IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES,	)	
Appellee,	)	BRIEF OF ELECTRONIC
	)	FRONTIER FOUNDATION,
v.	)	AMERICAN CIVIL LIBERTIES
	)	UNION, AND ACLU OF THE
Senior Airman (E-4)	)	DISTRICT OF COLUMBIA
HANK W. ROBINSON,	)	AS AMICI CURIAE IN SUPPORT
U.S. Air Force,	)	OF APPELLEE
Appellant.	)	
	)	Crim. App. Dkt. No 38942
	)	USCA Dkt. No. 17-0504/AF
	)	

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 Colombia, pursuant to Rules 26(a)(3) of this Court, respectfully submit this brief as amici curiae in support of Appellant Hank W. Robinson.

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)
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

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 38,000 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.

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.

Both ACLU and EFF have participated as amici curiae in several cases regarding the application of the Fifth Amendment to compelled password disclosure and decryption, including *United States v. Mitchell*, No. 17-0153, 2017 WL 3841376 (C.A.A.F. Aug. 30, 2017); *Commonwealth v. Gelfgatt*, 11 N.E.3d 605 (D. Mass. 2013); and *United States v. Apple MacPro Computer*, 851 F.3d 238 (3d Cir. 2017).

---

[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.

INTRODUCTION

For the second time this year, this Court is called on to resolve an important question concerning the scope of the Fifth Amendment's protections for passcode-based decryption. Cases involving compelled disclosure of memorized passcodes are increasingly common, as more Americans secure their digital devices, and the vast universe of sensitive information they contain, with passcode-based encryption software.

In *United States v. Mitchell*, 76 M.J. 413, 418–19 (C.A.A.F. 2017), this Court established that investigators' request to provide a memorized passcode to decrypt a phone constitutes "interrogation" and, therefore, is impermissible under the Fifth Amendment after a suspect has invoked his right to counsel.

This case arises in a similar posture: there is no dispute that Senior Airman Robinson was in custody, had requested counsel, and was asked by investigators to divulge his phone's passcode. The only factual distinction between *Mitchell* and this case is Robinson's intervening provision of consent to search his phone—a distinction that does not merit a different holding.

The decision below was rendered before, and without the benefit of, this Court's guidance in *Mitchell*. Consequently, to the extent the Air Force Court of Criminal Appeals determined that a request for a passcode did not constitute "interrogation," that decision was in error. *See United States v. Robinson*, 76 M.J. 663, 671 (A.F. Ct. Crim. App. 2017) (citing *Rhode Island v. Innis*, 446 U.S. 291 (1980)).

The Court of Appeals also rested its decision on a second, but related, flaw: it erroneously equated two separate Fifth Amendment inquiries—the investigator's request for Robinson's consent to search his phone, on the one hand, and the

investigator's request for Robinson to state the passcode to his phone, on the other. *See id.* (citing *United States v. Roa*, 24 M.J. 297 (C.M.A. 1987)).

As this Court recognized in *Mitchell*: "[A]sking [a suspect] to *state* his passcode involves more than a mere consent to search[.]" *Mitchell*, 76 M.J. at 418 (emphasis in original). Just as consenting to a search of one's home does not mean an individual agrees to answer additional questions about the home, so too Robinson's consent to a search of his phone is not tantamount to consent to provide additional answers about the phone.

Indeed, a request to state an encrypted device's passcode calls for a fundamentally different response than a request for consent to search for two reasons: First, a suspect's recitation of a memorized passcode to an encrypted device can be self-incriminating. Given the presence of potentially incriminating evidence on the device, recitation of the passcode provides investigators with a direct link to evidence on the phone that, without the passcode, they would not be able to meaningfully access or use against him. Second, a request for a suspect to provide an encrypted device's passcode is testimonial and communicative because it requires the suspect to reveal to investigators the contents of his mind—contents that are absolutely privileged by the Fifth Amendment. Providing the passcode to an encrypted device is additionally testimonial because decryption involves translating otherwise unintelligible evidence into a form that can be used and understood by investigators.

Both aspects of password-based decryption—recalling a memorized passcode and translating data from unintelligible to intelligible—are types of testimonial communications that (if self-incriminating) lie at the heart of the Fifth Amendment's protection against being compelled to become a witness against oneself.

Finally, this Court should reject any invitation by the government to apply the foregone conclusion doctrine to this case. The doctrine, which only applies in the context of production of physical evidence, simply has no application here, where Robinson was asked to state a memorized passcode.

