IN THE SUPREME COURT OF PENNSYLVANIA
MIDDLE DISTRICT

NO. 56 MAP 2018

COMMONWEALTH OF PENNSYLVANIA,

Appellee,

v.

JOSEPH J. DAVIS,

Appellant.

BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION

Appeal from the Order of the Superior Court (Docket No. 1243 MDA 2016), Filed on November 30, 2017, Reconsideration Denied on February 5, 2018, Affirming a Judgment of Contempt Entered on June 30, 2016 by the Luzerne County Court of Common Pleas, Criminal Division, at Nos. CP-40-CR-291-2016 and CP-40-MD-11-2016

Thomas J. Farrell (PA No. 48976)
Farrell & Reisinger, LLC
300 Koppers Building
436 Seventh Avenue
Pittsburgh, PA 15219
(412) 894-1380
tfarrell@farrellreisinger.com

Attorneys for Amicus Curiae
Electronic Frontier Foundation

On the Brief:

Jamie Williams
Andrew Crocker
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109

IN THE SUPREME COURT OF PENNSYLVANIA
MIDDLE DISTRICT

NO. 56 MAP 2018

COMMONWEALTH OF PENNSYLVANIA,

Appellee,

v.

JOSEPH J. DAVIS,

Appellant.

BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION

Appeal from the Order of the Superior Court (Docket No. 1243 MDA 2016), Filed on November 30, 2017, Reconsideration Denied on February 5, 2018, Affirming a Judgment of Contempt Entered on June 30, 2016 by the Luzerne County Court of Common Pleas, Criminal Division, at Nos. CP-40-CR-291-2016 and CP-40-MD-11-2016

Thomas J. Farrell (PA No. 48976)
Farrell & Reisinger, LLC
300 Koppers Building
436 Seventh Avenue
Pittsburgh, PA 15219
(412) 894-1380
tfarrell@farrellreisinger.com

Attorneys for Amicus Curiae
Electronic Frontier Foundation

On the Brief:

Jamie Williams
Andrew Crocker
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Constitutional Provisions

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 37,000 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 that individuals are not placed at the mercy of advancements in technology—and that constitutional protections, including the Fifth Amendment privilege against self-incrimination, are carried into the digital age.

In this regard, EFF has participated as *amicus curiae* in several cases regarding the application of the Fifth Amendment to the compelled disclosure of passwords and the compelled decryption of digital devices, including *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (11th Cir. 2012); *United States v. Spencer,* No. 17-CR-00259-CRB-1, 2018 WL 1964588 (N.D. Cal. Apr. 26, 2018); *United States v. Apple MacPro Computer*, 851 F.3d 238 (3rd Cir. 2017); *United States v. Mitchell*, 76 M.J. 413 (CAAF 2017); *United States v. Fricosu*, 841 F. Supp. 2d 1232 (D. Colo. 2012); *United States v.*

[1] *Amicus* certifies, pursuant to Rule 531(b)(2) of the Pennsylvania Rules of Appellate Procedure, that no person or entity, other than *Amicus*, its members, or its counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part.

Decryption of a Seized Data Storage System, No. 2:13-mj-449-RTR, 2013 WL 12327372 (E.D. Wis. Apr. 19, 2013); *Commonwealth v. Gelfgatt*, 11 N.E.3d 605 (Mass. 2013).

INTRODUCTION

In this case, prosecutors seek to compel the defendant to provide the password required to decrypt his computer's entire hard drive in violation of the Fifth Amendment's privilege against self-incrimination. While the encryption of personal devices is relatively new, the dilemma faced by law enforcement here is an old one: investigators seek additional evidence of a crime, and they believe that only the criminal suspect himself has the knowledge necessary to access that evidence. Decades—if not centuries—of precedent and practice support the conclusion that, in cases like this one, a suspect cannot be compelled to recall and use information that exists only in his mind in order to aid the government's prosecution. *See Curcio v. United States*, 354 U.S. 118, 128 (1957).

The lower court nevertheless ruled that Appellant may be compelled to recall from memory and then reproduce to law enforcement the password for decrypting his computer. The court erroneously concluded that the disclosure of Appellant's password from memory would not be testimonial. It reasoned that the existence, custody, and authenticity *of the password* are foregone conclusions. *Commonwealth v. Davis*, 176 A.3d 869, 875–76 (Pa. Super. Ct. Nov. 30, 2017), *reargument denied* (Feb. 5, 2018), *appeal granted,* No. 169 MAL 2018, 2018 WL 4775622 (Pa. Oct. 3, 2018).

