NO. 15-3537

IN THE UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

UNITED STATES OF AMERICA,

APPELLEE,

v.

APPLE MACPRO COMPUTER, et al.

JOHN DOE,

MOVANT-APPELLANT.

On Appeal from the United States District Court
for the Eastern District of Pennsylvania
Case No. 2:15-mj-00850-001

The Honorable L. Felipe Restrepo, United States District Court Judge

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION AND AMERICAN CIVIL LIBERTIES UNION IN SUPPORT OF MOVANT-APPELLANT AND REVERSAL

Kit Walsh
Adam Schwartz
Mark Rumold
Jamie Williams
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Email: kit@eff.org
Telephone: (415) 436-9333

Counsel for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *Amici Curiae* Electronic Frontier Foundation and American Civil Liberties Union state that they do not have parent corporations and that no publicly held corporation owns 10 percent or more of their stock.

Dated: April 6, 2016

By: /s/ Kit Walsh

Kit Walsh
Adam Schwartz
Mark Rumold
Jamie Williams
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
kit@eff.org

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENT OF INTEREST[1]

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that works to protect free speech and privacy in the digital world. Founded in 1990, EFF has over 26,000 active donors and dues-paying members across the United States. EFF represents the interests of technology users in both court cases and broader policy debates surrounding the application of law in the digital age. EFF has participated as *amicus curiae* in several cases regarding the application of the Fifth Amendment to compelled decryption, including *In re Grand Jury Subpoena*, 670 F.3d 1335 (11th Cir. 2012); *United States v. Fricosu*, 841 F. Supp. 2d 1232 (D. Colo. 2012); *United States v. Decryption of a Seized Data Storage System*, No. 2:13-mj-449-RTR (D. Wisc. 2013); and *Commonwealth v. Gelfgatt*, 11 N.E.3d 605 (Mass. 2013).

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with approximately 500,000 members dedicated to the principles of liberty and equality embodied in the Constitution and this nation's civil rights laws. Since its founding in 1920, the ACLU has frequently appeared before the Supreme Court and other federal courts in numerous cases implicating Americans' right to privacy.

[1] Pursuant to Federal Rule of Appellate Procedure Rule 29(c), *Amici* certify that no person or entity, other than *Amici*, their members, or their counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part. Both parties consent to the filing of this brief.

Amici submit this brief to help the Court apply the Fifth Amendment in a manner that ensures the constitutional rights of those who use encryption. Encryption is a fundamental and widely used safeguard for businesses and individuals to protect their privacy and security. Principled application of the Fifth Amendment's self-incrimination privilege is therefore vital.

INTRODUCTION

"At the time of the American Revolution," the nation's founders "did not believe codes and ciphers were employed for purposes of evil and cruelty."[2] Rather, encryption was "an essential instrument for protecting critical information[.]"[3]

Today, this critical information is digital. For many, if not most, Americans, our computers, phones, and other electronic devices contain a catalogue of information as diverse as the thoughts in our mind. These devices, and the information they contain, define our "familial, political, professional, religious, and sexual associations." *United States v. Jones*, 565 U.S. ___, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., *concurring*).

Like the founders, Americans today use encryption to protect their devices and the critical information they contain.

In this case, through the ongoing imposition of civil contempt, the government seeks to compel the target of their investigation ("Mr. Doe") to facilitate law enforcement's ability to understand information stored on encrypted

---

[2] Ralph E. Weber, *Masked Dispatches: Cryptograms and Cryptology in American History, 1775-1900*, National Security Agency Center for Cryptologic History (2013), xi (internal quotations omitted), https://www.nsa.gov/about/_files/cryptologic_heritage/publications/prewii/masked_dispatches.pdf.

[3] *Id*.

electronic devices—information the government believes will disclose evidence of criminal activity.

This compulsion places Mr. Doe in precisely the "cruel trilemma" of self-incrimination, perjury, or contempt—that the Fifth Amendment was designed to protect against. *See Murphy v. Waterfront Comm'n of New York Harbor*, 378 U.S. 52, 55 (1964). The principles animating the self-incrimination privilege remain as relevant today as they were at our nation's founding, and the circumstances present here do not justify bending those principles to accommodate present law enforcement desires.

Accordingly, the order of the court below should be reversed for two reasons:

First, compelled decryption is inherently testimonial because it compels a suspect to use the contents of their mind to translate unintelligible evidence into a form that can be used against them. The Fifth Amendment provides an absolute privilege against such self-incriminating compelled decryption.

Second, even if compelled decryption were not inherently testimonial, it would be in this case because complying with the order would communicate facts that are not foregone conclusions already known to the government. *See In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335, 1346, 1349 (11th Cir. 2012). Specifically, the government has not demonstrated its knowledge of the existence

of any specific files on the encrypted drives with reasonable particularity.

Thus, the order the government seeks to enforce is unconstitutional. If the Court orders the decryption of any encrypted information on condition of immunity, then Mr. Doe must be provided both use and derivative use immunity. *See Kastigar v. United States*, 406 U.S. 441, 453 (1972).

