MISSING THE METAPHOR: COMPULSORY DECRYPTION AND THE FIFTH AMENDMENT

JEFFREY KIOK*

* J.D. Candidate, Boston University School of Law, 2015; B.A., Political Science and History, Tufts University, 2009. Thanks to Professor Tracey Maclin and the *Public Interest Law Journal* editorial staff, particularly Douglas Yang, Lauren Stoia, Mike Killoy, Michael Gregory, Mark Rapisarda, Shauna Harris, and Violeta Haralampieva, for helping produce this article. Questions for the author regarding this article should be sent to jeffrey.kiok@gmail.com.

I. INTRODUCTION

The Government's use of subpoenas or other compulsory processes to require criminal defendants to decrypt encrypted media or otherwise provide passwords to encrypted media violates the Fifth Amendment's protection against self-incrimination, because the act of production is testimonial in nature. However, under the Supreme Court's "foregone conclusion" doctrine, if the Government knows what it is looking for and can independently prove authentication of the evidence, then the Government does not use compulsory testimony from a defendant to prove its case.[1]

Some courts[2] and commentators[3] have analogized decryption to unlocking a safe or opening a door. This incorrectly analyzes the underlying technology in constructing a theoretical framework upon which to analyze the legal issue. Unlike a locked box, which secures a useable document or data inside a container, encryption renders the underlying document or data utterly unintelligible, made legible only through a mathematical decryption process.[4] The analytical problems in using a framework that does not represent how encryption actually functions is compounded by the nature of how encryption software is designed and advertised in a "user-friendly" manner, using metaphors which do not represent how the software works.

This Article will begin by providing a brief background of cryptology in Part I.A, both generally and specifically as it pertains to modern encryption. Part II.A will analyze Supreme Court precedent as it pertains to the testimonial nature of compulsory production, while Part II.B will examine how lower courts have applied those precedents to encryption. Part II.C will analyze the small volume of legal literature on encryption, and Part III will contain the substantive analysis of the framework in which judges and practitioners should view the Fifth Amendment as it pertains to encryption.

---

[1] Fisher v. United States, 425 U.S. 391 (1976).

[2] *See* discussion *infra* Part II.B.

[3] *See* discussion *infra* Part II.C.

[4] *See* discussion *infra* Part I.A (discussing how cryptographic systems work).

A. *Cryptology, a Technical & Historical Overview*

1. What is Cryptology?

"*Cryptology* is the study of secret writing."[5] Secret writing is the transformation of a message into something unintelligible.[6] Secret writing is different from hidden writing, which is the process of hiding the presence of a message (e.g., invisible inks).[7] In cryptology, the original message that can be read by humans is called "plaintext," while the encrypted or unreadable message is called "ciphertext."[8] The transformation of plaintext to ciphertext can be called "encoding," or "enciphering."[9] The system of the transformation to ciphertext is called a "cryptologic system" or "cryptosystem."[10] The reverse—the transformation of ciphertext to plaintext—can be called "decoding" or "decrypting."[11] "Cryptography is the science of secret writing with the goal of hiding the meaning of [the plaintext]," while "cryptanalysis is the science . . . of *breaking* cryptosystems."[12]

Encryption has a long history spanning from hieroglyphics in ancient Egypt to the Continental Army of the United States.[13] Some of the simplest cryptosystems are called "monoalphabetic substitution ciphers," in which one letter is substituted for another.[14] Julius Caesar famously used such a cipher, substituting for any letter of plaintext the letter four letters beyond the plaintext letter.[15] Thus, "A" in plaintext becomes "D" in ciphertext, "B" becomes "E," "C" becomes "F" and so on.[16] The computer era radically changed cryptology, transforming it from a mostly linguistic enterprise to a mathematical and statistical science.[17] While the math of modern encryption is complicated, the fundamentals remain the same: a mathematical cryptosystem takes plaintext and encrypts it into ciphertext.[18] Thus, like with Caesar's cipher or modern encryption, when

---

[5] JOHN F. DOOLEY, A BRIEF HISTORY OF CRYPTOLOGY AND CRYPTOGRAPHIC ALGORITHMS 4 (2013).

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] *Id.*; CHRISTOF PAAR & JAN PELZL, UNDERSTANDING CRYPTOGRAPHY: A TEXTBOOK FOR STUDENTS AND PRACTITIONERS 3 (2010).

[13] *Id.* at 2; DOOLEY, *supra* note 5, at 1–3 (2013).

[14] DOOLEY, *supra* note 5, at 12.

[15] DOOLEY, *supra* note 5, at 11–12.

[16] DOOLEY, *supra* note 5, at 12 (A complete key would look like the following:
Plaintext: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Ciphertext: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C).

[17] DOOLEY, *supra* note 5 at 75.

[18] *See generally* PAAR & PELZL, *supra* note 12, at 2; DOOLEY, *supra* note 5, at 88–117

an encrypted message or data is sent or stored, what is being sent or stored is the ciphertext, not the plaintext.