This ruling improperly expands the foregone conclusion rationale—a limited exception to the Fifth Amendment privilege against self-incrimination—to compel the disclosure of a memorized password. The lower court's expansive application of the foregone conclusion exception would, if upheld, undermine core Fifth Amendment protections, not only in cases involving serious crimes like those alleged here, but in all cases, for all Americans.

This holding is based on a flawed understanding of the foregone conclusion exception.

First, the Supreme Court has applied the foregone conclusion exception narrowly, to the compelled production of specific, existing business or financial records. The exception does not apply in the context of attempts to compel suspects to recite, write, type, or otherwise reproduce the contents of their minds, such as a memorized password.

Second, even if the foregone conclusion exception did apply outside that narrow context, and if the government had sought to compel Appellant to produce the decrypted contents of his computer rather than disclosure of his password, the exception would still have no application in this case. The government has not established that any and all testimonial aspects of the act of producing the decrypted hard drive—or more precisely, whatever records it contains—would be foregone conclusions. *See In re Grand Jury Subpoena Duces Tecum Dated March*

25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012); *G.A.Q.L. v. State*, No. 4D18-1811, 2018 WL 5291918, at *6 (Fla. Dist. Ct. App. Oct. 24, 2018). This would require, among other things, the government to show with reasonable particularity that it knew of the contents of the entire computer—and that the existence of the individual files, as well as the defendant's control over them and their authenticity, was a foregone conclusion.[2] *See United States v. Hubbell,* 530 U.S. 27, 45 (2000). For an *entire* device or hard drive, this would be an all-but impossible task. Here, the government has identified two files that it suspects are located on Appellant's computer, but it has not attempted to make the required showing with regard to these files.

The order compelling Appellant to disclose the passcode should be reversed.

---

[2] The government need not identify exact file names, but it must show with specificity that the files sought exist. *In re Grand Jury Subpoena*, 670 F.3d at 1348–49.

ARGUMENT

I. COMPELLED PASSWORD DISCLOSURE OR USE BY THE TARGET OF A CRIMINAL INVESTIGATION IS TESTIMONIAL AND THEREFORE PRIVILEGED BY THE FIFTH AMENDMENT.

A. The Fifth Amendment Prohibits the Compelled Recitation or Reproduction of the Contents of a Suspect's Mind.

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 come within the self-incrimination privilege, an individual must show three things: (1) compulsion, (2) testimony, and (3) self-incrimination. *Hubbell*, 530 U.S. at 34.

The privilege distinguishes between compelled "testimony," which is protected, and rote physical acts, which generally are not. *Id.* at 43. "[M]ere physical act[s]" are not testimonial if they do not express or rely on the contents of a person's mind. *Id.* The Supreme Court has thus concluded that wearing a particular shirt, providing a blood sample, or providing a handwriting exemplar may all fall into the category of unprivileged physical acts. *Holt v. United States*, 218 U.S. 245, 252–53 (1910); *Schmerber v. California*, 384 U.S. 757, 761 (1966); *Gilbert v. California*, 388 U.S. 263, 266–67 (1967).

In contrast, privileged testimony includes communications, direct or indirect, verbal or non-verbal, that require a person to use "the contents of his own mind" to truthfully relay facts. *Hubbell*, 530 U.S. at 43 (citing *Curcio v. United States*, 354 U.S. 118, 128 (1957)). The testimonial nature of a communication does not turn

on whether it is spoken, but whether it requires, by "word or deed," a truthful "expression of the contents of an individual's mind." *Doe v. United States* ("*Doe II*"), 487 U.S. 201, 219 & n.1 (1988) (Stevens, J., dissenting). Thus, even "[p]hysical acts will constitute testimony if they probe the state of mind, *memory*, perception, or cognition of the witness." *Braswell v. United States*, 487 U.S. 99, 126 (1988) (Kennedy, J. dissenting) (emphasis added).

Distilled to its essence, testimony occurs when the government seeks: (1) verbal or non-verbal "truthtelling," *Hubbell*, 530 U.S. at 44 (internal citations and quotation marks omitted); that (2) relies on or probes the "contents of [a suspect's] own mind." *Id.* at 43 (quoting *Curcio*, 354 U.S. at 128).

