IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES,	)	
Appellant,	)	BRIEF OF ELECTRONIC
	)	FRONTIER FOUNDATION,
v.	)	AMERICAN CIVIL LIBERTIES
	)	UNION, AND ACLU OF THE
Sergeant (E-5)	)	DISTRICT OF COLUMBIA
EDWARD J. MITCHELL, II,	)	AS AMICI CURIAE IN SUPPORT
United States Army,	)	OF APPELLEE
Appellee.	)	
	)	Crim. App. Dkt. No 20150776
	)	USCA Dkt. No. 17-0153/AR
	)	

TO THE HONORABLE JUDGES OF THE UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES

The Electronic Frontier Foundation, the American Civil Liberties Union, and the ACLU of the District of Columbia, pursuant to Rules 26(a)(3) of this Court, respectfully submit this brief as Amicus Curiae in support of Appellee Edward J. Mitchell, II.

Jamie Williams*
Mark Rumold
ELECTRONIC
FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
jamie@eff.org

* Motion for Appearance
pro hac vice pending

Brett Max Kaufman*
Patrick Toomey
AMERICAN CIVIL
LIBERTIES UNION
125 Broad Street—18th Fl.
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2654
bkaufman@aclu.org

Counsel for Amici Curiae

Arthur B. Spitzer
(CAAF Bar No. 23420)
Scott Michelman
ACLU OF THE
DISTRICT OF
COLUMBIA
4301 Connecticut Ave.,
NW, Suite 434
Washington, DC 20008
Tel: (202) 457-0800
aspitzer@acludc.org

INDEX OF BRIEF

TABLE OF CASES, STATUTES, AND OTHER AUTHORITIES

Cases

Statutes

Other Authorities

Constitutional Provisions

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 34,000 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 is particularly interested in ensuring the constitutional rights of those who use encryption—a fundamental and widely used safeguard for businesses and individuals to protect their privacy and security. In that regard, 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 Duces Tecum*, 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*, Case No. 2:13-mj-449-RTR (E.D. Wis. 2013); *Commonwealth v. Gelfgatt*, 11 N.E.3d 605 (D. Mass. 2013); and *United States v. Apple MacPro Computer, et al.*, Case No. 15-3537 (3d Cir. 2016) (decision pending).

[1] 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.

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. The ACLU of the District of Columbia is the Washington, D.C. affiliate of the ACLU.

INTRODUCTION

The investigators in this case compelled Sergeant (SGT) Edward Mitchell to not only unlock his personal iPhone by entering a passcode, but also to decrypt the information stored on it—all for the purpose of facilitating their ability to access the phone's encrypted contents.

As the military judge correctly found, this type of compelled password- or passcode-based decryption is inherently testimonial. This is true for two independent reasons, not merely the one reason specifically identified by the military judge.

First, as the military judge found, the compelled entry of a memorized passcode forces one to reveal the contents of his or her mind to investigators—contents that are absolutely privileged by the Fifth Amendment.

Second, the process of decryption itself is testimonial because it involves translating otherwise unintelligible evidence into a form that can be used and understood by investigators.

Both aspects of compelled decryption—translating data from unintelligible to intelligible *and* providing a memorized passcode—are the types of testimonial communication that lie at the heart of the Fifth Amendment's protection against self-incrimination. The Fifth Amendment thus provides an absolute privilege against self-incriminating compelled decryption.

Moreover, even if compelled decryption were not inherently testimonial (it is), compelling SGT Mitchell to enter his numeric passcode was testimonial in this case because the information stored on his iPhone was not a foregone conclusion already known to the government. *See In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335, 1346, 1349 (11th Cir. 2012). Specifically, the investigators did not demonstrate with reasonable particularity that they knew of any specific files stored on the phone prior to compelling SGT Mitchell to unlock and decrypt it.

This Court should therefore affirm the military judge's ruling that SGT Mitchell's act of unlocking and decrypting his iPhone was testimonial, and that compelling SGT Mitchell to unlock and decrypt the device was unconstitutional.