2. Modern Stored Encryption

Today, most personal computers and Operating Systems (OSs) have built-in encryption capabilities.[19] Additionally, there is free and open-source software available today, such as TrueCrypt, which can provide the same capabilities as encryption built into an OS.[20] Beyond free software, there are also free OSs, such as the Linux Ubuntu OS, which also support full-disk encryption.[21] All these major OSs can provide similar features: full-disk encryption as well as encrypting individual files or folders on a computer.[22] All similarly provide "on-the-fly" encryption, which means that the software encrypts the hard drive such that the user enters the password a single time, and whenever a file or portion of the hard drive is accessed, the encryption software automatically decrypts the file or portion that is being accessed.[23] In on-the-fly encryption, such as Apple's FileVault 2, Windows BitLocker, Ubuntu, or TrueCrypt, the user can encrypt the entire hard drive, including the hard drive on which their

---

(discussing the "Advanced Encryption Standard" (AES), one of the most used cryptographic systems).

[19] *See* APPLE, INC., *OS X: About FileVault 2*, http://support.apple.com/kb/ht4790 (last visited Feb. 21, 2015) (FileVault 1 available on Mac OS 10.3, while FileVault 2 became available on OS 10.7); MICROSOFT, CORP., *BitLocker Drive Encryption*, http://windows.microsoft.com/en-us/windows7/products/features/bitlocker (last visited Feb. 21, 2015) (available for the "Ultimate" and "Enterprise" editions of Windows 7, and "Pro" and "Enterprise editions of Windows 8).

[20] *See* TRUECRYPT FOUNDATION, *TrueCrypt User Guide*, https://www.grc.com/misc/truecrypt/TrueCrypt%20User%20Guide.pdf (last visited Feb. 21, 2015). *See also* SIMON SINGH, THE CODE BOOK: THE EVOLUTION OF SECRECY FROM MARY QUEEN OF SCOTS TO QUANTUM CRYPTOGRAPHY 293–316 (1999) (discussing "Pretty Good Privacy" one of the first free consumer-level encryption programs, which is no longer in wide use but was popular in the 1990's). Note that in May 2014, TrueCrypt strangely and with little explanation closed its door. Alex Harn, *Encryption Software TrueCrypt Closes Doors in Odd Circumstances,* THE GUARDIAN (May 30, 2014), http://www.theguardian.com/technology/2014/may/30/encryption-software-truecrypt-closes-doors; *see* TrueCrypt, http://truecrypt.sourceforge.net/ (last visited Feb. 22, 2014) ("WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues
This page exists only to help migrate existing data encrypted by TrueCrypt.").

[21] *See* ELECTRONIC FRONTIER FOUNDATION, *Privacy in Ubuntu 12.10: Full Disk Encryption*, https://www.eff.org/deeplinks/2012/11/privacy-ubuntu-1210-full-disk-encryption (last visited Feb. 21, 2015). Full disk encryption encrypts an entire hard drive, rather than just a folder or directory of the hard drive.

[22] *See* ELECTRONIC FRONTIER FOUNDATION, *supra* note 21; APPLE, INC., *supra* note 19; MICROSOFT, CORP., *supra* note 19; TRUECRYPT, *supra* note 20.

[23] *See* ELECTRONIC FRONTIER FOUNDATION, *supra* note 21; APPLE, INC., *supra* note 19; MICROSOFT, CORP., *supra* note 19; TRUECRYPT, *supra* note 20.

OS resides, and then simply enter a password when the system boots (turns on).[24] This password permits the OS to decrypt the portion that is being accessed momentarily, and then write new encrypted files to the hard drive.[25] In terms of cryptology, these types of file systems transform the entire hard drive from plaintext to ciphertext, and the password permits the OS to momentarily transform the ciphertext that is being accessed back to plaintext so that the user can access the data.[26]

The nature of on-the-fly encryption is important to understand: all of the encryption and decryption occurs essentially without the user noticing.[27] When the computer is shut down, any plaintext files that were being viewed (in Random Access Memory or RAM)[28] by the user are destroyed and only the ciphertext, or encrypted data, remains.[29] If the user shuts down the computer and starts it up again, the user must enter his or her password again.[30]

Modern encryption has also found its way onto mobile devices, such as cell phones and tablets.[31] For instance, the Apple iPhone running iOS 8 *cannot* be unlocked by Apple without a passcode, which is a change from its previous operating systems.[32] Apple's iPhone held approximately 42.4% of the "smart phone" market share in July 2014.[33] Because Apple is no longer able to bypass

---

[24] *See* ELECTRONIC FRONTIER FOUNDATION, *supra* note 21; APPLE, INC., *supra* note 19; MICROSOFT, CORP., *supra* note 19; TRUECRYPT, *supra* note 20.

[25] *See* ELECTRONIC FRONTIER FOUNDATION, *supra* note 21; APPLE, INC., *supra* note 19; MICROSOFT, CORP., *supra* note 19; TRUECRYPT, *supra* note 20.