B. The Compelled Recollection or Use of a Memorized Password is Testimonial.

The order issued by the lower court requires Appellant to give the government the password to his computer. This is testimony; it is the (1) truthful recollection of (2) a password stored only in Appellant's mind. So long as it is both compelled (it is) and self-incriminating (the government believes it will be),[3]

---

[3] Critically, the compelled testimony need not itself be incriminating to fall within the privilege, so long as the testimony provides a "link in the chain of evidence" needed to prosecute. *Hoffman v. United States*, 341 U.S. 479, 486 (1951); *Doe v. United States*, 487 U.S. 201, 208 n.6 (1988) (Compelled testimony that communicates information that may "lead to incriminating evidence" falls within the privileged, even if the information is not itself inculpatory); *see also United States v. Mitchell*, 76 M.J. 413, 418 (C.A.A.F. 2017) (government request for

his response is privileged by the Fifth Amendment. Many courts have recognized that not only reciting but also writing, typing, entering, or otherwise reproducing a password from memory are testimonial communications protected by the Fifth Amendment. *See, e.g., SEC v. Huang*, No. 15-cv-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*, No. 14-cr-1439, 89 Va. Cir. 267, 2014 WL 10355635, at *4 (Va. Cir. Ct. Oct. 28, 2014) ("[T]he production of a password forces the Defendant to 'disclose the contents of his own mind.'"); *Seo v. State*, No. 29A05-1710-CR-2466, 2018 WL 4040295, at *2 (Ind. Ct. App. Aug. 21, 2018); *G.A.Q.L.*, 2018 WL 5291918, at *4; *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d at 1346 ("[T]he decryption . . . of the hard drives would require the use of the contents of Doe's mind and could not be fairly characterized as a physical act that would be nontestimonial in nature.").

In cases involving an order that a defendant provide a password associated with a digital device, such as a computer or hard drive, "the government is not seeking documents or objects—*it is seeking testimony from the Defendant* . . . that will be used to incriminate him." *United States v. Kirschner*, 823 F. Supp. 2d 665,

---

password was interrogation reasonably likely to elicit an incriminating response). Here, the government believes the password to the encrypted hard drive will serve as *the* link to incriminating information stored on computer.

669 (E.D. Mich. 2010) (emphasis added). In *Kirschner*, the court quashed a subpoena for the production computer passwords, reasoning that, under *Hubbell* and *Doe*, the subpoena would have required the suspect "to divulge through his mental processes his password." *Id.*

Similarly, the Fifth Circuit held in *United States v. Green*, 272 F.3d 748, 753 (5th Cir. 2001), that there is "no serious question" that asking an arrestee to disclose the locations and open the combination locks of cases containing firearms constituted "testimonial and communicative" acts. According to the court, the defendant's disclosure of the locations and opening the locks of the cases constituted testimony as to his "knowledge of the presence of firearms in these cases and of the means of opening these cases." *Id.*

As in all of these cases, the government in this case is seeking compelled testimony from Appellant reproducing from memory his computer's password in order to aid in his prosecution. Without a grant of immunity, the Fifth Amendment's privilege against self-incrimination prohibitions compelling such incriminating testimony. *See Curcio*, 354 U.S. at 128 (compelling a suspect "to convict himself out of his own mouth . . . is contrary to the spirit and letter of the Fifth Amendment").

II. THE NARROW FOREGONE CONCLUSION EXCEPTION HAS NO APPLICATION IN THIS CASE.

The lower court erroneously held that the compelled disclosure of Appellant's passcode is justified pursuant to the foregone conclusion exception. For over forty years, and with few exceptions, the foregone conclusion doctrine has only been applied in the context of the production of specific business and financial records, and only if the government shows that any and all testimony inherent in the compelled act of production is a foregone conclusion. The exception is not applicable to the compelled disclosure of a memorized password; the few courts that have applied the foregone conclusion rationale in the context of orders to recall and/or use a memorized password have done so in error.

The foregone conclusion exception would also not apply to the compelled production of the entire contents of Appellant's computer, rather than specific, known files. The government has not demonstrated with reasonable particularity prior knowledge of the contents of the entire computer or of any other testimonial statements inherent in such an act of production. The lower court's erroneous and expansive application of the foregone conclusion exception should be reversed.