BACKGROUND

I. BY ENTERING HIS PASSCODE, SGT MITCHELL UNLOCKED *AND* DECRYPTED HIS PHONE.

On January 8, 2016, after repeated demands by investigators, SGT Mitchell entered his numeric passcode into his iPhone 6. This single act did two separate things: it unlocked the phone's data, and it decrypted the information contained within the phone. SGT Mitchell's iPhone 6 was, by default, running a version of Apple's iOS 8 mobile operating system.[2] Locking a device running iOS 8 automatically encrypts the data stored on it:

[2] Apple, Inc., Press Release, "Apple Announces iPhone 6 & iPhone 6 Plus—The Biggest Advancements in iPhone Histor*y*" (Sept. 9, 2014), http://www.apple.com/p

> By setting up a device passcode, the user automatically enables Data Protection. iOS supports four-digit and arbitrary-length alphanumeric passcodes. In addition to unlocking the device, a passcode provides entropy for certain encryption keys. This means an attacker in possession of a device can't get access to data in specific protection classes without the passcode.
>
> The passcode is entangled with the device's UID [Unique ID], so brute-force attempts must be performed on the device under attack. . . . The stronger the user passcode is, the stronger the encryption key becomes.[3]

II. ENCRYPTION IS DISTINCT FROM MERELY LOCKING UP DATA; IT TRANSFORMS DATA SO THAT IT EXISTS IN AN UNINTELLIGIBLE FORMAT UNTIL DECRYPTED.

Encryption and locking are two distinct things—as are their counterparts, decryption and unlocking.

Placing information behind a lock, like a vault door (or a password not connected to a cryptographic key), merely places a physical (or technological) barrier around that information. But the information itself does not change form. Just as if someone were to pick the lock of a vault door to gain access to sensitive documents stored within, if someone were to break into a locked (and unencrypted)

r/library/2014/09/09Apple-Announces-iPhone-6-iPhone-6-Plus-The-Biggest-Advancements-in-iPhone-History.html ("Both models include iOS 8[.]").

[3] Apple, Inc., iOS Security (Sept. 2014), https://www.documentcloud.org/documents/1302613-ios-security-guide-sept-2014.html. Today, the current version of iOS supports six-digit, four-digit, and arbitrary-length alphanumeric passcodes. Apple, Inc., iOS Security, iOS 9.3 or later (May 2016), https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

device and access the information stored on it, they would be able to read and understand all of that information.

Encryption, on the other hand, transforms data into a scrambled, 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]

When information is encrypted on a phone, computer, or other electronic device, it exists *only* in its scrambled format. As a result, if someone were to break into an encrypted device and access or "read" the information stored on it, they would not be able to understand it—unless they somehow also had access to the decryption key necessary for translating the information back into its unscrambled and intelligible state.

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

Thus, while encryption has been compared to keyed locks or combination safes to illustrate the general proposition that encryption is a tool for data security, these are imperfect analogies that do not accurately reflect how the technology works.[7]

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 "Armed Forces" becomes "bsnfe gpsdft." A person might possess a slip of paper bearing "bsnfe gpsdft," 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). Computer-assisted encryption parallels this manual encryption method, using more sophisticated algorithms to transform readable data into seemingly random data.[8]

Electronically stored data can be encrypted in different ways. "File encryption" encrypts only specific, individual files on a computer or other storage device.[9] "Disk encryption" or "drive encryption" encrypts all of the data occupying

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

[8] *Id*.

[9] *See* David G. Ries & John W. 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.

a specific storage area.[10] This is similar to "device encryption," which encrypts all of the data stored on a particular device, such as a cell phone or other portable electronic device.

For example, those 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. They could also use *device encryption* to protect the entire contents of their computer (or, their iPhone, as was the case here).

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

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

[10] *Id*. 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 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.

