MARK RUMOLD (SBN 279060)
mark@eff.org
ANDREW CROCKER (SBN 291596)
JAMIE L. WILLIAMS (SBN 279046)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Fax: (415) 436-9993

Counsel for Amicus Curiae

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA,

v.

RYAN MICHAEL SPENCER,

Case No. 3:17-cr-00259-CRB

BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT'S OBJECTIONS TO MAGISTRATE JUDGE'S ORDER

Hon. Charles R. Breyer

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Rules

Statutes

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 40,000 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 individuals to protect their privacy and security. EFF has participated as amicus curiae in several cases regarding the application of the Fifth Amendment to compelled password use and disclosure and decryption, including *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (11th Cir. 2012); *United States v. Apple MacPro Computer, et al.*, 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. Decryption of a Seized Data Storage System*, No. 2:13-mj-449-RTR (D. Wisc. 2013); and *Commonwealth v. Gelfgatt*, 11 N.E.3d 605 (Mass. 2013).

[1] Amicus EFF certifies 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.

SUMMARY OF THE ARGUMENT

In this case, prosecutors seek to compel a criminal defendant to decrypt portions of three electronic devices—an iPhone, a laptop, and an external hard drive—through the recollection and use of memorized passwords that investigators believe the defendant knows.

While encryption of personal electronic devices is relatively new, the dilemma faced by law enforcement in this case is an old one: investigators believe additional evidence of a crime exists, but they have thus far been unable to access it. One person, the government believes, has the knowledge necessary to access that additional evidence: the criminal suspect himself. 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). Absent a grant of immunity, that compulsion violates the Fifth Amendment's privilege against self-incrimination.

The magistrate judge's contrary decision—compelling Spencer to recall from memory and then use passwords to his electronic devices—was therefore in error. First, the truthful recollection and use of information like a memorized password is per se testimonial and therefore privileged. *United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010); *see also United States v. Hubbell*, 530 U.S. 27, 41-46 (1990). Second, the magistrate's application of the foregone conclusion doctrine—a doctrine historically applicable only in the context of the production of specific business or financial records—was in error. *See Goldsmith v. Superior Court*, 152 Cal. App. 3d 76 (Cal. 1984). Even assuming the doctrine applies, the government has not made the required showings in this case. *See In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (11th Cir. 2012).

For these reasons, explained in more depth below, the magistrate's order should be reversed.

BACKGROUND

I. ENCRYPTION

Central to the issue before the court are three personal electronic devices that are encrypted, either in whole or in part.

Encryption is the process of transforming plain, understandable information into unreadable letters, numbers, or symbols using a fixed formula or process.[2] Only those who possess the corresponding "key"—in this case, a key derived from a memorized password—can "decrypt" the information and thereby return the message to its original form.[3] Computer-assisted encryption uses sophisticated algorithms to transform readable data into seemingly random information.

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

II. ENCRYPTION'S UBIQUITY

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 alike.

Computer and software manufacturers consider disk encryption 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.[4] Device encryption is also a standard

---

[2] *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).

[3] *Id.*

[4] 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.

feature for the leading smart phone operating systems, Apple iOS and Android.[5]

In addition, government agencies recommend encryption to protect personal data and Internet traffic.[6] Many federal and state laws require or encourage encryption to protect sensitive information.[7] In this increasingly connected world, encryption is a pervasive and integral part of modern life.

III. THE GOVERNMENT'S ABILITY TO BREAK ENCRYPTION

Despite encryption's overall benefit, it is not impenetrable. The federal government has a variety of investigative techniques that allow them to gain lawful access to encrypted information without the compelled assistance of a criminal suspect.

For example, law enforcement may be able to circumvent many forms of encryption by exploiting software or hardware flaws in the encryption software or the device. In one recent, well-publicized example, FBI officials were able to break the encryption on an iPhone used by one of the perpetrators of the San Bernardino terrorist attack.[8] According to recent reports, law enforcement agencies at local, state, and federal levels have contracted with private companies to

---

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

[6] *See, e.g.*, Federal Trade Commission, *Start With Security: A Guide for Business* (Jun. 2015) ("Use strong cryptography to secure confidential material[.]"), 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), https://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf.

[7] *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; Cal. Civil Code § 1798.29(a) (requiring notification in event of data breach for unencrypted information).