A. The Foregone Conclusion Exception Applies Only to the Production of Specified, Preexisting Business Records.

In *Fisher v. United States*, 425 U.S. 391, 410 (1976), the Supreme Court held that despite the testimony implicit in an act of production, the government

could nonetheless compel (i) the production of specific, preexisting tax records, (ii) if it could show that any testimonial aspects associated with the act of production were a "foregone conclusion." The Court recognized that the act of producing the tax records at issue carried "implicit" testimony about the records' existence, authenticity, and location in the defendants' possession. *Id.* at 410. The government, however, had independent confirmation of the existence and authenticity of the documents it sought relating to the accountants' preparation of the defendants' tax records—from the accountants who created them—and knew the documents were in possession of the defendants via their attorneys. *Id.* at 412–13. The Court concluded that the Fifth Amendment was therefore not implicated; any testimony implicit in the production was a "foregone conclusion," so the contents of the defendants' mind were not being used against them. *Id.* at 411.

The Court also noted that while "[s]pecial problems of privacy" might arise in the case of a subpoena seeking production of more sensitive documents, like a personal diary, such problems were not at issue in a case involving tax records prepared by an accountant and relating to the defendants' businesses. *Id.* at 394 nn.2–3, 401 n.7 (citing *United States v. Bennett*, 409 F.2d 888, 897 (2d Cir. 1969)).

In the 42 years since *Fisher* was decided, the Supreme Court has applied the foregone conclusion exception only when the government seeks to compel the production of preexisting business or other financial records, and even then only if

those documents are adequately specified by the government. *Hubbell*, 530 U.S. at 44–45 (holding that the case "plainly [fell] outside of" the foregone conclusion exception where the government sought "general business or tax records that [fell] within the broad categories described in this subpoena" rather than specific, known files).

In *United States v. Doe* ("*Doe I*"), 465 U.S. 605, 612–614 (1984), for example, the Court refused to apply the foregone conclusion exception because the subpoena at issue sought not specific, known files, but rather several broad categories of general business records—including the telephone records of several of the respondent's companies and all records pertaining four bank accounts. The Court cited the Third Circuit's decision in the case below: "'The most plausible inference to be drawn from the broad-sweeping subpoenas is that the Government, unable to prove that the subpoenaed documents exist—or that the appellee even is somehow connected to the business entities under investigation—is attempting to compensate for its lack of knowledge by requiring the appellee to become, in effect, the primary informant against himself.'" *Id.* at 613 n.12 (quoting *In re Grand Jury Empanelled Mar. 19, 1980*, 680 F.2d 327, 335 (3d Cir. 1982)). The Court recognized that production of the documents would constitute a tacit admission of both their existence and the defendant's possession of them, and "relieve the Government of the need for authentication." *Id.* at 614 n.13. This was

"sufficient to establish a valid claim of the privilege against self-incrimination." *Id.*

The Court has applied the foregone conclusion exception to only specific, preexisting business and financial records for good reason. These records are a unique category of material that, to varying degrees, has been subject to compelled production and inspection by the government for over a century. *See, e.g.*, *Braswell*, 487 U.S. at 104; *Shapiro v. United States*, 335 U.S. 1, 33 (1948). Lower courts, too, have overwhelmingly applied the exception only in cases concerning the compelled production of specific, preexisting business and financial records. *See, e.g., United States v. Bell,* 217 F.R.D. 335, 341–42 (M.D. Pa. 2003) ("tax avoidance" materials advertised on the website for the defendant's business); *United States v. Gippetti*, 153 F. App'x 865, 869 (3d Cir. 2005) (Cayman National Bank bank and credit card account records); *United States v. Sideman & Bancroft, LLP*, 704 F.3d 1197, 1200 (9th Cir. 2013) (business and tax records); *United States v. Bright*, 596 F.3d 683, 689 (9th Cir. 2010) (credit card records associated with an offshore account); *In re Grand Jury Subpoenas Served Feb 27, 1984*, 599 F. Supp. 1006, 1012 (E.D. Wash. 1984) (records related to a business partnership); *cf. Burt Hill, Inc. v. Hassan*, No. CIV.A. 09-1285, 2010 WL 55715, at *2 (W.D. Pa. Jan. 4,

2010) (contents of electronic storage devices used by the defendants while they were employed by the plaintiff).[4]

In this case, the government does not seek an order compelling the production of an existing record, let alone a specific, preexisting business or financial record, but rather but an order compelling the Appellant to recall his memorized password and reproduce those contents of his mind for law enforcement. *See G.A.Q.L.*, 2018 WL 5291918, at *6 (Kuntz, J., concurring) (the Court has applied the exception only "when the compelled testimony has consisted of existing evidence such as documents"). Appellant's memorized password is not a pre-existing record. "'The password is not a physical thing. If [Appellant]