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.[11] Computer and software manufacturers consider disk encryption a basic computer security measure and include disk encryption tools as a standard feature on most new computers.[12] Government agencies recommend encryption to protect personal data and Internet traffic.[13] Many federal and state laws require or encourage encryption to protect sensitive information.[14] And device encryption is increasingly a standard feature

[11] *See, e.g.*, Paul Mah, "Five essential security measures to protect your business—no matter its size," *PCWorld* (Jun. 20, 2013), http://www.pcworld.com/article/2042358/five-essential-security-measures-to-protect-your-business-no-matter-its-size.html.

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

[13] *See, e.g.*, Federal Trade Commission, *Start With Security: A Guide for Business* (Jun. 2015), 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), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf ("The primary security controls for restricting access to sensitive information stored on end user devices are encryption and authentication.").

[14] *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);

for new smart phones. As noted, Apple first introduced iPhone device encryption in 2014, via iOS 8.[15]

Studies show that the use of encryption around the world is common and 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. Indeed, in this increasingly connected world, encryption is a pervasive and integral part of modern life.

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).

[15] Cyrus Farivar, "Apple expands data encryption under iOS 8, making handover to cops moot," *Ars Technica* (Sept. 17, 2014), http://arstechnica.com/apple/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot/.

[16] A 2016 report by the Ponemon Institute, co-sponsored by French defense contractor Thales, reported over 100 percent growth in the use of encryption among surveyed companies from 2005 to 2015. *See* Ponemon Institute, *Global Encryption and Key Management Trends*, 3 (2016), https://www.thales-esecurity.com/knowledge-base/analyst-reports/global-encryption-trends-study.

[17] Bruce Schneier, Kathleen Seidel & Saranya 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.

ARGUMENT

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

In this case, all three elements are satisfied. For the reasons outlined in Appellee's Answer, and as the military judge found, it is clear that the government compelled SGT Mitchell to enter his passcode to unlock and decrypt his iPhone 6.[18] Equally clear is that this was done because the investigators believed the iPhone might contain information that could incriminate SGT Mitchell. Indeed, the investigators had, earlier that day, obtained a verbal warrant to confiscate and search his iPhone, along with his other electronic devices. (Appellee's Answer, p. 4; App. Ex. XXIV.)

And as outlined herein, SGT Mitchell's compelled and potentially incriminating disclosure—entering his passcode to unlock *and* decrypt his

[18] *See* Appellee's Answer, pp. 16–17; *see also Maryland v. Shatzer*, 559 U.S. 98, 105 (2009) (statements made in response to questioning that violates *Edwards v. Arizona*, 451 U.D. 477 (1981), are presumed involuntary). Discussion of why *Edwards* was violated here and why SGT Mitchell did not voluntarily enter his passcode is beyond the scope of this brief, which focuses solely on the testimonial nature of compelled decryption.

iPhone—was "testimonial." *See Hubbell*, 530 U.S. at 34. This is true for two reasons.

First, compelled decryption is inherently testimonial, not only because it forces a person to reveal the contents of his or her mind to investigators, but also because it involves translating otherwise unintelligible evidence into a form that can be used and understood by investigators. Second, SGT Mitchell's compelled disclosure was testimonial in this case because the evidence sought (and obtained) was not a foregone conclusion. The compelled disclosure thus violated the Fifth Amendment.

I. PASSCODE-BASED DECRYPTION IS INHERENTLY TESTIMONIAL—NOT A MERE PHYSICAL ACT—AND THEREFORE ABSOLUTELY PRIVILEGED BY THE FIFTH AMENDMENT.

A. Compelled Entry of a Passcode Is a Testimonial Communication 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). 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 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.9 (Stevens, J., *dissenting*).