[8] *See* Joel Rubin, et al., *FBI unlocks San Bernardino shooter's iPhone and ends legal battle with Apple, for now*, L.A. Times (Mar. 28, 2016), *available at* http://www.latimes.com/local/lanow/la-me-ln-fbi-drops-fight-to-force-apple-to-unlock-san-bernardino-terrorist-iphone-20160328-story.html.

decrypt even the most recent smartphones for as little as fifty dollars each.[9]

The government can also use automated methods to repeatedly guess passwords. In this case, the government represented that one method of cracking passwords, a so-called "brute force attack"—essentially, an automated method of attempting every possible combination of letters and numbers in the password—would require an unacceptably long period of time to complete. *See* Declaration of Christopher Marceau, ¶¶ 15-18. What the government omits, however, is that other methods of cracking passwords—using on-demand computing power combined with more advanced techniques based on commonly used words or phrases, as well as specific information available to law enforcement about the password—could dramatically reduce the time required to crack the password.[10]

Alternatively, investigators may obtain passwords without compelling a suspect to divulge them. For example, law enforcement could obtain a warrant to install a camera to record a suspect's keystrokes as they decrypt a device, thereby obtaining the password. Or they can install hardware or software called a "keylogger" that captures the characters typed using the device, including passwords.[11] Both these methods result in disclosure of the passcode from the suspect, without the government compelling that disclosure.

But, even where encryption proves impenetrable, technology has, on balance, made our lives more transparent than ever before, enabling law-enforcement surveillance on a scale

---

[9] Joseph Cox, *Cops Around the Country Can Now Unlock iPhones, Records Show*, Motherboard (Apr. 12, 2018), https://motherboard.vice.com/en_us/article/vbxxxd/unlock-iphone-ios11-graykey-grayshift-police.

[10] Andy Greenberg, *Hacker Lexicon: What Is Password Hashing?*, Wired (June 8, 2016), https://www.wired.com/2016/06/hacker-lexicon-password-hashing; Dan Goodin, *Why passwords have never been weaker—and crackers have never been stronger*, Ars Technica (Aug. 20, 2012), https://arstechnica.com/information-technology/2012/08/passwords-under-assault.

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

previously unimaginable. We live in a "golden age of surveillance,"[12] and law enforcement regularly takes advantage of the vast amount of sensitive information now available about all of us.

ARGUMENT

I. COMPELLED PASSWORD-BASED DECRYPTION BY THE TARGET OF A CRIMINAL INVESTIGATION IS TESTIMONIAL AND THEREFORE PRIVILEGED BY THE FIFTH AMENDMENT.

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

The privilege distinguishes between compelled "testimony," which is protected, and rote physical acts, which generally are not. *Id.* at 43. "[M]ere physical acts" 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, 210 n.9 (1988) & 219 (Stevens, J., dissenting). Indeed, 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)

---

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

(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 quotations omitted); that (2) relies on or probes the "contents of [a suspect's] own mind." *Id.* at 43 (citing *Curcio*).

A. The compelled recollection and use of a memorized password is testimonial.

The order sought here requires Spencer to truthfully recall from his memory, then use, the passwords to his encrypted devices. That (1) truthful recollection and use of (2) a password stored only in his mind is "testimony." And, so long as it is both compelled (it is) and self-incriminating (the government believes it will be[13]), Spencer's response is privileged by the Fifth Amendment.

Many courts, faced with similar orders, have recognized the testimony inherent in recalling or disclosing a memorized password. *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 v. Huang*, No. 15-cv-269, 2015 WL 5611644, at *3 (E.D. Pa. Sept. 23, 2015) ("Defendants' confidential passwords are personal in nature and Defendants may properly invoke the Fifth Amendment privilege to avoid production of the passwords."); *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.'"); *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012) ("[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."); *see also United States v. Green*, 272 F.3d 748, 753, 749–50 (5th Cir. 2001) (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

[13] Critically, the compelled testimony need not *itself* be incriminating to fall within the privilege. Testimony can still be self-incriminating, 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); *see also United States v. Mitchell*, 76 M.J. 413, 418 (CAAF 2017) (government request for password was interrogation reasonably likely to elicit an incriminating response). Here, the government believes the passwords to the encrypted portions of the devices will serve as *the* link to incriminating information stored on the devices.

communicative" acts)

The government seeks to avoid this straightforward result by describing its proposed compulsion as an act of production—the type of mere physical act that might fall outside the self-incrimination privilege. In *Hubbell*, the Supreme Court recognized, and rejected, that approach. The Court concluded:

> In sum, we have no doubt that the constitutional privilege against self-incrimination protects the target of a grand jury investigation from being compelled to answer questions designed to elicit information about the existence of sources of potentially incriminating evidence. That constitutional privilege has the same application to the testimonial aspect of a response to a subpoena seeking discovery of those sources.