BACKGROUND

I. ENCRYPTION TRANSFORMS DATA SO THAT IT EXISTS IN AN UNINTELLIGIBLE FORMAT.

Encryption is a process by which a person can transform plain, understandable information into unreadable letters, numbers, or symbols using a fixed formula or process.[4] Only those who possess the corresponding decryption "key" can return the message to its original form.[5] Decryption is the process by which the transformed or scrambled "ciphertext" is converted back into readable text.[6]

To give a simple example of encryption, applying a classic "shift cipher" to offset each letter in the alphabet by one (*e.g.*, A becomes B), the phrase "Third

[4] *See* Tricia Black, *Taking Account of the World As it Will Be: The Shifting Course of U.S. Encryption Policy*, 53 Fed. Comm. L.J. 289, 292 (2001).

[5] *Id.*

[6] David Gripman, *Electronic Document Certification: A Primer on the Technology Behind Digital Signatures*, 17 Marshall J. Computer & Info. L. 769, 774 (1999).

Circuit" becomes "Uijse Djsdvju." Computer-assisted encryption parallels this manual encryption method, using more sophisticated algorithms to transform readable data into seemingly random numbers.[7]

When information is encrypted on a computer, it exists *only* in its scrambled format. Like the pieces of a jigsaw puzzle or confetti made from a shredded document, the information is scrambled and unintelligible, not locked behind a physical barrier like a vault door. While analogies to vaults with keyholes or combination locks may be useful to illustrate the fact that encryption is a tool for data security, they are imperfect analogies that do not accurately reflect the technology's operation.[8]

Any person in possession of an encrypted drive is able to "read" all of the information on the drive in the scrambled format in which it is stored, but the information will not make sense unless it is translated into an intelligible format via the process of decryption. In the shift cipher example noted above, a person might possess a slip of paper bearing "Uijse Djsdvju," but it will only be intelligible to someone who knows both the algorithm (*i.e.,* rotation of the alphabet) and the specific key (*i.e.*, rotate one letter backwards).

Electronically stored data can be encrypted in different ways. One option,

---

[7] *Id*.

[8] *See, e.g.*, Jeffrey Kiok, *Missing the Metaphor: Compulsory Decryption and the Fifth Amendment*, 24 B.U. Pub. Int. L.J. 53, 77 (2015).

known as "file encryption," encrypts only specific, individual files on a computer or other storage device.[9] Another option, known as "disk encryption" or "drive encryption," encrypts all of the data occupying a specific storage area.[10] For example, someone seeking to use encryption to protect sensitive information within their electronic tax return documents could use file encryption to separately encrypt each individual tax return file stored on their computer, while leaving other files on the same computer unencrypted. They could also use disk encryption to encrypt their computer's entire hard drive, thereby encrypting all tax returns as well as every other file on the drive, including the files for the computer's operating system. The two hard drives at issue here are encrypted with Apple's FileVault, a disk encryption system.[11]

Disk encryption makes it impossible to distinguish between encrypted data and unused computer space. Disk encryption programs typically fill free drive space with random data, "display[ing] random characters if there are files *and* if there is empty space," thus obscuring "what, if anything, was hidden[.]" *See In re Grand Jury Subpoena*, 670 F.3d at 1347 (emphasis in original). Decrypting a drive

---

[9] *See* Ries & Simek, *Encryption Made Simple For Lawyers,* 29 GPSolo 6 (Dec. 2012), https://www.americanbar.org/publications/gp_solo/2012/november_december2012privacyandconfidentiality/encryption_made_simple_lawyers.html.

[10] *Id*.

[11] *See* Apple, *Use FileVault to encrypt the startup disk on your Mac* (Sept. 4, 2015), https://support.apple.com/en-us/HT204837 (last viewed Mar. 23, 2016).

thus reveals whether there is any meaningful information on the drive, the quantity of files on the drive, *and* the actual contents of files stored on the drive.

An encrypted drive is similar to a massively (if not impossibly) complex jigsaw puzzle, with billions of individual pieces and no clues about how to assemble them. There is no barrier that prevents a person from opening the box and inspecting the pieces inside, but that inspection does not reveal what the assembled puzzle would depict. While trial and error would theoretically enable solving such a puzzle, in practice its immense complexity would mean that only a person who already knows what the final image is supposed to look like, or who has numbered the pieces and remembers their correct ordering, could put the pieces together and complete the puzzle.

II. ENCRYPTION IS A COMMON AND CRITICAL TOOL FOR PRIVACY AND SECURITY.

Encryption is integral for safeguarding the privacy and security of sensitive information. Using strong encryption is now a routine practice and industry standard for individuals and businesses alike.

Companies use encryption to secure proprietary business information, like trade secrets, and sensitive customer information, like bank account records, credit card numbers, and social security numbers.[12] Computer and software

[12] *See, e.g.*, Paul Mah, *Five essential security measures to protect your business—no matter its size*, PCWorld (Jun. 20, 2013) ("The first step is to

manufacturers consider disk encryption a basic computer security measure and include disk encryption tools as a standard feature on most new computers.[13] Government agencies recommend encryption to protect personal data and Internet traffic.[14] And many federal and state laws require or encourage encryption to protect sensitive information.[15]

Studies show that the use of encryption around the world is common and

---

implement full-disk encryption on each one of your company's PCs."), http://www.pcworld.com/article/2042358/five-essential-security-measures-to-protect-your-business-no-matter-its-size.html.

[13] For example, both Microsoft Windows and Apple's OS X offer encryption tools. *See* Apple, *What is OS X – Security*, https://www.apple.com/osx/what-is/security/; Microsoft, *Bitlocker Drive Encryption Overview*, http://technet.microsoft.com/en-us/library/cc732774.aspx.