---

[4] Courts also routinely decline to apply the foregone conclusion exception to cases involving the compelled production of physical evidence, such as guns or drugs, because the act of production in such cases would constitute an implicit admission of guilty knowledge. *See Commonwealth v. Hughes*, 380 Mass. 583, 592 (1980) (ordering the production of a gun would require the defendant to make "implicitly a statement about its existence, location and control to which the Commonwealth says it would allude at trial to show he had possession and control at some point after the alleged crime"); *State v. Dennis*, 16 Wash. App. 417, 423 (1976) (the act of "procuring the cocaine from its hiding place . . . served more graphically than words to convey the incriminating fact that [the defendant] knew of the presence and precise location within his home of the contraband substance"); *Goldsmith v. Superior Court*, 152 Cal. App. 3d 76, 87 n.12 (1984) (holding that compelling the production of a weapon allegedly used in a crime, where that government had independent evidence that the defendant possessed the gun at the time of and after the offense, would be like compelling a confession from an accused "as soon as the government announced (or was able to show) that [in] a future trial it could produce enough independent evidence to get past a motion for a directed verdict of acquittal") (citation omitted).

knows the password, it only exists in his mind.'" *See Baust*, 2014 WL 10355635, at *3 (quoting *In re Grand Jury Subpoena (Boucher)*, No. 2:06–MJ–91, 2007 WL 4246473, at *6 (D. Vt. Nov. 29, 2007), *appeal granted, decision rev'd*, 2009 WL 424718 (D. Vt. Feb. 19, 2009)).

"Whatever the scope of this 'foregone conclusion' rationale," *Hubbell*, 530 U.S. at 44, it does not allow the government to compel a suspect to speak, write, type, or otherwise reproduce the contents of their mind to aid in their prosecution. The compelled recollection or use of Appellant's memorized password is testimonial and therefore privileged, and the foregone conclusion exception is thus not applicable in this case. The Court's analysis need not proceed further. Expanding the foregone conclusion exception to apply beyond its typical narrow confines risks a broad erosion of the privilege against self-incrimination.

B. Even If the Foregone Conclusion Analysis Were to Apply, the Government Must Show That Any and All Testimony Inherent in the Compelled Production Is a Foregone Conclusion.

For the reasons stated above, the foregone conclusion rationale can never apply to the compelled disclosure of passwords. *See Baust*, 2014 WL 10355635, at *4 (knowledge of a password itself can never be a foregone conclusion; if it were, the government "would not need to compel Defendant to produce it because they would already know it").

In some cases, rather than compelling suspects to provide their passwords, the government has instead sought to compel them to directly decrypt encrypted devices, by typing or otherwise entering their password on the digital device. Even assuming the foregone conclusion rationale can ever be applied in the context of decryption orders, and even if the government here sought a decryption order rather than production of a password, the foregone conclusion exception would still not apply in this case. That is because the government does not carry its burden in the foregone conclusion analysis when it demonstrates knowledge of the existence, location, and authenticity *of a device or its password.* Instead, the government must make that showing with respect to the particular information it ultimately seeks. *In re Grand Jury Subpoena*, 670 F.3d at 1346; *Huang*, 2015 WL 5611644, *3. It has not done so here.

The foregone conclusion exception only applies in cases like *Fisher*, where the government can show that *any and all* testimony inherent in the compelled act of production would be a foregone conclusion. *See* 425 U.S. at 411; *see also In re Grand Jury Subpoena*, 670 F.3d at 1345 (noting that in *Fisher*, "the Government had knowledge of each fact that had the potential of being testimonial"). An act of production is not a violation of the Fifth Amendment, even when it conveys a fact, if the government can show with reasonable particularity that it has independent knowledge of the material sufficiently comprehensive to render "any testimonial

aspect a 'foregone conclusion.'" *Id.* at 1346. By contrast, where an act of production implies a statement of fact that the government has not shown to be a foregone conclusion, compelling that act of production would violate the Fifth Amendment. *See, e.g., Hubbell*, 530 U.S. at 45 (finding that respondent's act of production had at least two testimonial aspects, with respect to the existence and location of the documents, that were not foregone conclusions; the government failed to show "that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent").