In contrast, "mere physical act[s]" that do not express the contents of a person's mind are not testimonial. *Hubbell*, 530 U.S. at 43. Depending on the circumstances, this might include 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, 761 (1966), providing a handwriting exemplar, *Gilbert v. California*, 388 U.S. 263, 266–67 (1967), or producing certain business documents, *Fisher v. United States*, 425 U.S. 391, 412–13 (1976).[19]

As the Supreme Court noted in *Hubbell*, the compelled entry of a safe's combination is testimonial because it requires the compelled use of the "contents of [an individual's] own mind" and is thus within the Fifth Amendment's privilege. 530 U.S. at 43 (internal quotations omitted). Meanwhile, the compelled production of a lockbox's key is not testimonial, because it involves "a mere physical act[.]" *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

[19] 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 v. United States* ("*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.

Hubbell and *Doe*, the subpoena would have required the suspect "to divulge through his mental process his password").

Here, just as with the compelled entry of a safe's combination or computer password, compelling SGT Mitchell to enter his iPhone's numeric passcode was testimonial. *See Hubbell*, 530 U.S. at 43; *Kirschner*, 823 F. Supp. 2d at 669. All three—a safe combination, a computer password, and a phone passcode—compel the suspect to use of the contents of his own mind. Nothing more is necessary to implicate the privilege. Thus, the military judge was correct in holding that "remembering, recalling, and entering a password is not a simple physical act"; rather, it "requires the use of the contents of the accused's mind and is testimonial in nature"—it is a "testimonial act." (App. Ex. LIV, p. 8; App. Ex. LXXXV, p. 9).

Furthermore, the testimonial nature of compelling entry of a numeric passcode does not turn on whether a suspect enters his decryption key himself versus handing that key over to a government agent. In either case, the accused is required to use the contents of his mind—and the government is "relying on the [suspect's] truthtelling[.]" *See Hubbell*, 530 U.S. at 44 (quoting *Fisher v. United States*, 425 U.S. 391, 394 (1976); internal quotations omitted); *Doe II*, 487 U.S. at 219 (Stevens, J., *dissenting*) (The accused cannot "be compelled to reveal the combination to his wall safe—by word or deed."). Thus, in either case, the compelled production is testimonial and protected by the Fifth Amendment.

B. The Unique Features of Encryption Make Compelled Decryption Inherently Testimonial.

Compelled decryption is testimonial for an additional reason: it involves a translation of information for law enforcement. It is not simply a vehicle to unlock information already in existence.

Unlike the compelled entry of a numeric vault combination—which merely provides access to preexisting documents—compelled decryption transforms preexisting, scrambled data. 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.").

Here, the investigators were not merely seeking the surrender of *inaccessible* documents, as in the case of a safe or lockbox. They were seeking the *transformation and explanation* of data. The investigators were in possession of all the information they sought but they could not understand it. In this sense, they possessed the pieces of an extremely complex jigsaw puzzle that they were unable to complete, and they sought SGT Mitchell's unique knowledge to assemble the puzzle for the purpose of aiding in his own prosecution.

Because compelled, passcode-based decryption requires using the contents of the suspect's mind to explain, or translate, data for the government, it is inherently testimonial and therefore always protected by the privilege.

C. 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 to the innocent." *Doe II*, 487 U.S. at 212–13 (*quoting Murphy v. Waterfront Comm'n of New York Harbor*, 378 U.S. 52, 55 (1964)) (internal quotations omitted).

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). It represents the founders' "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 or her most private spaces. *Id*. at 1042.[20]

Forced decryption encroaches on "the right of each individual 'to a private enclave where he may lead a private life.'" *Doe II*, 487 U.S. at 212. "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). Our phones and electronic devices contain "a digital record of nearly every aspect of [users'] lives — from the

[20] Four circuits have held that the self-incrimination privilege shields the contents of an individual's private papers. *See In re Steinberg*, 837 F.2d 527, 530 (1st Cir. 1988); *ICC v. Gould*, 629 F.2d 847, 859 (3d Cir. 1980), *cert denied* 449 U.S. 1077 (1981); *Butcher v. Bailey*, 753 F.2d 465, 469 (6th Cir. 1985); *Barrett v. Acevedo*, 169 F.3d 1155, 1168 (8th Cir. 1999); *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."). As *Riley* teaches, government access to information stored on electronic devices raises profound privacy concerns, concerns that strike at "the heart of our sense of privacy." *Doe I*, 465 U.S. at 619 n. 2 (Marshall, J., and Brennan, J., *concurring*).

mundane to the intimate." *Riley v. California*, 134 S. Ct. 2473, 2490 (2014). Thus, electronic devices, "[w]ith all they contain and all they may reveal, they 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)).