[14] *See, e.g.*, Federal Trade Commission, "Start With Security: A Guide for Business" (Jun. 2015) ("Use strong cryptography to secure confidential material during storage and transmission."), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business; National Institute of Standards and Technology, NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices* (Nov. 2007) ("The primary security controls for restricting access to sensitive information stored on end user devices are encryption and authentication."), http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf.

[15] *See, e.g.*, 15 U.S.C. § 6801(b) (requiring security measures for consumer financial data) & 12 C.F.R. § 364, App. B (interagency rules interpreting § 6801 to require assessment of need for encryption of that information); 32 C.F.R. § 310, App. A (E)(1) (requiring encryption for unclassified Department of Defense employee information); 45 C.F.R. § 164.312(a)(2)(iv), (e)(2)(ii) (requiring HIPPA "covered entities" to consider implementing encryption for health information); Mass. Gen. Law ch. 93H § 2 (requiring security measures for protection of personal information) & 201 Mass. Code. of Regs. 17.00 (implementing § 2 to require encryption); Cal. Civil Code § 1798.29(a) (requiring notification in event of data breach for unencrypted information).

increasing each year.[16] A recent international survey found 865 hardware and software encryption products available from 55 countries.[17] And for decades, Americans have benefitted from the protection afforded by encryption systems—such as using an ATM or logging into an encryption-protected website using a username and password—often without realizing it. In these cases, encryption set up by the bank or website works behind the scenes to protect sensitive data.

Encryption also protects data in the event of theft of physical devices. This is especially important for portable devices, like phones and laptops, which can be easily lost or stolen and typically contain sensitive information. According to a 2010 study by Intel and the Ponemon Institute of 329 public and private institutions, more than 86,000 laptops were lost or stolen over a 12-month period,

[16] A 2016 joint report by the Ponemon Institute and French defense contractor Thales reported over 100% growth in the use of encryption among surveyed companies from 2005 to 2015. *See Global Encryption and Key Management Trends* at 3 (2016), https://www.thales-esecurity.com/knowledge-base/analyst-reports/global-encryption-trends-study. Further, according to Google's March 2016 Transparency Report, the use of encrypted communications has increased dramatically as more providers enable and maintain their support for secure communications. According to their data, 84% of email messages from Gmail to other providers are encrypted, while 72% of messages from other providers to Gmail are encrypted. Google, *Transparency Report, Email encryption in transit* (Mar. 25, 2016), https://www.google.com/transparencyreport/saferemail/.

[17] Schneier, Seidel & Vijayakumar, *A Worldwide Survey of Encryption Products, Version 1.0* (Feb. 11, 2016), https://www.schneier.com/cryptography/paperfiles/worldwide-survey-of-encryption-products.pdf.

an average of 263 laptops per organization.[18] When a device falls into the wrong hands, encryption protects sensitive data from being misused.[19]

Encryption also protects against outside intrusions into computers, including attacks from identity thieves, other criminals, or foreign governments. If sensitive files are accessed, encryption typically prevents the adversary from ascertaining the contents of the files.[20] The threat of unauthorized access is an increasing concern. For example, a 2014 Pew Research Center survey found that 18% of online adults have had important personal information, such as a Social Security Number, credit card number, or bank account information, stolen—up from the 11% who reported personal information theft in 2013.[21] The federal government, too, has endured data breaches where the absence of encryption likely exacerbated

---

[18] Intel, *The Billion Dollar Lost Laptop Problem: Benchmark Study of U.S. Organizations*, at 1, 6 (Oct. 31, 2010), https://www-ssl.intel.com/content/dam/doc/white-paper/enterprise-security-the-billion-dollar-lost-laptop-problem-paper.pdf.

[19] *See, e.g.*, Paul McNamara, *Latest "lost" laptop holds treasure-trove of unencrypted AT&T payroll data*, Network World (June 5, 2008), http://www.networkworld.com/community/node/28453.

[20] *See, e.g.,* Shawn Henry, Executive Assistant Director, FBI, Speech at Information Systems Security Association International Conference, Baltimore, Maryland (Oct. 20, 2011), https://www.fbi.gov/news/speeches/responding-to-the-cyber-threat.

[21] Mary Madden, *More online Americans say they've experienced a personal data breach*, Pew Research Center (Apr. 14, 2014), http://www.pewresearch.org/fact-tank/2014/04/14/more-online-americans-say-theyve-experienced-a-personal-data-breach/.

the severity of the breach.[22]

In sum, encryption is a widely used and critical tool to safeguard sensitive digital information. Using encryption is no more suspect than locking the door of your home; it is a routine, innocent, and increasingly necessary part of modern life.

III. ENCRYPTION HAS A VENERABLE HISTORY IN THE UNITED STATES.

People around the world have long used coded communication for numerous purposes, including political dissent, preservation of personal privacy, and commerce.[23]

Many of our nation's founders used available encryption technologies in their day. James Madison encrypted the contents of many of his letters, including part of a May 27, 1789 letter to Thomas Jefferson describing his plan to introduce a Bill of Rights.[24] Jefferson, too, was a frequent user of encryption and even invented his own cipher system, now known as the Jefferson Disk.[25] Benjamin

---

[22] *See, e.g.*, David Perrera, *Agency didn't encrypt feds' data hacked by Chinese*, Politico (Jun. 4, 2015), http://www.politico.com/story/2015/06/personal-data-of-4-million-federal-employees-hacked-118655.