530 U.S. at 43. Stated another way: just as the government may not compel the target of an investigation to verbally answer questions designed to uncover incriminating evidence, it cannot use its power to compel the production of physical evidence as an end-around these constitutional limitations.

The same principle applies here. Just as the government cannot compel Spencer to announce the passwords to the encrypted drives in court or before a grand jury, the government cannot achieve the same end through its power to compel the production of physical evidence. *See Kirschner*, 823 F. Supp. 2d at 669; *Hubbell*, 530 U.S. at 43 (privileged response to subpoena was like "telling an inquisitor the combination to a wall safe").

Nor does the testimonial nature of the recollection and use of a password turn on whether Spencer announces the password to investigators, or whether he types it directly into a computer. *See Doe II*, 487 U.S. at 213 (stating Fifth Amendment is intended to "spare the accused from having to reveal, *directly or indirectly*, his knowledge of facts relating him to the offense") (emphasis added). Instead, "[i]t is the extortion of information from the accused" that triggers the privilege. *Pennsylvania v. Muniz*, 496 U.S. 582, 594 (1990) (internal quotation and citation omitted). Testimony is thus accomplished when the extortion occurs, even if that extortion simply provides a link to additional incriminating evidence. *Doe II*, 487 U.S. at 211 n.10. Again, that is precisely what the government seeks here: extortion of the password from Spencer so that the government can access the encrypted portions of the devices, even if the government disclaims

interest in the passwords themselves. *See In re Grand Jury Subpeona*, 670 F.3d at 1346.

In the final analysis, all the necessary elements of a testimonial communication are present here: the government is compelling Spencer to recall a memorized password from the contents of his mind and to use that password in order to furnish a link to evidence that the government believes will incriminate him. That is a compelled, testimonial communication privileged by the Fifth Amendment.

B. Compelled decryption contains additional testimonial aspects.

The magistrate further erred by failing to recognize the unique testimonial attributes of decryption. By its nature, decryption involves a process of translation and creation; it does not simply unlock or surrender information already in existence. These unique characteristics underscore the testimony inherent in the communication compelled here.

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. *See supra* at 1. 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 translates and transforms existing, scrambled data into a new, readable form.

Thus, when law enforcement compels a suspect to decrypt a device, investigators are not merely seeking the "surrender" of information or evidence already in existence. *Fisher v. United States*, 425 U.S. 391, 411 (1976) (quoting *In re Harris*, 221 U.S. 274, 279 (1911)). To the contrary, investigators are already in possession of all the information they seek: they possess the allegedly incriminatory devices, and they can see and access the data stored on it. They simply cannot *understand* the data in its current form. And, in order to understand it, they seek to compel Spencer to use his unique knowledge to translate the data into an understandable form.

This compelled translation—by a suspect, relying on his truthful recollection and use of a memorized password—is additionally testimonial and privileged by the Fifth Amendment.

C. The values animating the self-incrimination privilege reinforce the testimonial nature of password-based decryption.

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 the right of each individual to a private enclave where he may lead a private life[,]" and "our realization that the privilege, while sometimes a shelter to the guilty, is often a protection of the innocent." *Doe II*, 487 U.S. at 212-13 (*quoting Murphy*, 378 U.S. at 55 (1964)) (internal quotations omitted).

Each element of the "cruel trilemma" is at work in cases of compelled, password-based decryption. 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.[14] The privilege was designed to prevent suspects from facing this "trilemma" in the first instance. *See id.* at 212.