Ultimately, the protections of the Fifth Amendment's self-incrimination privilege are "'as broad as the mischief against which it seeks to guard.'" *Schmerber v. California*, 384 U.S. 757, 764 (1966) (quoting *Counselman v. Hitchcock*, 142 U.S. 547, 562 (1892)). The Supreme Court has explained that the privilege is rooted in "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[.]" *Doe v. United States*, 487 U.S. 201, 212 (1988) (quoting *Murphy v. Waterfront Comm'n of N.Y. Harbor*, 378 U.S. 52, 55 (1964)) (internal quotations omitted). And, in today's digital world, where our phones and other electronic devices contain the "sum of an individual's private life," *Riley v. California*, 134 S. Ct. 2473, 2489 (2014), that privilege must extend to the compelled disclosure of the memorized passcodes that protect such sensitive information.

This Court should thus find that the military judge abused his discretion by not suppressing all the evidence derived from Robinson's cellphone search and set aside the findings and sentence.

BACKGROUND

During the course of his interrogation on December 22, 2014, Robinson invoked his right to counsel and consented to a search of his iPhone 5s. After obtaining a signed search consent form, the investigator returned to the interrogation room to ask Robinson if he "could give [investigators] the password to [his] phone." *See* Appellant's Brief in Support of the Issues ("AOB"), p. 7; JA

38, 146, 192. Under these circumstances, Robinson's compliance was compelled.[2] The password was necessary because Robinson's phone was running a version of Apple's iOS 8 mobile operating system.[3] The data on locked devices running iOS 8 is automatically encrypted: "all the important data on your phone—photos, messages, contacts, reminders, call history—are encrypted by default."[4]

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.[5] Only those who possess the corresponding encryption "key"—in this case, Robinson's passcode—can return the message to its original form.[6] Decryption is the process by which the transformed or scrambled

---

[2] Amici assume, for purposes of this brief, that—absent the application of this Court's decision in *Roa* to the request for Robinson's passcode—the facts of this case support the conclusion that the disclosure of the passcode was "compelled." *See Miranda v. Arizona*, 384 U.S. 436, 458 (1966) ("Unless adequate protective devices are employed to dispel the compulsion inherent in custodial surroundings, no statement obtained from the defendant can truly be the product of his free choice.").

As described in Robinson's opening brief, Robinson was brought in to OSI as a suspect—not voluntarily—to be booked and interrogated. His passcode was requested during a custodial interrogation, inside an interrogation room, after he had invoked his right to the assistance of counsel, and after the investigator reinitiated questioning, despite his request for counsel. *See* AOB, p. 14.

[3] The OSI's Report of Investigation noted that Robinson's iPhone5s was running iOS 8.1.2.

[4] Kevin Poulsen, "Apple's iPhone Encryption is a Godsend, Even if Cops Hate It," *Wired* (Oct. 8. 2014), https://www.wired.com/2014/10/golden-key/.

[5] *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).

[6] *Id.*

"ciphertext" is converted back into readable text.[7]

When information is encrypted on a phone, computer, or other electronic device, it exists *only* in its scrambled format.[8] 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.

Thus, unlike the compelled opening of a safe or the compelled provision of a key to a lockbox—which merely provide access to preexisting evidence—compelled decryption transforms and translates existing, scrambled data into a new, readable form. Without obtaining the passcode from Robinson, investigators' search of his device would have yielded largely meaningless, encrypted data.

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) a testimonial communication, (2) self-incrimination, and (3) compulsion. *United States v. Hubbell*, 530 U.S. 27, 34 (2000).

The protections set forth in *Edwards v. Arizona*, 451 U.S. 477 (1981), and the mandatory warnings required by *Miranda v. Arizona*, 384 U.S. 436 (1966),

---

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

[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).

constitute two layers of "prophylaxis" designed to protect the accused's Fifth Amendment rights—including the prohibition on self-incrimination.

Despite these protections, this Court, like others, has determined that law enforcement may request consent to a search, even after counsel has been requested, without running afoul of *Edwards* or the Fifth Amendment. *See United States v. Roa*, 24 M.J. 297, 299 (1987). According to this line of cases, this is so because the "privilege against self-incrimination protects only *testimonial evidence*, not physical evidence." *Id*. (emphasis added). And, under that theory, providing consent is neither "a self-incriminating statement" nor "'in itself evidence of a testimonial or communicative nature.'" *See Smith v. Wainwright*, 581 F.2d 1149, 1152 (5th Cir. 1978) (quoting *United States v. Lemon*, 550 F.2d 467, 472 (9th Cir.1977)); *see also Doe*, 487 U.S. at 218 (compelled directive to bank authorizing disclosure of contents of bank accounts was not "testimonial").