[23] *See* John A. Fraser, III, *The Use of Encrypted, Coded and Secret Communications Is an "Ancient Liberty" Protected by the United States Constitution*, 2 Va. J.L. & Tech. 2, 1 (1997).

[24] *Id.* at 43 & n.123.

[25] *Id.* at 24 n. 76; *see also* Jefferson Disk, Crypto Museum, http://www.cryptomuseum.com/crypto/usa/jefferson/.

Franklin also invented his own cipher, in addition to publishing a textbook on early encryption technologies.[26] And there is evidence that Alexander Hamilton used a cipher to communicate with his relatives and political associates.[27] The founders viewed cryptology as an essential instrument for protecting information, both political and personal.[28]

IV. ENCRYPTION DOES NOT UNDULY HINDER LAW ENFORCEMENT.

Despite encryption's overall benefit, it is not impenetrable. Indeed, law enforcement officials have investigative techniques that enable them to gain lawful access to encrypted drives without compelling a defendant to aid in his own prosecution.

For example, investigators may obtain a warrant to install a camera to record a suspect's keystrokes as they decrypt a device; they can install a hardware device or software (called a "keylogger") that captures the characters typed using the device, including passwords;[29] it is even possible to distinguish between different

---

[26] Fraser, *supra* n.23, at 20, 33.

[27] *Id.* at 46.

[28] *See* Weber, *supra* n.1, at ix.

[29] *See* Declan McCullagh, *Feds use keylogger to thwart PGP, Hushmail*, CNET (Jul. 20, 2007), http://www.cnet.com/news/feds-use-keylogger-to-thwart-pgp-hushmail/; Bob Sullivan, *FBI software cracks encryption wall,* NBC News (Nov. 20, 2001), http://www.nbcnews.com/id/3341694/ns/technology_and_science-security/t/fbi-software-cracks-encryption-wall/

keystrokes based on audio recordings that can then be used to recreate passwords.[30] It is also possible to circumvent many forms of encryption by exploiting software or hardware flaws, or by using automated methods to repeatedly guess passwords.[31]

Even where encryption proves impenetrable, technology has, on balance, made our lives more transparent than ever before, enabling law-enforcement surveillance on a scale previously unimaginable. We live in a "golden age of surveillance,"[32] and law enforcement has already taken advantage of the vast amount of sensitive information now readily available about all of us.

Encryption allows individuals to reclaim some of that lost privacy, but there is no question that, as a general matter, technology has flung the curtains open, not drawn them tight. The development of new technologies demands that we reinforce—not abandon—our time-tested constitutional protections.

---

[30] Li Zhuang, Feng Zhou, and Doug Tygar, Keyboard Acoustic Emanations Revisited (Nov. 2015), http://www.cs.berkeley.edu/~tygar/papers/Keyboard_Acoustic_Emanations_Revisited/preprint.pdf

[31] *See, e.g.*, Bree Fowler & Brandon Bailey, *How the FBI might hack into an iPhone without Apple's Help*, AP (Mar. 22, 2016), http://www.bigstory.ap.org/article/abdfa21419c2416ca05f5f4f3b150e2d/how-fbi-might-hack-iphone-without-apples-help.

[32] *See*, Peter Swire, *The FBI Doesn't Need More Access: We're Already in the Golden Age of Surveillance*, Just Security (Nov. 17, 2014), https://www.justsecurity.org/17496/fbi-access-golden-age-surveillance/.

ARGUMENT

The Fifth Amendment to the Constitution guarantees that "[n]o person shall be . . . compelled in any criminal case to be a witness against himself." U.S. Const. amend. V. To come within the self-incrimination privilege, an individual must show three things: (1) compulsion, (2) a testimonial communication, and (3) self-incrimination. *United States v. Hubbell*, 530 U.S. 27, 34 (2000).

In this case, the government is attempting to compel Mr. Doe to disclose information that it believes may incriminate him. The only question is whether the disclosure it seeks to compel is "testimonial." *See id*. at 34.

As explained below, it is—both inherently and on the particular facts of this case. The Fifth Amendment thus prohibits it.

I. DECRYPTION IS INHERENTLY TESTIMONIAL, NOT A MERE PHYSICAL ACT, AND THEREFORE ABSOLUTELY PRIVILEGED BY THE FIFTH AMENDMENT.

The privilege against self-incrimination protects against compelled "testimonial" communications: those that require a person to use "the contents of his own mind" to communicate some fact. *Curcio v. United States*, 354 U.S. 118, 128 (1957). Compelled decryption is precisely the type of testimonial communication that lies at the heart of the Fifth Amendment's protection against self-incrimination.

A. The unique features of encryption make decryption inherently testimonial.

A communication need not be verbal to be testimonial. *Doe v. United States* ("*Doe II*"), 487 U.S. 201, 210 n.9 (1988) (noting agreement on this point with Justice Stevens' dissent, *id*. at 219). The focus, for Fifth Amendment purposes, is not on whether the communication is spoken, but whether it involves, by "word or deed," an "expression of the contents of an individual's mind." *Id*. at 219, 220 n.1 (Stevens, J., *dissenting*).