Forced decryption also encroaches on "the right of each individual to a private enclave where he may lead a private life." *Id.* Electronic devices, "[w]ith all they contain and all they may reveal, . . . hold for many Americans 'the privacies of life.'" *Riley v. California*, 134 S. Ct. 2473, 2494-95 (2015) (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)). "Laptop computers, iPads and the like are simultaneously offices and personal diaries. They contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails." *United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013) (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," *Riley*, 134 S. Ct. at 2495—affords some limited measure of security in an otherwise insecure digital world. Conversely, compelled decryption is a blunt instrument, forcing a suspect to potentially expose his most deeply private information for government inspection. *See United States v. Doe* ("*Doe I*"), 465 U.S. 605, 619 (1984) (Marshall, J., and Brennan, J., *concurring*) ("[U]nder the Fifth

[14] The order here highlights the untenable position facing an accused who is required to provide testimony to assist in their own prosecution. 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.

Amendment there are certain documents no person ought to be compelled to produce at the Government's request.")

Properly construed, the self-incrimination 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)). Because the order places Spencer in the "cruel trilemma" and compels him to provide government access to his most private spaces, the order violates two of the privilege's central concerns.

II. THE MAGISTRATE'S DECISION MISAPPLIED THE FOREGONE CONCLUSION DOCTRINE.

The magistrate's decision to apply the foregone conclusion doctrine in the context of an order to recall and use a memorized password was mistaken in two respects. First, for over forty years, and with few exceptions, the foregone conclusion doctrine has been applied only in the context of the production of specific business and financial records. Second, and even assuming the doctrine applies, the applicable standard has not been satisfied in this case.

The doctrine stems from the Supreme Court's decision in *Fisher*, which held that the production of specific, known business records could be compelled, notwithstanding the testimonial aspects associated with the production. 425 U.S. at 413. In the typical case, producing records in response to a subpoena carries "implicit" testimony—about the records' existence, authenticity, and the individual's possession of the records. *Id.* at 410. But, because the government's knowledge of the records in *Fisher* was sufficiently comprehensive, their production was "not [a question] of testimony but surrender." *Id.* at 411 (citations and quotations omitted). The testimony implicit in the production was therefore a "foregone conclusion." *Id.*

The few courts to apply the doctrine in the context of orders to recall and use a memorized password have done so in error. But, even assuming the doctrine can apply in this context, the magistrate erred by failing to follow the standard articulated by the Eleventh Circuit in *In re Subpoena Deuces Tecum*, 670 F.3d 1335, 1346 (11th Cir. 2011).

A. The foregone conclusion doctrine does not apply in the context of compelled, password-based decryption.

In the 42 years since *Fisher* was decided, the foregone conclusion doctrine has been overwhelmingly applied *only* in cases concerning the compelled production of business and other financial records. Absent specific guidance from the Supreme Court or the Court of Appeals, this Court should decline the government's invitation to expand the doctrine's application beyond that narrow scope.

Amicus is unaware of a single court in this circuit to apply the foregone conclusion doctrine beyond the context of the production of specific business or financial records. *See, e.g.*, *In re Grand Jury Subpoena, Dated Apr. 18, 2003*, 383 F.3d 905, 907 (9th Cir. 2004) (subpoena for business records); *United States v. Sideman & Bancroft, LLP*, 704 F.3d 1197, 1200 (9th Cir. 2013) (production of business and tax records); *United States v. Bright*, 596 F.3d 683, 689 (9th Cir. 2010) (credit card records associated with offshore account); *In re Grand Jury Subpoenas Served Feb 27, 1984*, 599 F. Supp. 1006, 1012 (E.D. Wash. 1984) (records related to business partnership).[15]

The doctrine has been confined to business and financial records for good reason. First, records of that type occupy 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 v. United States*, 487 U.S. 99, 104 (1988); *Shapiro v. United States*, 335 U.S. 1, 33 (1948); *but see Curcio*, 354 U.S. at 128 (holding that, even in the context of business records, "forcing the custodian to testify orally as to the whereabouts of nonproduced records requires him to disclose the contents of his own mind" and is therefore privileged).

Second, expanding the doctrine—to embrace the compelled production of any type of physical evidence—would represent a fundamental shift in the power of prosecutors and the scope of the self-incrimination privilege. Indeed, its limits are not clear. Under the government's theory of the doctrine, it could compel a murder suspect to produce a missing murder weapon; a suspected

---

[15] *See also United States v. Taylor*, 2007 WL 805662, *1 (D. Ariz. Mar. 14, 2007) (records related to tax liability); *United States v. Griggs*, 2009 WL 5201847, *1 (D. Ariz. Nov. 25, 2009) (same); *Larue v. United States*, 2015 WL 9809798, *1 (D. Or. Dec. 22, 2015) (foreign bank records).

drug dealer to produce drugs the government knew were stored on his property; or a suspected thief to unlock a safe and produce the stolen goods it contained—so long as the government could sufficiently establish prior knowledge of the "implicit" testimony involved in those acts.