Consenting to a search of a physical place or object is fundamentally different from disclosing information about that place or object (such as a passcode), for two reasons: First, reciting a passcode is self-incriminating when it provides the government with a direct link to incriminating evidence investigators could not otherwise access. Second, reciting a memorized passcode is evidence of a testimonial or communicative nature, because it requires disclosing the contents of the accused's mind to law enforcement and, in the context of decryption, the translation of unintelligible data into evidence that can be used against him.

Thus, unlike a request for consent to search, a request for a suspect to disclose the memorized passcode to an encrypted device containing incriminating evidence seeks a testimonial response. In the context of a custodial interrogation, after a suspect's invocation of the right to counsel, the introduction of evidence obtained as a result of compelled testimony is therefore prohibited by the Fifth Amendment.

I. DISCLOSURE OF A MEMORIZED PASSCODE TO AN ENCRYPTED DEVICE CONTAINING POTENTIALLY INCRIMINATING EVIDENCE IS SELF-INCRIMINATING.

The Fifth Amendment's privilege against self-incrimination is "protection against the prosecutor's use of incriminating information derived *directly or indirectly*" from compelled testimony. *Hubbell*, 530 U.S. at 38 (emphasis added). The privilege "not only extends to answers that would in themselves support a conviction under a federal criminal statute but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant for a federal crime." *Hoffman v. United States*, 341 U.S. 479, 486 (1951). That is, a communication need not *itself* be incriminating: it may still fall within the privilege, so long as it "may 'lead to incriminating evidence' . . . even if the information itself is not inculpatory." *Hubbell*, 530 U.S. at 38 (quoting *Doe*, 487 U.S. at 208, n. 6).

In *Mitchell*, this Court held that an investigator's request for a phone's passcode, or PIN, was "an express question, reasonably likely to elicit an incriminating response." 76 M.J. at 418. Likewise, this Court found that a "passcode itself . . . is incriminating information in the Fifth Amendment sense, and thus privileged." *Id.*

The same is true here: the investigators sought to search Robinson's phone because they believed it would contain evidence regarding the allegations against him. They needed Robinson's passcode in order to decrypt the phone's contents. Robinson's recitation of his password was thus a direct—and necessary—"link in the chain of evidence needed to prosecute" Robinson for a crime. *Hoffman*, 341 U.S. at 486. Thus, wholly aside from whether the passcode, itself, was incriminating, Robinson's recitation of the passcode was sufficiently incriminating

because it formed a "link in the chain of evidence" necessary to secure incriminating information.[9]

Moreover, the investigators should have known that their request was likely to elicit an incriminating response. Indeed, the sole purpose for their request was to facilitate their ability to access and understand any incriminating evidence that was stored on Robinson's phone. *Cf. States v. Smith*, 3 F.3d 1088, 1098–99 (7th Cir. 1993) (officer should have known that a question about the ownership of a bag containing incriminating evidence of a drug conspiracy would elicit an incriminating response); *United States v. Henley*, 984 F.2d 1040, 1043 (9th Cir. 1993) (agent should have known that his question about the ownership of a car was likely to elicit incriminating response: "The FBI agent obviously hoped to find evidence in the car incriminating Henley; that's why he wanted to search it.").

II. PASSCODE-BASED DECRYPTION IS TESTIMONIAL PER SE.

Password-based decryption by the target of a criminal investigation is also testimonial per se—both because it involves disclosing the contents of the accused's mind to investigators, and also because it involves using those contents

---

[9] The Court of Appeals incorrectly assumed that the only self-incriminating component of the request for Robinson's passcode involved his ownership, dominion, or control of the phone. *See Robinson*, 76 M.J. at 671 ("Because there was no dispute as to Appellant's ownership, dominion, or control over the phone, his knowledge of the passcode did not incriminate him.").

That conclusion appears to have turned on principles arising from the "foregone conclusion doctrine." *See id.* at 669–70, 671. That doctrine, however, is typically employed to evaluate whether or not a physical act—generally, producing specific physical documents—would constitute *testimony* for purposes of the Fifth Amendment. *See Fisher v. United States*, 425 U.S. 391, 408 (1976). Whatever the precise scope of the foregone conclusion doctrine and its application to self-incrimination, *see Hubbell*, 530 U.S. at 44, it has no application in this case. *See* Section III, *infra* at 13–14.

to translate otherwise unintelligible evidence into a form that can be used and understood by investigators.