In contrast, "mere physical act[s]" that do not disclose the contents of a person's mind are not testimonial. *Hubbell*, 530 U.S. at 43. The Supreme Court has identified certain physical acts that, under the circumstances, were deemed non-testimonial, including: wearing a particular shirt, *Holt v. United States*, 218 U.S. 245, 252-53 (1910); providing a blood sample, *Schmerber v. California*, 384 U.S. 757 (1966); providing a handwriting exemplar, *Gilbert v. California*, 388 U.S. 263 (1967); and producing certain business documents, *Fischer v. United States*, 425 U.S. 391 (1976).[33]

In assessing the testimonial nature of decryption, it is superficially tempting

[33] When the government demands the physical production of records from a suspect, the suspect's resulting "act of production" is testimonial if it "entail[s] implicit statements of fact." *Doe II*, 487 U.S. at 209. For example, "by producing documents in compliance with a subpoena, the witness would admit that the papers existed, were in his possession or control, and were authentic." *Id.* This so-called "Act of Production Doctrine" is discussed in more depth in Section II (A) below.

to rely on the oft-stated analogy between the compelled entry of a safe's combination versus the compelled production of a lockbox's key. *See Hubbell*, 530 U.S. at 42. Under *Hubbell*, the former, which requires the compelled use of the "contents of [an individual's] mind," is testimonial and thus within the Fifth Amendment's privilege; the latter, a mere "physical act," is not. *Id.; see also United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) (quashing a subpoena for computer passwords, reasoning that, under *Hubbell* and *Doe*, the subpoena would have required the suspect "to divulge through his mental process his password").

But unlike entering in a numeric combination *or* handing over a key, both of which merely provide access to preexisting documents, decryption transforms preexisting, scrambled data. Here, the government is not seeking the surrender of inaccessible documents, as in the case of a safe or lockbox. The government possesses the drives and can read the information contained on them. But the government seeks a *transformation and explanation* of that data. As described above, the government in essence possesses the pieces of an extremely complex jigsaw puzzle, but one it has been unable to complete. For this, the government wants Mr. Doe to use his unique knowledge to assemble the puzzle and to aid in his prosecution.

Moreover, translating unintelligible data via decryption communicates the

content and characteristics of each and every file within the encrypted space. *See Hubbell*, 530 U.S. at 43. Indeed, it communicates whether any files exist at all. *See id*. at 43 ("[W]e have no doubt that the constitutional privilege against self-incrimination protects . . . from being compelled to answer questions designed to elicit information about the existence of sources of potentially incriminating evidence.").

Thus, compelled decryption using a password requires using the contents of the suspect's mind to explain data to the government. That is inherently testimonial and therefore is always protected by the privilege.

B. Prohibiting compelled decryption furthers the values animating the Fifth Amendment's privilege against self-incrimination.

The principles animating the privilege against self-incrimination reinforce the conclusion that decryption is inherently testimonial. Ultimately, "the protection of the privilege 'is as broad as the mischief against which it seeks to guard.'" *Schmerber*, 384 U.S. at 764 (quoting *Counselman v. Hitchcock*, 142 U.S. 547, 562 (1892)). The Supreme Court has explained that the privilege is rooted in our nation's "unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury, or contempt[,]" "our respect for the inviolability of the human personality and the right of each individual to a private enclave where he may lead a private life[,]" and "our realization that the privilege, while sometimes a shelter to the guilty, is often a protection of the innocent." *Doe II*, 487 U.S. at

212-13 (*quoting Murphy*, 378 U.S. at 55 (1964)) (internal quotations omitted).

Each element of the "cruel trilemma" is at work in cases of compelled decryption. The government gives those using encryption a choice: either provide us the allegedly incriminating information you possess; lie about your inability to do so; or be subject to a contempt order for failure to cooperate.[34] But the self-incrimination privilege's central purpose was to prevent this "trilemma" in the first place. *See id*. at 212.

Forced decryption also encroaches on "the right of each individual to a private enclave where he may lead a private life." *Id.* Electronic devices, "[w]ith all they contain and all they may reveal, . . . hold for many Americans 'the privacies of life.'" *Riley v. California*, 134 S. Ct. 2473, 2494-95 (2015) (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)). "Laptop computers, iPads and the like are simultaneously offices and personal diaries. They contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails." *United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013). Electronic devices may thus contain "a digital record of nearly every aspect of [users'] lives — from the mundane to the intimate." *Riley*, 134 S.

[34] This case highlights the untenable position facing an accused who is ordered to provide testimony to assist in their own prosecution. A person who does not know or cannot remember the password to a device (as Mr. Doe has represented in this case) may be unable, not merely unwilling, to comply with a court's order. The self-incrimination privilege ensures that an innocent person cannot be imprisoned for failing to comply with an impossible order.

Ct. at 2490.

This is precisely the type of material that implicates "the Founders' deep concern with safeguarding the privacy of thoughts and ideas—what we might call freedom of conscience—from invasion by the government." *Cotterman*, 709 F.3d at 965. Using encryption to secure these devices—containing the very "privacies of life," *Riley*, 134 S. Ct. at 2495—affords some limited measure of security in an otherwise insecure digital world. Conversely, compelled decryption is a blunt instrument, forcing a suspect to potentially expose their private life for government inspection. Such compelled intrusion encroaches on an individual's "private enclave where he may lead a private life." *Doe II*, 487 U.S. at 213; *see also Boyd*, 116 U.S. at 634.

Properly construed, the Fifth Amendment's self-incrimination privilege "enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment." *In re Grand Jury Proceedings*, 632 F.2d 1033, 1043 (3d Cir. 1980). Indeed, as this Circuit has recognized:

> [T]he framers of the Bill of Rights, in declaring that no man should be a witness against himself in a criminal case, evinced their judgment that in a free society, based on respect for the individual, the determination of guilt or innocence by just procedures, in which the accused made no unwilling contribution to his conviction, was more important than punishing the guilty.

