of storage space for free to consumers. Security was the only advantage that Lavabit had over larger competitors like Google and Yahoo. If the company were forced to subvert such a fundamental aspect of its security—the private encryption keys were the company's self-described "crown jewels," Lavabit Br. at 4—it would have lost its only competitive advantage, as well as the trust of its 400,000 users.

These concerns are not speculative. Several years ago, the United States Drug Enforcement Agency (DEA) compelled Hushmail—a Canada-based

---

[47] *See* Somini Sengupta, *In Latest Breach, Hackers Impersonate Google to Snoop on Users in Iran*, N.Y. Times, Aug. 30, 2011, http://www.nytimes.com/2011/08/31/technology/internet/hackers-impersonate-google-to-snoop-on-users-in-iran.html.

[48] The government forbade Lavabit from telling anyone that its security had been breached, *see* App. 1–2, 11–12, but the company would have been required to disclose the breach as soon as it was legally able to do so. Most states, including Lavabit's home state of Texas, require companies to report security breaches that expose customers' personal information. *See* Tex. Bus. & Com. Code Ann. § 521.053 (requiring companies to notify state residents where encrypted data has been acquired by an unauthorized person who has the key to decrypt it).

company that then dominated the secure web-based email service market—to subvert the security of its encrypted email service by modifying its service to secretly capture the passwords of several users, unlock their respective private encryption keys, and decrypt their emails, all pursuant to a Canadian court order obtained through a mutual legal assistance treaty.[49] Hushmail's court-ordered cooperation with the investigation did not directly implicate the privacy of non-targeted users, but the company had advertised its product as a secure email service, and was thus subjected to a barrage of negative publicity after information about its surveillance assistance appeared in court documents.[50] Although Hushmail remains in business, news coverage about the surveillance assistance it was forced to provide destroyed the company's reputation as a provider of secure, encrypted email. Whereas the government required Hushmail to provide only particular users' data, Lavabit faced a demand for the private encryption keys protecting *all* of its users' data, and would likely have fared much worse.

---

[49] Ryan Singel, *Encrypted E-Mail Company Hushmail Spills to Feds*, Wired (Nov. 7, 2007, 3:39 PM), http://www.wired.com/threatlevel/2007/11/encrypted-e-mai/.

[50] *See, e.g.*, Mark Hopkins, *Hushmail Offers Feds a Peek at Users' Data*, Mashable (Nov. 7, 2007), http://mashable.com/2007/11/07/hushmail-offers-feds-a-peek-at-users-data/; John Leyden, *Hushmail Open to Feds with Court Orders*, The Register (Nov. 8, 2007), http://www.theregister.co.uk/2007/11/08/hushmail_court_orders/; Mike Masnick, *Hushmail Turns Out to Not Be Quite so Hush Hush*, Techdirt (Nov. 9, 2007, 12:37 AM), http://www.techdirt.com/articles/20071108/093110.shtml.

Other secure electronic communication service providers have also shuttered their businesses in the wake of Lavabit's ordeal. Silent Circle, one of Lavabit's competitors, shut down its secure email service the day after Lavabit closed its doors.[51] Jon Callas, one of Silent Circle's founders and its Chief Technology Officer, said that although the company had not received any "subpoenas, warrants, security letters, or anything else by any government," it saw the "writing [on] the wall" after Lavabit's case became public and decided it was best to shut down the company's email service right away.[52] And CryptoSeal, a provider of virtual private networks that can be used to browse the Internet anonymously, announced that its own decision to shut down was largely influenced by what happened to Lavabit.[53] Ryan Lackey, one of CryptoSeal's cofounders and a onetime contractor for the United States Army, explained that "[t]he post-Lavabit interpretation of a pen register order being enough to complete turnover of the

[51] Pammy Olson, *Encryption App Silent Circle Shuts Down Email Service "To Prevent Spying,"* Forbes (Aug. 9, 2013, 12:41 PM), http://www.forbes.com/sites/parmyolson/2013/08/09/encryption-app-silent-circle-shuts-down-e-mail-service-to-prevent-spying/.

[52] Jon Callas, *To Our Customers*, Silent Circle (Aug. 9, 2013), http://silentcircle.wordpress.com/2013/08/09/to-our-customers/.

[53] Ryan Gallagher, *Citing "Terrifying" Surveillance Tactics, Yet Another U.S. Privacy Service Shuts Down*, Slate (Oct. 22, 2013, 3:51 PM), http://www.slate.com/blogs/future_tense/2013/10/22/cryptoseal_yet_another_u_s_privacy_service_shuts_down.html.

service, if that's the most effective way for [the government] to get pen register data, is terrifying."[54]

The Court's decision in *New York Telephone* also hinged on the observation that the company's assistance was "essential to the fulfillment of the purpose—to learn the identities of those connected with the gambling operation—for which the pen register order had been issued." 434 U.S. at 175. Here, on the other hand, the government could have obtained the information it sought through alternative means that would not have fatally compromised Lavabit's secure email service. Lavabit offered to write new code that would allow it to provide daily updates of the non-content information related to the target of the government's investigation, including 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. The government resisted Lavabit's proposed accommodation, even though it would have provided access to the information sought without compromising Lavabit's private keys, on the ground that it would not have provided "real-time access" to the target's data. *Id.* Despite the government's objection, Lavabit's proposed alternative would have substantially achieved the government's investigatory objectives with significantly less interference to Lavabit's legitimate business interests.

[54] *Id.*

Although Lavabit could have originally designed an email service that would have made it easier for the company to assist the government's investigation, the unreasonable burden analysis does not depend on such counterfactuals. Rather, this Court must determine whether the district court's orders were unreasonably burdensome to the service that Lavabit actually (and lawfully) built. Whatever limits exist on the government's power to compel the assistance of third parties in criminal investigations, those limits surely prohibit the government from demanding that a company destroy its entire business for the sake of information that could be obtained through other means.

CONCLUSION

For the foregoing reasons, this Court should vacate the district court's contempt finding, reverse the associated fines assessed against Lavabit, and compel the government to return or destroy Lavabit's private keys.

Respectfully submitted,

Dated: October 24, 2013

By: /s/ Alexander A. Abdo

Alexander A. Abdo
Brian M. Hauss
Catherine Crump
Nathan F. Wessler
Ben Wizner
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Telephone: 212.549.2500
Facsimile: 212.549.2654
Email: aabdo@aclu.org

Rebecca K. Glenberg
AMERICAN CIVIL LIBERTIES UNION OF VIRGINIA FOUNDATION, INC.
530 E. Main Street, Suite 310
Richmond, VA 23219
Telephone: 804.644.8080
Facsimile: 804.649.2733
Email: rglenberg@acluva.org

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a) because it contains 6,794 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(a)(7)(B)(iii).
2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type-style requirements of Federal Rule of Appellate Procedure 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in 14-point Times New Roman.

/s/ Alexander A. Abdo

Alexander A. Abdo

October 24, 2013

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 24th day of October, 2013, the foregoing *Amici Curiae* Brief for American Civil Liberties Union was filed electronically through the Court's CM/ECF system. Notice of this filing will be sent by e-mail to all parties by operation of the Court's electronic filing system.

/s/ Alexander A. Abdo

Alexander A. Abdo