A. Reciting a memorized passcode requires disclosing the contents of an accused's mind to law enforcement.

The privilege against self-incrimination protects compelled "testimony," which includes communications—direct or indirect, spoken or physical—that require a person to use "the contents of his own mind" to relay facts. *Curcio v. United States*, 354 U.S. 118, 128 (1957); *Hubbell*, 530 U.S. at 38, 43; *Pennsylvania v. Muniz*, 496 U.S. 582, 595 & n.9 (1990).

A communication is thus testimonial if it produces, by "word or deed," an "expression of the contents of an individual's mind." *Doe*, 487 U.S. at 219 & n.1 (Stevens, J., *dissenting*); *id.* at 210 n.9; *Braswell v. United States*, 487 U.S. 99, 126 (1988) (Even "[p]hysical acts will constitute testimony if they probe the state of mind, memory, perception, or cognition of the witness.") (Kennedy, J. *dissenting*). The privilege protects any "cognition caused by the state, the paradigmatic example being the retrieval of information from memory." Ronald Allen & M. Kristin Mace, *The Self-Incrimination Clause Explained and Its Future Predicted*, 94 J. Crim. L. & Criminology 243, 268 (2004); *see also Doe*, 487 U.S. at 215 (communication not testimonial where "the Government is not relying upon the 'truthtelling'" of the suspect) (citation and internal quotations omitted).

Ultimately, any compelled "truthtelling" that relies on the "contents of a [suspect's] mind" is testimonial. *Hubbell*, 530 U.S. at 43, 44 (citation and internal quotations omitted); *Doe*, 487 U.S. at 215. And courts have found the disclosure of memorized passwords to be precisely the type of "truthtelling" that is protected by the Fifth Amendment. *See 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"); *Sec. & Exch. Comm'n v. Huang*, No. CV 15-269, 2015 WL 5611644, at *3 (E.D. Pa. Sept. 23, 2015) ("Defendants' confidential passcodes are personal in nature and Defendants may properly invoke the Fifth Amendment privilege to avoid production of the passcodes."); *Commonwealth v. Baust*, 89 Va. Cir. 267, at *4 (Va. Cir. Ct. 2014) ("[T]he production of a password forces the Defendant to 'disclose the contents of his own mind.'"); *see also United States v. Green*, 272 F.3d 748, 753, 749–50 (5th Cir. 2001) (there is "no serious question" that asking a suspect in custody to disclose the locations and open the combination locks of cases containing firearms after he had been given his Miranda warnings and had requested counsel was "custodial interrogation" resulting in "testimonial and communicative" acts).[10]

Here, the government relied on Robinson "truthful[ly]" disclosing the "'contents of his own mind'"—*i.e.*, his memorized passcode—to obtain evidence contained on Robinson's phone. *See Hubbell*, 530 U.S. at 42, 43 (quoting *Curcio*, 354 U.S. at 128). Robinson's compelled disclosure of his phone's passcode was therefore testimonial.

[10] The Court of Appeals cited the unpublished decision in *United States v. Venegas*, 594 Fed. Appx. 822 (5th Cir. 2014), as holding that both requests for consent to search and requests for a phone's passcode are neither testimonial nor communicative in nature. *See Robinson*, 76 M.J. at 670. Although the defendant in *Venegas* disclosed his phone's passcode after consenting to a search of his phone, the Fifth Circuit did not actually address the question of whether the request for the phone's passcode was testimonial. It held only that "'[a] statement granting "consent to a search . . . is neither testimonial nor communicative in the Fifth Amendment sense."'" *Venegas*, 594 F. App'x at 827 (citations omitted; quotations, ellipsis, and bracketed language in the original).

B. Passcode-based decryption is testimonial because it requires a suspect to translate information.

Passcode-based decryption is also testimonial because it involves the translation and creation of information for law enforcement. It does not simply unlock or surrender information already in existence. *Cf. Fisher*, 425 U.S. at 411 (the act of producing papers is "not [a question] of testimony but of surrender") (citation and internal quotations omitted).

Because of its unique technical characteristics, *see supra* at 4–6, decryption communicates the content and features of each and every file within an encrypted space. Indeed, it communicates whether any files exist at all, demonstrating its testimonial nature. *See Hubbell*, 530 U.S. at 43 ("[W]e have no doubt that the constitutional privilege against self-incrimination protects [a suspect] from being compelled to answer questions designed to elicit information about the existence of sources of potentially incriminating evidence.").