Id. (internal quotations omitted). It is, accordingly, a "firmly embedded tenet of American constitutional law" that the Fifth Amendment protects the accused from

assisting law enforcement access to his most private spaces. *Id*. at 1042.[35] Compelled decryption—the forced disclosure of *different* information, through the application of the contents of an individual's mind—always violates that tenet, and thus always violates the Fifth Amendment.

II. EVEN IF COMPELLED DECRYPTION WERE AN "ACT OF PRODUCTION," IT NONETHELESS VIOLATES THE FIFTH AMENDMENT UNLESS THE EXISTENCE OF THE EVIDENCE THE GOVERNMENT SEEKS IS A "FOREGONE CONCLUSION."

Alternatively and independently, even if decryption were viewed as the surrender of preexisting documents, compelling decryption by Mr. Doe would violate the Fifth Amendment because it would communicate information that is not a "foregone conclusion."

[35] This Circuit's precedent applying the protections of the self-incrimination privilege to shield the contents of an individual's private papers remains the law of this Circuit and remains sound under governing Supreme Court precedent. *See In re Grand Jury Proceedings*, 632 F.2d 1033 (3d Cir. 1980); *ICC v. Gould*, 629 F.2d 847 (3d Cir. 1980), *cert denied* 449 U.S. 1077 (1981); *see also United States v. Doe* ("*Doe I*"), 465 U.S. 605, 619 (1984) (Marshall, J., and Brennan, J., *concurring*) ("[U]nder the Fifth Amendment there are certain documents no person ought to be compelled to produce at the Government's request."). Three other circuits have similarly rejected the contention that the Supreme Court has eliminated Fifth Amendment protection for private papers. *See Butcher v. Bailey*, 753 F.2d 465, 469 (6th Cir. 1985); *Barrett v. Acevedo*, 169 F.3d 1155, 1168 (8th Cir. 1999); *In re Steinberg*, 837 F.2d 527, 530 (1st Cir. 1988). As *Riley* teaches, government access to information stored on electronic devices raises profound privacy concerns, concerns that strikes at "the heart of our sense of privacy." *Doe I*, 465 U.S. at 619 n. 2 (Marshall, J., and Brennan, J., *concurring*). The Fifth Amendment therefore protects such information from compelled disclosure.

A. The Fifth Amendment protects testimonial acts of production that are explicitly or implicitly communicative and not foregone conclusions.

When the government demands the surrender of records from a suspect, the suspect's resulting "act of production" is testimonial if it "entail[s] implicit statements of fact." *Doe II*, 487 U.S. at 209. The facts need not be direct evidence of guilt, but can be information that forms "a link in the chain of evidence needed to prosecute." *Hoffman v. United States*, 341 U.S. 479, 486 (1951); *see Hubbell*, 530 U.S. at 38. For example, "by producing documents in compliance with a subpoena, the witness would admit that the papers existed, were in his possession or control, and were authentic." *Id.* Production is always testimonial where the government does not know the existence and location of the evidence, or where production would implicitly authenticate the evidence. *Doe II*, 487 U.S. at 210

Where the act of surrender implies testimonial facts, the government may only compel a suspect to surrender records if those facts are a "foregone conclusion" already known to the government. *Id*. at 44. This depends upon whether, prior to production, the government could have described the pertinent facts "with reasonable particularity." *Id.* at 29-30; *see also United States v. Ponds*, 454 F.3d 313, 320 (D.C. Cir. 2006) (holding the government must prove its prior knowledge of the pertinent facts with "reasonable particularity" to establish they are a "foregone conclusion"); *In re Grand Jury Subpoena*, 383 F.3d 905, 910 (9th Cir. 2004) (same); *In re Grand Jury Subpoena*, 1 F.3d 87, 93 (2d Cir. 1993)

(same). A foregone conclusion only exists when the resulting production "adds little or nothing to the sum total of the Government's information." *United States v. Fisher*, 425 U.S. 391, 411 (1976). That burden is a stringent one and is not met where the government demonstrates solely its knowledge of the existence, location, and authenticity of the *device*; it must make that showing with respect to the *information* it seeks. *SEC v. Huang*, No. 15-269, 2015 WL 5611644, at *2 (E.D. Pa. Sept. 23, 2015), discussing *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335, 1346 (11th Cir. 2012).

The government could not meet this burden in *Hubbell*, 530 U.S. at 44-45, because it had no "prior knowledge of either the existence or the whereabouts" of the 13,120 pages produced by the suspect in response to a subpoena. The government could not overcome its failure of proof by arguing that business people "always possess general business and tax records that fall within the broad categories described in the subpoena." *Id.* at 45.

On the other hand, the government met this burden in *Fisher* when it sought, from a suspect, accounting records that "belong[ed] to the accountant, were prepared by him, and are the kind usually prepared by an accountant working on the tax returns of his client." 425 U.S. at 411. Under these circumstances, "[t]he existence and location of the papers [we]re a foregone conclusion." *Id.*

B. As the Eleventh Circuit and other federal courts have correctly determined, decryption is a presumptively testimonial act of production because it reveals the existence, location, and authenticity of encrypted files.