In the context of compelled production of decrypted hard drives or digital devices, multiple courts have declined to hold that the foregone conclusion rationale was satisfied for the act of producing decrypted files, because producing the files would constitute an implicit admission of guilty knowledge. For example, in the leading opinion, *In re Grand Jury Subpoena,* the Eleventh Circuit held that an order to produce a decrypted hard drive had multiple testimonial aspects: it would be "tantamount to testimony by [the defendant] of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; *and* of his capability to decrypt the files." *See In re Grand Jury Subpoena*, 670 F.3d at 1346 (emphasis added). The court explained that, in the context of compelled production of the contents of

a decrypted computer, the foregone conclusion exception only applies if the government can demonstrate with reasonable particularity that it knows of the specific information on the hard drive. The government must show with "reasonable particularity" the "specific file names" of the records sought, or, at minimum, a showing that the government 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. "[C]ategorical requests for documents the Government anticipates are likely to exist simply will not suffice." *Id.* at 1347 (citing *Hubbell*, 530 U.S. at 45; *Doe I*, 465 U.S. at 613–14 & nn.11–13).

The Eleventh Circuit concluded that the government had failed to satisfy this standard because it did not establish 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."[5]

[5] Significantly, the Eleventh Circuit rejected the government's assertion that use of encryption alone demonstrated that the suspect "was trying to hide something." *In re Grand Jury Subpoena*, 670 F.3d at 1347. 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.*

Id. at 1347 (emphasis in original). Thus, the government did not know "the existence or the whereabouts" of the records it sought. *Id.*

The Florida Court of Appeals also recently held that the government had failed to satisfy the standard for application of the foregone conclusion exception. *G.A.Q.L.*, 2018 WL 5291918, at *5.[6] "Without reasonable particularity as to the documents sought behind the passcode wall, the facts of this case 'plainly fall outside' of the foregone conclusion exception and amount to a mere fishing expedition." *Id.* (quoting *Hubbell*, 530 U.S. at 44); *see also Huang*, 2015 WL 5611644, at *3 (denying a motion to compel the defendants to supply passwords to their smartphones because the SEC could not establish with "reasonable particularity" that any documents sought resided in the locked phones). *Cf. Boucher*, 2009 WL 424718, *2 (denying a motion to quash a subpoena to provide

[6] Courts, including the Florida court in *G.A.Q.L.*, have often treated orders compelling a suspect to recall and recite, type, or otherwise reproduce a memorized password (in order to decrypt an entire device) as orders compelling the production of preexisting documents (that happen to be encrypted). This stems from courts' recognition that, in cases involving a demand that a suspect recite or enter a decryption password, what the government ultimately seeks is not the password itself but rather the evidence on the device. *See, e.g., G.A.Q.L.*, 2018 WL 5291918, at *4 ("the 'evidence sought' in a password production case such as this is not the password itself; rather, it is the actual files or evidence on the locked phone"). The appropriate focus of the inquiry, however, is *what the government actually demands* a suspect to produce. The conceptual difference between a request to compel the production of documents and a request to compel a suspect to recite, type, or otherwise reproduce a password from memory is a critical one; the foregone conclusion exception can never apply in the later situation, as it involves pure testimony—not an act of production of existing records.

an unencrypted version of a hard drive where, after the defendant admitted that he sometimes downloaded child pornography and showed the border agents the drive where he downloaded files, the agents examined the defendant's computer and observed thousands of file names reflecting apparent child pornography); *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1235 (D. Colo. 2012) (compelling a fraud suspect to decrypt a laptop where the laptop, bearing the suspect's name, was seized from the suspect's bedroom, and where the suspect had admitted on a record jail call that the laptop contained incriminating information); *United States v. Apple MacPro Computer*, 851 F.3d 238, 248 (3rd Cir. 2017) ("Unlike *In re Grand Jury Subpoena,* the Government has provided evidence to show both that files exist on the encrypted portions of the devices and that Doe can access them.").

Here, even if the government had sought to compel the production of the records on Appellant's hard drive, because the government has not established that the contents of the hard drive are a foregone conclusion, the requirements necessary to satisfy the foregone conclusion exception would not be met. Namely, by producing the contents of the computer, Appellant would be tacitly "admit[ing] their existence and his possession" and "would relieve the Government of the need for authentication." *See Doe I*, 465 U.S. at 614, n.13 ("[I]f the Government obtained the documents from another source, it would have to authenticate them before they would be admissible at trial."); *see also Baust*, 2014 WL 10355635, at

*4 (compelling production of unencrypted recording that may have been transmitted to defendant's encrypted cell phone would violate defendant's Fifth Amendment privilege against self-incrimination: "Defendant would be admitting the recording exists, it was in his possession and control, and that the recording is authentic").