Consequently, the investigators here were not merely seeking the surrender of known but inaccessible documents. They were seeking the *transformation* and *explanation* of data. The investigators were in possession of all the information they sought, but without the passcode, 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 Robinson's unique knowledge—his memorized passcode—to assemble the puzzle for the purpose of aiding in his own prosecution.

This compelled translation—by a suspect, relying on his truthful recollection and use of a memorized passcode—is thus additionally testimonial.

III. RECITING A MEMORIZED PASSCODE IS NOT AN ACT OF PRODUCTION AND THE "FOREGONE CONCLUSION DOCTRINE" THEREFORE HAS NO APPLICATION HERE.

The court below—at the government's urging, *see Robinson*, 76 M.J. at 669—appears to have improperly relied on a narrow exception to the self-incrimination privilege, known as the "foregone conclusion" doctrine, to conclude that Robinson's recitation of his memorized passcode raises no Fifth Amendment concerns. *See id.* at 669–70, 671.

Reliance on the foregone conclusion doctrine was wholly misplaced: the doctrine applies only to testimonial *acts of production*. Yet, here, investigators requested that Robinson *verbally* provide them with the passcode. That response cannot be interpreted as an "act of production," let alone one that was a "foregone conclusion." Expanding a narrow exception to allow the government to compel verbal testimony risks allowing the exception to swallow the rule.

The privilege against self-incrimination distinguishes between compelled "testimony," which is protected, and rote physical acts, which generally are not. "[M]ere physical act[s]" that do not express or rely on the contents of a person's mind are not testimonial and thus not protected. *Hubbell*, 530 U.S. at 43. For example, wearing a particular shirt, *Holt v. United States*, 218 U.S. 245, 252–53 (1910), providing a blood sample, *Schmerber*, 384 U.S. at 761, providing a handwriting exemplar, *Gilbert v. California*, 388 U.S. 263, 266–67 (1967), all have been found to be non-testimonial physical acts.

Nevertheless, and despite being a physical act, a suspect's act of producing documents may still be testimonial if that production "entail[s] implicit statements of fact." *Doe*, 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." *Hubbell*, 530 U.S. at 36 (citation

and internal quotations omitted). Producing evidence is always testimonial where the government does not know the existence and location of the evidence, or where production would implicitly authenticate the evidence. *See Doe*, 487 U.S. at 205, 210, 215–16.

Courts have recognized a narrow exception to this rule, primarily in the context of document production. The government may compel a suspect to surrender records, even where the act of surrender implies testimonial facts, if all of the facts attendant with that production are a "foregone conclusion" already known to the government. *Hubbell*, 530 U.S. at 44. A foregone conclusion exists only when the resulting act of production "adds little or nothing to the sum total of the Government's information." *Fisher*, 425 U.S. at 411.

But, as all this shows, central to the application of the foregone conclusion doctrine is a compelled *act of production*. None existed here. Investigators requested that Robinson "give"—that is, state or say—his memorized passcode, which he did. AOB, p. 7; JA 192. Investigators did not ask Robinson to *produce* a preexisting copy of the passcode that they could use to decrypt the phone themselves. The narrow foregone conclusion doctrine has no application here, where it is wholly untethered to an act of production.

Extending the foregone conclusion doctrine to verbal testimony would constitute a dramatic expansion of the doctrine—one that threatens a broader deterioration of the self-incrimination privilege. This Court should reject such an invitation.

CONCLUSION

For these reasons, this Court should find that the military judge abused his discretion by not suppressing all the evidence derived from Robinson's cellphone search and set aside the findings and sentence.

Date: September 28, 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)
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 4,051 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: September 28, 2017

CERTIFICATE OF FILING AND SERVICE

I certify that a copy of the foregoing Motion for Leave to File Brief of Electronic Frontier Foundation, American Civil Liberties Union, and ACLU of the District of Columbia as Amici Curiae, Brief of Amici Curiae Electronic Frontier Foundation, American Civil Liberties Union, and ACLU of the District of Columbia In Support of Appellant, and Motion(s) To Appear Pro Hac Vice, transmitted by electronic means with the consent of the counsel for Appellee Air Force Appellate Government Division Maj. Tyler B. Musselman tyler.b.musselman.mil@mail.mil, and counsel for Appellant, Maj. Patricia Encarnación-Miranda patricia.encarnacionmiranda.mil@mail.mil and Maj. Mark C. Bruegger mark.c.bruegger.mil@mail.mil, and the Clerk of the Court Joseph R. Perlak, efiling@armfor.uscourts.gov on September 28, 2017.

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