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—and the sensitive data they contain—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 his or her entire private life to wholesale inspection by government agents. Such compelled intrusion encroaches on an individual's "private enclave where he may lead a private life." *Doe II*, 487 U.S. at 212; *see also Boyd*, 116 U.S. at 634.

II. THE "FOREGONE CONCLUSION" EXCEPTION DOES NOT APPLY HERE.

Alternatively, and independently, even assuming compelled decryption was not inherently testimonial, the compelled decryption underlying this case violated the Fifth Amendment because the information communicated was not a "foregone conclusion."

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). 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." *Hubbell*, 530 U.S. at 56, n. 19 (quoting *Doe I*, 465 U.S. at 613). 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 production 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. *Hubbell*, 530 U.S. at 44. This depends upon whether, prior to production, the government could have described the pertinent facts "with reasonable particularity." *Id.* at 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." *Fisher*, 425 U.S. at 411. That burden is a stringent one—and it is one not met where the government demonstrates solely its knowledge of the existence, location, and authenticity *of the device*. Instead, the government must make this 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*, 670 F.3d at 1346).

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. And it 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 taxpayers in two cases *specific* financial records that had been prepared by the taxpayers' accountants and provided by the taxpayers to their attorneys, who had been retained by the taxpayers in connection with the IRS investigations. 425

U.S. at 394. The government knew that the documents were in the attorneys' possession and could independently confirm their existence and authenticity through the accountants who created them. *See id.* at 411 (noting that the records in question "belong[ed] to the accountant" and "were prepared by him"). Under these circumstances, "[t]he existence and location of the papers [we]re a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers." *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 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 [the suspect’s] mind.” *Id.* at 1349. As explained above, this is true of all password- or passcode-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. Thus, while requests describing a general category of documents may satisfy the Fourth Amendment’s particularity requirement, the Fifth Amendment demands something more.

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, the Eastern District of Pennsylvania denied a motion to compel the defendants to supply passwords to their smartphones because it would "require intrusion into the knowledge of Defendants" and because the SEC could not establish with "reasonable particularity" that any documents sought resided in the locked phones. *Id.* at *3. In *In re Boucher*, No 06-91, 2009 WL 424718, *2–*3 (D. Vt. Feb. 19, 2009), the court denied a motion to quash a similar subpoena after finding that the foregone conclusion test was satisfied; the government had viewed contents of the drive in question, knew the existence and location of the drive's files, and ascertained that the files may consist of images or videos of child pornography. And in *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1235–37 (D. Colo. 2012), the court also found the foregone conclusion test satisfied and ordered a fraud suspect to decrypt information on a laptop; she had admitted in a recorded phone call that incriminating information was on the laptop. In both *In re Boucher* and *Fricosu*—and unlike in either *Huang* or *In re Grand Jury Subpoena*—the government had specific evidence that the information to be disclosed via 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. The dissent—applying the correct standard—concluded that the government had not shown that it 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*).

C. The Foregone Conclusion Test Was Not Satisfied Here.

Applying the Eleventh Circuit's two-part test, the existence of specific, incriminating files on the iPhone was not a foregone conclusion.

As to the first step, as explained above, by its very nature, using a memorized passcode to decrypt data "make[s] use of the contents of [the target's] mind." *In re Grand Jury Subpoena*, 670 F.3d at 1345.