Unlike in the courts in *Boucher*, *Fricosu*, and *Apple MacPro*, where the government had preexisting knowledge of either specific incriminating files *on the drives* or testimony from an eyewitness who saw the subject access incriminating content from the specific device at issue, the government's evidence here is far less particular. *See Boucher*, 2009 WL 424718, *2 (agent observed apparent child pornography on computer); *Fricosu*, 841 F. Supp. 2d at 1235 (suspect admitted information sought "was on my laptop"); *Apple MacPro*, 851 F.3d at 248 (Doe's sister "witnessed Doe unlock his Mac Pro while connected to the hard drives to show her hundreds of pictures and videos of child pornography"); *see also In re Grand Jury Subpoena,* 670 F.3d at 1348–49, 1349 n.27 (distinguishing *Boucher* and *Fricosu*).

Even for the two files the government alleges that Appellant at some point may have accessed or shared, that the files remain on Appellant's computer is a matter of pure speculation. *See United States v. Greenfield*, 831 F.3d 106, 120–23 (2d Cir. 2016) (declining to apply the foregone conclusion exception where the

government established only that a suspect *at some point past* was in possession of the specific records sought, but not that possession remained ongoing).

Even if the government were to establish that the existence, authenticity, and control of *particular files* were a foregone conclusion, such a finding would at most support compelling Appellant provide to the government only those specific files. It would not support an order compelling Appellant to decrypt and produce the entire contents of his computer's hard drive. Here, the government has failed to identify with reasonable particularity even the existence of a single file on Appellant's device. At this stage, whatever the computer contains, it is decidedly not a foregone conclusion.

A few courts in recent years—including the lower court in this case—have misconstrued the standard necessary for application of the foregone conclusion exception in the context of compelled decryption orders. These courts have assumed the foregone conclusion exception is satisfied were the government can show knowledge of the existence, location, and authenticity *of a device or its password*, and the general possibility that files are stored on the devices. *See, e.g., State v. Stahl*, 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016) ("the relevant question is whether the State has established that it knows with reasonable particularity that the passcode exists, is within the accused's possession or control, and is authentic"); *but see G.A.Q.L.*, 2018 WL 5291918, at *4 ("[T]he trial court

specifically held that the 'existence, custody, and authenticity of the passcodes are a foregone conclusion' in the order appealed. This holding, which focuses on the passcodes rather than the data behind the wall, misses the mark.").[7]

This overbroad construction of the foregone conclusion exception impermissibly shifts the government's burden from the information to be produced—the proper focus of the foregone conclusion doctrine—to pure testimony, the password. *See Huang*, 2015 WL 5611644, *3; s*ee also Doe I*, 465 U.S. at 614 n. 12. To establish that any and all testimonial aspects of the act of production were foregone conclusions, the government must show independent knowledge of the existence, location, and authenticity *of the particular information it seeks*. *In re Grand Jury Subpoena*, 670 F.3d at 1346; *Huang*, 2015 WL 5611644, *3. The government has not done so here.

The lower court's erroneous application of the foregone conclusion exception should be reversed.

---

[7] In *Commonwealth v. Gelfgatt*, 11 N.E.3d 605 (Mass. 2014), Massachusetts' highest court also 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).

III. THE VALUES ANIMATING THE PRIVILEGE AGAINST SELF-INCRIMINATION REINFORCE THE TESTIMONIAL NATURE OF THE COMPELLED PRODUCTION OR USE OF ENCRYPTION PASSWORDS.

The Supreme Court has explained that the self-incrimination 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 of 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 v. Waterfront Commission of New York Harbor*, 378 U.S. 52, 55 (1964)) (internal quotation marks omitted).

Each element of the "cruel trilemma" is at work in cases of compelled disclosure or use of decryption passwords. The government gives those using encryption a choice: either provide the allegedly incriminating information you possess; lie about your inability to do so; or fail to cooperate and be held in contempt.[8] The privilege was designed to prevent suspects from facing this "trilemma" in the first instance. *See id.* at 212 (quoting *Murphy*, 378 U.S. at 55).

---

[8] A person who does not know or cannot remember the password to a device 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.