The only published federal appellate court opinion regarding the application of the Fifth Amendment to the testimonial act of decryption is *In re Grand Jury Subpoena*, 670 F.3d 1335. There, the Eleventh Circuit began its analysis by stating a two-part test for determining whether decryption was testimonial: first, whether the decryption "would make use of the contents of his or her mind"; and second, whether the government could show with "reasonable particularity" that any testimonial aspects of the decryption were "foregone conclusions." *Id.* at 1345-46.

As to the first step, the court held that decryption is testimony about a suspect's "knowledge of the existence and location of potentially incriminating files"; of their "possession, control, and access to the encrypted portions of the drives"; and of their "capability to decrypt the files." *Id.* at 1346. These communicative acts of decryption "would certainly use the contents of his mind." *Id.* at 1349. As explained above, this is true of all password-based decryption.

As to the second step, the court found that the government had failed to show that it knew "whether any files exist and are located on the hard drives"; whether the suspect was "even capable of accessing the encrypted portions of the drives"; and "whether there was data on the encrypted drives." *Id.* at 1346-47. The court emphasized that because disk encryption generates "random characters if

there are files *and* if there is empty space, we simply do not know what, if anything, was hidden based on the facts before us." *Id.* at 1347 (emphasis in original). Thus, like in *Hubbell* and unlike in *Fisher*, the government did not know "the existence or the whereabouts" of the records it sought. *Id*.

Further, where the government does not know "specific file names," it must show with "reasonable particularity" that it seeks "a certain file," and can establish that "(1) the file exists in some specified location, (2) the file is possessed by the target of the subpoena, and (3) the file is authentic." *Id.* at 1349 n.28. On the other hand, "categorical requests for documents the Government anticipates are likely to exist simply will not suffice." *Id.* at 1347.

Finally, the Eleventh Circuit rejected the government's assertion that the act of encryption shows the suspect "was trying to hide something." Rather, "[j]ust as a vault is capable of storing mountains of incriminating documents, that alone does not mean that it contains incriminating documents, or anything at all." *Id*.

Three lower federal court decisions are consistent with the Eleventh Circuit's approach. In *Huang*, 2015 WL 5611644, at *2, relying on the Eleventh Circuit opinion, the court denied a motion to compel the defendants to supply passwords to their smartphones because it would "require intrusion into the knowledge of the Defendants" and because the SEC could not establish with "reasonable particularity" that any documents sought resided in the locked phones.

However, in *In re Boucher*, No 06-91, 2009 WL 424718, *2 (D. Vt. Feb. 19, 2009), the court denied a motion to quash a similar subpoena. There, border agents found, in a traveler's laptop computer, files with titles suggesting child pornography. The traveler stated that he sometimes unknowingly downloaded child pornography and showed the agents the drive where he downloaded files. In that file, the agents located apparent child pornography. Likewise, in *United States v. Fricosu*, 841 F. Supp. 2d 1232 (D. Colo. 2012), the court ordered a fraud suspect to decrypt information on a laptop. The police had seized a laptop with the suspect's name on it from her bedroom, and while in custody, she admitted in a recorded phone call that incriminating information was on the laptop. *Id.* at 1235. In both cases, the government had far more specific evidence than in either *Huang* or *In re Grand Jury Subpoena* that the information to be disclosed by the suspects' decryption was a foregone conclusion.

In *Commonwealth v. Gelfgatt*, 11 N.E.3d 605 (Mass. 2014), Massachusetts' highest court took an erroneously narrow view of the Fifth Amendment's protection from compelled decryption. It performed a "foregone conclusion" analysis, but without the "reasonable particularity" standard. *Id.* at 614-15. Applying the correct standard, the dissent concluded that the government had not shown the suspect had "any knowledge as to the existence or content of any particular files or documents on any particular computer." *Id.* at 622 (Lenk, J.,

dissenting).[36]

C. The government cannot satisfy the foregone conclusion test here.

Applying the Eleventh Circuit's two-part test, the existence of incriminating files on the encrypted drives at issue is not a foregone conclusion.

As explained above, by its very nature, using a secret password to decrypt data satisfies the first step of the court's test—that decryption "make[s] use of the contents of [the target's] mind." 670 F.3d at 1345.

As to the second step, the government cannot prove with reasonable particularity that all of the information that would be exposed by compelling Mr. Doe to decrypt the hard drives (even assuming he is able to do so) is a foregone conclusion. While EFF does not have access to the sealed documents filed with the district court, the publicly available record shows that the government's investigation of Mr. Doe has relied on testimony, provided after the search warrant was executed, of two individuals who gave no reliable insight into the contents of Mr. Doe's external drives. The first witness, Mr. Doe's sister, based her testimony on events that allegedly occurred the year prior and was unable to say that she had

[36] In an unpublished opinion, *United States v. Gavegnano*, 305 F. App'x 954 (4th Cir. 2009), held that compelled disclosure of a password is not testimonial. That issue is distinct from the question presented here: whether compelled *decryption* is testimonial and therefore privileged. Moreover, as explained above, the court's conclusion was incorrect.

ever viewed *any* file that existed on the encrypted drives, let alone an incriminating one. *See* Mr. Doe's Opening Brief, at 11-12. The second witness, Detective Christopher Tankelewicz, admitted that he could only guess that incriminating evidence was on the hard drives. *See id.* at 12-14.