As to the second step, the government has not established with reasonable particularity that *all* of the information exposed by SGT Mitchell's compelled decryption was a foregone conclusion at the time of the production—let alone any specific file. Indeed, the government presented no evidence demonstrating that it knew with reasonable particularity that any specific files would be found on the phone. Instead, the government relies on the fact that the investigators had a verbal warrant to search the phone. *See* Brief on Behalf of Appellant, p. 26. But suspicion that a person has committed an offense—even suspicion sufficient to establish probable cause—is not sufficient to satisfy the government's burden of proving with reasonable particularity "the existence [and] the whereabouts" of specific files. *See* 670 F.3d at 1347 (requests for documents "the Government anticipates are likely to exist simply will not suffice"). And neither reasonable suspicion nor probable cause is sufficient to satisfy the government's heightened burden when seeking to overcome SGT Mitchell's Fifth Amendment protection against self-incrimination, given that the agents had no knowledge of "specific" files or pieces of evidence located on the device. *See id.* at 1349, n. 28.

The government's case thus falls far short of the specific factual bases presented in *Boucher* and *Fricosu* for satisfying the foregone conclusion doctrine. *Boucher*, 2009 WL 424718, *2 (agent observed apparent child pornography); *Fricosu*, 841 F. Supp. 2d at 1235 (suspect admitted specific information "was on my laptop"). Just as in *In re Grand Jury Subpoena* and *Huang*, the government cannot establish that it knew with reasonable particularity "whether any files exist[ed] and [were] located" on the iPhone prior to compelling SGT Mitchell to decrypt the device. *See In re Grand Jury Subpoena,* 670 F.3d at 1346–47. It therefore cannot establish that the existence of even a single file on SGT Mitchell's iPhone was a foregone conclusion, let alone all of the files contained on the device.

CONCLUSION

For these reasons, this Court should affirm the military judge's holding.

Date: January 30, 2017

Respectfully submitted,

/s/ Jamie Williams

Jamie Williams
Mark Rumold
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 436-9333
Fax: (415) 436-9993
jamie@eff.org

Counsel for Amicus Curiae
Electronic Frontier Foundation

Brett Max Kaufman
Patrick Toomey
AMERICAN CIVIL LIBERTIES
UNION
125 Broad Street—18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2654
bkaufman@aclu.org

Counsel for Amicus Curiae
American Civil Liberties Union

Arthur B. Spitzer
(CAAF Bar No. 23420)
Scott Michelman
ACLU OF THE DISTRICT
OF COLUMBIA
4301 Connecticut Ave., NW,
Suite 434
Washington, DC 20008
Tel: (202) 457-0800
aspitzer@acludc.org

Counsel for Amicus Curiae
American Civil Liberties Union
of the District of Columbia

CERTIFICATE OF COMPLIANCE WITH RULE 24

This brief complies with the type-volume limitation of Rule 24(c) and Rule 26(f) because:

X This brief contains [5,768] words, no more than one-half the maximum length authorized by Rule 24 for a brief for an appellant/petitioner,

or

__ This brief contains [less than 650] lines of text.

This brief complies with the typeface and style requirements of Rule 37.

/s/ Jamie Williams
Jamie Williams

Attorney for *Amicus Curiae*
Electronic Frontier Foundation

Dated: January 30, 2017

CERTIFICATE OF FILING AND SERVICE

I certify that a copy of the foregoing Unopposed Motion for Leave to File Brief of *Amicus Curiae* Electronic Frontier Foundation, Brief of *Amicus Curiae* Electronic Frontier Foundation In Support of Appellee, and Motions To Appear Pro Hac Vice, were transmitted by electronic means with the consent of the parties to the counsel for Appellee CPT Joshua B. Fix, Joshua.b.fix2.mil@mail.mil, counsel for Appellant CPT Samuel E. Landes, samuel.e.landes.mil@mail.mil, and the Clerk of the Court Bill DeCicco, efiling@armfor.uscourts.gov on January 30, 2017.

/s/ Jamie Williams
Jamie Williams
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 436-9333