Unsurprisingly, courts have rejected that approach. *See Commonwealth v. Hughes*, 404 N.E. 2d 1239, 1246 (1980) (order to produce gun would require testimonial response); *State v. Dennis*, 16 Wash. App. 417, 423-24 (1976) (act of producing cocaine hidden in freezer was testimonial); *Green*, 272 F.3d 748, 753 (opening safes with combination locks was testimonial); *cf. Baltimore City Dep't of Social Services v. Bouknight*, 493 U.S. 549, 561 (1990) (upholding order to produce child, not under foregone conclusion doctrine, but as part of a regulatory regime unrelated to enforcement of criminal laws).

Here, just as in those cases, the government seeks a criminal suspect's assistance in producing physical evidence—images or videos of child pornography—that it believes exist but that it cannot currently access. Where that type of knowledge gap exists, compelled production is, by definition, *never* a foregone conclusion. Here, for example, Spencer's knowledge of the password is not a foregone conclusion because, if it were, the government "would not need to compel Defendant to produce it because they would already know it." *Baust*, 89 Va. Cir. at *4. *See also Doe I*, 465 U.S. at 614 n. 12.

The court in *Goldsmith v. Superior Court*, 152 Cal. App. 3d 76 (Cal. 1984)—another case reversing an order compelling the production of a weapon allegedly used in a crime—identified the broader problem with orders like the one the government seeks here:

> Implicit in the prosecution's position . . . is the argument that independent evidence establishes defendant's possession of the gun at the time of the offense and after [... , and therefore] the evidence is unworthy of Fifth Amendment protection. . . . The [prosecution's] argument is indeed curious. It is as if we were asked to rule that a confession could be coerced 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.

Goldsmith, 152 Cal. App. 3d at 87 n.12, quoting *Hughes*, 404 N.E. 2d at 1245 (internal quotations and citations omitted).

The magistrate's order adopted just such a "curious" argument, articulating a rule that

allows testimony to be compelled once the government has satisfied an amorphous evidentiary standard. *See* Order at 11 ("The Court holds that if the respondent's knowledge of the relevant encryption passwords is a foregone conclusion, then the Court may compel decryption [i.e., compel recollection and use of the password] under the foregone conclusion doctrine."). That approach represents a serious departure from the traditional conception of the self-incrimination privilege.

"Whatever the scope of this 'foregone conclusion' rationale," *Hubbell*, 530 U.S. at 44, expanding it to apply beyond its typical narrow confines risks a broader erosion of the self-incrimination privilege. The small handful of courts to adopt that approach, at the government's invitation, have done so in error. This Court should decline the government's similar invitation.

B. If the foregone conclusion doctrine applies, the government must demonstrate with reasonable particularity that specific information exists on each of the encrypted devices.

For all the reasons described above, the compelled recollection and use of a memorized password is testimonial and therefore privileged, and the foregone conclusion doctrine should not be applied at all. The Court's analysis need not proceed further.

But, assuming the foregone conclusion doctrine can be invoked in this context, the order below misapplied it: the government does not carry its burden when it demonstrates knowledge of the existence, location, and authenticity of a *device or its password* and the general possibility that files are stored on the devices.[16] Instead, the government must make that showing with respect to the particular information it seeks. *In re Grand Jury Subpoena*, 670 F.3d at 1346; *Huang*, 2015 WL 5611644, *3. It has not done so here.

1. <u>If the foregone conclusion doctrine applies, *In re Grand Jury Subpoena* articulates the correct standard.</u>

As the Eleventh Circuit's decision *In re Grand Jury Subpoena* explains, the government

[16] The magistrate, relying on dicta in a footnote from the *Apple MacPro*, suggested that compelled decryption might be appropriate if the government can establish only that a suspect knows the password to a device. Order at 11 (quoting *United States v. Apple MacPro Computer, et al.*, 851 F.3d 238, 248 n.7 (3rd Cir. 2017)). But, by focusing solely on the password, the magistrate impermissibly shifted 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.

must demonstrate with reasonable particularity that it knows of the specific information on a device before compelling a suspect to decrypt the device.

