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

INTEREST OF *AMICI CURIAE*

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

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

are a popular target among hackers.

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 com3.7s85iJihiciSeb85iJineSuLe(it)9(.2

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*, Wikiped004 TcM2odr>s3b84 0 Tdi -8.s C0-0 0 278 1,

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

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. R

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 niqun u i [(t)0.5(h)-8iSL tquL te L t u athe

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.

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

telephone companies, to build surveillance capabilities into their networks that enable the government to intercept users' communications and related metadata in

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-

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

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,

2011, for /CS0 c /o4sCS0-1.92.4ad,5(m)]TJ c 0.087 Tw 17104 -6.2224 7Td.3(ple)3,5(,)6.2

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]

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

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

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