Forced disclosure or entry of a decryption key also encroaches on "the right of each individual to a private enclave where he may lead a private life." *Id.* (quoting *Murphy*, 378 U.S. at 55) (internal quotation marks omitted). 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) (en banc). Electronic devices may thus contain "a digital record of nearly every aspect of [users'] lives — from the mundane to the intimate." *Riley*, 134 S. Ct. at 2490.

Using encryption to secure these devices—containing the very "privacies of life," *id.* at 2495 (citation omitted)—affords some limited measure of security in an otherwise insecure digital world. Indeed, encryption is integral for safeguarding the privacy and security of sensitive, electronically stored information. The use of strong encryption is now a routine practice for individuals and an industry standard for businesses. Computer and software manufacturers consider disk encryption to be a basic computer security measure and include disk encryption software as a standard feature on most new computers. For example, the two most widely used

operating systems for personal computers—Microsoft Windows and Apple Mac OS—both offer encryption tools.[9] Device encryption is also a standard feature for the leading smart phone operating systems, Apple iOS and Android.[10]

In addition, government agencies recommend encryption to protect personal data and Internet traffic.[11] Many federal and state laws require or encourage encryption to protect sensitive information.[12] In this increasingly connected world, encryption is a pervasive and integral part of modern life.

Allowing the government to force a suspect to disclose or enter the password for decrypting a personal device on a mere showing that an individual knows the

---

[9] Apple, *MacOS Security*, https://www.apple.com/macos/security/ (describing Mac OS FileVault 2 encryption); Microsoft, *BitLocker*, https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview.

[10] Apple, *This Is How We Protect Your Security*, https://www.apple.com/privacy/approach-to-privacy; Android, *Encryption*, https://source.android.com/security/encryption/.

[11] *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 ("Use strong cryptography to secure confidential material[.]"); National Institute of Standards and Technology, NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices* (Nov. 2007), https://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf.

[12] *See, e.g.*, 15 U.S.C. § 6801(b) (requiring security measures for consumer financial data); 12 C.F.R. § Pt. 364, App. B (2015) (interagency rules interpreting § 6801 to require assessment of need for encryption of that information); 32 C.F.R. § Pt. 310, App. A (E)(1) (2007) (requiring encryption for unclassified Department of Defense employee information); Cal. Civ. Code § 1798.29(a) (2017) (requiring notification in event of data breach for unencrypted information).

password—as the lower court in this case held—would render the protections for the "privacies of life" hollow by effectively "expand[ing] the contours of the foregone conclusion exception so as to swallow the protections of the Fifth Amendment." *G.A.Q.L.*, 2018 WL 5291918, at *4. Pursuant to the court's reasoning, "every password-protected [device] would be subject to compelled unlocking since it would be a foregone conclusion that any password-protected [device] would have a passcode." *Id.* The Constitution demands more before a suspect may be forced to expose his most private information for government inspection.

CONCLUSION

The order compelling Appellant to disclose his passcode should be reversed.

Dated: November 19, 2018

Respectfully submitted,

By:
Thomas J. Farrell (PA No. 48976)
Farrell & Reisinger, LLC
300 Koppers Building
436 Seventh Avenue
Pittsburgh, PA 15219
(412) 894-1380
tfarrell@farrellreisinger com

On the brief:
Jamie Williams
Andrew Crocker
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109

Attorneys for Amicus Curiae
Electronic Frontier Foundation

CERTIFICATE OF WORD COUNT COMPLIANCE

Pursuant to Pa. R.A.P. 2135, this is to certify that the Brief for *Amicus Curiae* Electronic Frontier Foundation complies with the word count limit set forth in Pa. R.A.P. 2135(a)(1). The word count as counted by the Microsoft Word word-processing program used to prepare this brief states that those sections that shall be included in the word count under Rule 2135(b) contain 6,268 words.

By: Thomas Farrell
Thomas J. Farrell
PA No.

Attorney for Amicus Curiae
Electronic Frontier Foundation

Date: November 19, 2018

CONFIDENTIAL INFORMATION AND CONFIDIENTIAL DOCUMENTS CERTIFICATION

Pursuant to Pa. R.A.P. 127, I certify that this filing complies with the provisions of the Public Access Policy of the Unified Judicial System of Pennsylvania: Case Records of the Appellate and Trial Courts that require filing confidential information and documents differently than non-confidential information and documents.

By: 
Thomas J. Farrell
PA No. 48976

Attorney for Amicus Curiae
Electronic Frontier Foundation

Date: November 19, 2018