A guess—even a "best guess," *id.*—is not sufficient to satisfy the government's burden of proving with reasonable particularity "the existence [and] the whereabouts" of suspect computer files. *See In re Grand Jury Subpoena,* 670 F.3d at 1347 (requests for documents "the Government anticipates are likely to exist simply will not suffice"). And a guess is certainly not sufficient to satisfy the government's heightened standard given that it has failed to identify "specific file names." *See id.* at 1349, n. 28. A guess also falls far short of the specific factual bases present in *Boucher* and *Fricosu*. *See Boucher*, 2009 WL 424718, *2 (agent observed apparent child pornography); *Fricosu*, 841 F. Supp. 2d at 1235 (suspect admitted information "was on my laptop").

The testimony proffered in this case fails to establish that the government knew with reasonable particularity "whether any files exist and are located on the hard drives" or even "whether there was data on the encrypted drives." *See In re Grand Jury Subpoena,* 670 F.3d at 1346-47. Just as in *In re Grand Jury Subpoena* and *Huang*, the government cannot establish that the existence of any records on Mr. Doe's encrypted hard drives is a foregone conclusion.

Even if the government were to satisfy its burden for *particular files*, and its burden of proving Mr. Doe's ability to decrypt them, such a finding would at most support compelling Mr. Doe to decrypt and provide to the government only those specific files for which the government had satisfied its stringent Fifth Amendment burden. It would not support an order compelling Mr. Doe to decrypt and produce the entire contents of the hard drives. But here, the government has failed to identify with reasonable particularity even the existence of a single file on the hard drives. Whatever is on the drives, if anything, is decidedly not a foregone conclusion.

III. IF A COURT ORDERS DECRYPTION ON CONDITION OF IMMUNITY, IT MUST PROVIDE BOTH USE AND DERIVATIVE USE IMMUNITY.

Decryption by the subject of a criminal investigation can only be constitutionally compelled through the provision of both use and derivative use immunity for the act of decryption.

The controlling federal statute provides that if a court orders a person to disclose evidence on condition of immunity from prosecution, "no testimony or other information compelled under the order (*or any information directly or indirectly derived from such testimony or other information*) may be used against the witness in any criminal case," with the exception of prosecutions for perjury and the like. 18 U.S.C. § 6002 (emphasis added). In *Kastigar*, 406 U.S. at 453, the

Supreme Court upheld this statute, explaining that immunity from both "use and derivative use" of compelled evidence is "coextensive" with Fifth Amendment guarantees. Thus, if the government compels testimony on condition of immunity, both the statute and Fifth Amendment require it to prove that any evidence it uses against the accused was "derived from a legitimate source wholly independent of the compelled testimony." *Id.* at 460.

In *Hubbell*, the Court explained that the Fifth Amendment's protection "encompasses compelled statements that lead to the discovery of incriminating evidence even though the statements themselves are not incriminating and are not introduced into evidence." 530 U.S. at 37. The Court reasoned:

> [T]he testimonial aspect of respondent's act of producing subpoenaed documents was the first step in a chain of evidence that led to this prosecution. The documents did not magically appear in the prosecutor's office like 'manna from heaven.' They arrived there only after respondent asserted his constitutional privilege, received a grant of immunity, and—under the compulsion of the District Court's order—took the mental and physical steps necessary to provide the prosecutor with an accurate inventory of the many sources of potentially incriminating evidence sought by the subpoena.

Id. at 42; *see also Ponds*, 454 F.3d at 323 ("When the government does not have reasonably particular knowledge of the existence or location of a document, and the existence or location of the document is communicated through immunized testimony, the contents of the document are derived from that immunized testimony, and therefore are off-limits to the government.").

In the context of judicial compulsion to decrypt digital information, the

Eleventh Circuit held that "act-of-production immunity," without immunity for "the contents of the production," was insufficient. *In re Grand Jury Subpoena*, 670 F.3d at 1350-51.

Here, the publicly available record does not indicate that the government has offered any immunity to Mr. Doe in exchange for the testimonial act of decryption. If the government does elect to offer such immunity, it must offer both use and derivative use immunity.

CONCLUSION

For these reasons, the imposition of civil contempt should be reversed.

Dated: April 6, 2016

By: /s/ Kit Walsh
Kit Walsh
Adam Schwartz
Mark Rumold
Jamie Williams
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
kit@eff.org

Counsel for Amici Curiae Electronic Frontier Foundation and American Civil Liberties Union

COMBINED CERTIFICATIONS

I hereby certify as follows:

1. That I, Kit Walsh, counsel for *Amici Curiae*, am a member of the Bar of this Court.

2. That the foregoing brief of *Amici Curiae* complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B). The brief is printed in proportionally spaced 14-point Times New Roman font, using Microsoft® Word for Mac 2011 and there are 6,963 words in the brief according to the word count of the word-processing system used to prepare the brief (excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii)). The brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5), and with the type style requirements of Fed. R. App. P. 32(a)(6).

3. That I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Third Circuit, pursuant to Third Circuit Rule 25.1(b) by using the appellate CM/ECF system on April 6, 2016. All participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

4. That the text of the electronic brief is identical to the text of the seven paper copies mailed to the Court pursuant to Local Rule 31.1(b)(3).

5. That the electronic file of this brief was scanned with Avast antivirus

software version 11.7.45814 and that no virus was detected.

Dated: April 6, 2016

By: /s/ Kit Walsh
Kit Walsh

Counsel for Amici Curiae
Electronic Frontier Foundation and
American Civil Liberties Union