The court 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 conclusion[s]" because the government "already knew of the materials" sought. *Id.* at 1345-46 (citing *Hubbell*, 530 U.S. at 44-45). That particularity might require knowing "specific file names," 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.

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 the suspect's "possession, control, and access to the encrypted portions of the drives"; and of the suspect's "capability to decrypt the files." *Id.* at 1346. These communicative acts of decryption "would certainly use the contents of his mind." *Id.* at 1349. As explained above, this is true of all password-based decryption (and, as explained above, should end the inquiry, *see supra* at 4-9).

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

[17] Significantly, the Eleventh Circuit rejected the government's assertion that the act of encryption shows the suspect "was trying to hide something." 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.*

Four other federal court decisions are consistent with the Eleventh Circuit's approach. In *Huang*, 2015 WL 5611644, at *2, relying on the Eleventh Circuit opinion, the court denied a motion to compel the defendants to supply passwords to their smartphones because it would "require intrusion into the knowledge of the Defendants" and because the SEC could not establish with "reasonable particularity" that any documents sought resided in the locked phones. In *In re Boucher*, No. 06-91, 2009 WL 424718, *2 (D. Vt. Feb. 19, 2009), the court denied a motion to quash a similar subpoena. There, border agents found, in a traveler's laptop computer, files with titles suggesting child pornography. The traveler stated that he sometimes downloaded child pornography and showed the agents the drive where he downloaded files. In that file, the agents located apparent child pornography. In *United States v. Fricosu*, 841 F. Supp. 2d 1232 (D. Colo. 2012), the court ordered a fraud suspect to decrypt information on a laptop. The police had seized a laptop from the suspect's bedroom with her name on it, and while in custody, she admitted in a recorded phone call that incriminating information was on the laptop. *Id.* at 1235. And in *Apple MacPro*, the Third Circuit applied the Eleventh Circuit's two-part test and found no clear error in a magistrate judge's determination that the foregone conclusion doctrine applied because "[u]nlike *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." *Id.* at 248.[18]

2. <u>If the foregone conclusion doctrine applies, the government has not satisfied its burden here.</u>

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

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

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

As to the second step, the government has not shown with the requisite specificity that all of the information that would be exposed by compelling Mr. Spencer to decrypt the devices (even assuming he is able to do so) is a foregone conclusion. The magistrate's conclusion to the contrary was based on Mr. Spencer's ability to access *other* parts of the seized iPhone and laptop as well as statements by a co-defendant who gave no reliable insight into the actual contents of the devices at issue. *See* Order at 16 ("Petersen did not claim to have seen Spencer open or display any files on the iPhone); *id.* at 17. Nor has the government introduced any evidence about the files it expects to find on the devices, let alone the "specific file names" it seeks. *See In re Grand Jury Subpoena*, 670 F.3d at 1349, n. 28.

This evidence is far less particular than that relied on by the *Boucher*, *Fricosu*, and *Apple MacPro* courts. In each of those cases, 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. *Boucher*, 2009 WL 424718, *2 (agent observed apparent child pornography); *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 & n.27 (distinguishing *Boucher* and *Fricosu*).

Even if the government were to satisfy its burden for *particular files*, and its burden of proving Spencer's ability to decrypt them, such a finding would at most support compelling Spencer to decrypt and provide to the government only those specific files. It would not support an order compelling Spencer to decrypt and produce the entire contents of the hard drives. Such an order is akin to allowing the government to order the production of all records in a file cabinet, simply because the government knows a suspect has a file cabinet.

Here, the government has failed to identify with reasonable particularity even the existence of a single file on the encrypted portion of the devices. At this stage, whatever they contain, if anything, is decidedly not a foregone conclusion.

Dated: April 17, 2018

By: /s/ Mark Rumold

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

Counsel for Amicus Curiae
Electronic Frontier Foundation

CERTIFICATE OF SERVICE

I hereby certify that on this 17th day of April, 2018 I caused copies of the foregoing Brief of Amicus Curiae Electronic Frontier Foundation to be served by electronic means via the Court's CM/ECF system on all counsel registered to receive electronic notices.

/s/ Mark Rumold
Mark Rumold

Counsel for Amicus Curiae
Electronic Frontier Foundation