[26] *See* ELECTRONIC FRONTIER FOUNDATION, *supra* note 21; APPLE, INC., *supra* note 19; MICROSOFT, CORP., *supra* note 19; TRUECRYPT, *supra* note 20.

[27] *See* ELECTRONIC FRONTIER FOUNDATION, *supra* note 21; APPLE, INC., *supra* note 19; MICROSOFT, CORP., *supra* note 19; TRUECRYPT, *supra* note 20.

[28] Random Access Memory is a type of temporary computer storage "available to the user for programs and data." MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 967 (10th ed. 1993); "RAM is volatile, so its contents are lost when the power fails or is turned off." DICTIONARY.COM, *Define RAM at Dictionary.com* (Feb. 21, 2014, 4:33 PM), http://dictionary.reference.com/browse/ram.

[29] *See* TRUECRYPT, *supra* note 20.

[30] *See* ELECTRONIC FRONTIER FOUNDATION, *supra* note 21; APPLE, INC., *supra* note 19; MICROSOFT, CORP., *supra* note 19; TRUECRYPT, *supra* note 20.

[31] Of note, the Supreme Court held in Riley v. California, 134 S. Ct. 2473 (2014) that police may not search cell phones absent a warrant.

[32] APPLE, INC., *Apple–Privacy–Government Information Requests*, [hereinafter *Apple Privacy*], http://www.apple.com/privacy/government-information-requests/ (last visited Feb. 21, 2015) ("On devices running iOS 8, your personal data such as photos, messages (including attachments), email, contacts, call history, iTunes content, notes, and reminders is placed under the protection of your passcode. Unlike our competitors, Apple cannot bypass your passcode and therefore cannot access this data. So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8.").

[33] COMSCORE, *comScore Reports July 2014 U.S. Smartphone Subscriber Market Share*,

a passcode on the phones, even if served with a lawful process, law enforcement will be forced to bypass the passcode itself.[34]

The language that encryption software companies use can be particularly misleading to legal scholars attempting to analogize the technology to an historical practice, because such language often obfuscates what is actually occurring in the encryption system. For example, TrueCrypt describes its software as creating encrypted "containers."[35] The software creates a virtual "volume" on a hard drive, into which the user can copy files, which will become encrypted with any variety of encryption options and methods.[36] Once created, the volume will appear available to a user using the TrueCrypt software, but will require a password in order to open it.[37] Absent the password, the contents of the volume are inaccessible, and one cannot tell that the volume contains any data at all.[38] When the password is correctly entered, the volume will mount[39] as a virtual drive, and files and folders can be dragged to it or otherwise copied, just like any other removal media (e.g., a hard drive, flash/drive, writable CD-ROM or DVD).[40]

The kind of language people use when talking about computers (e.g., files and folders) and the language that encryption companies often use to describe what their products "do" (e.g., creating encrypted "containers," encrypting a "file" or "folder," or using a "key" to "unlock" encrypted media) can cause people to improperly analogize how encryption software actually works. Thus, although TrueCrypt describes its encrypted virtual volumes as "containers," the analogy to a physical container only goes so far.[41] Looking at a hypothetical, imagine a physical container with a letter in plaintext inside it. The container may have a lock and key on the outside, but the letter inside is always in plaintext, regardless of whether the container is locked or unlocked. A TrueCrypt "container" using on-the-fly encryption is different: the data inside

---

http://www.comscore.com/Insights/Market-Rankings/comScore-Reports-July-2014-US-Smartphone-Subscriber-Market-Share (last visited Feb. 21, 2015).

[34] *See Apple Privacy*, *supra* note 32.

[35] Beginner's Tutorial: How to Create and Use a TrueCrypt Container, *available at* https://www.byui.edu/Documents/financial-services/Thompson_TrueCryptBeginnersTutorial.pdf.

[36] *Id.*

[37] *Id.*

[38] *See infra* note 150 (discussing expert's testimony that "blank space" on an encrypted hard drive "appears as random characters").

[39] Mounting is the process by which a storage device is connected and can be accessed by a computer. LINUX INFORMATION PROJECT, *Mounting Definition by the Linux Information Project*, http://www.linfo.org/mounting.html (last visited Feb. 21, 2015).

[40] Beginner's Tutorial: How to Create and Use a TrueCrypt Container, https://www.byui.edu/Documents/financial-services/Thompson_TrueCryptBeginnersTutorial.pdf (last visited Feb. 21, 2015).

[41] *See id.*

the container is *always* encrypted (ciphertext), both when the contents of the container are accessible (because the user inputted a password) and when they are not accessible.[42] The data inside the container only becomes readable in plaintext when the user both enters the password *and* actually accesses some of the data inside the container.[43] Thus, to return to our analogy, a TrueCrypt container is a locked container inside of which some letters are in ciphertext.[44] When one enters the password (or "key" to the container), one can access the letters inside. When you read one letter, your key transforms that one letter and only that one letter from ciphertext to plaintext, but it does not affect other letters that you are not reading.[45] Similarly, once you stop reading the letter, it immediately becomes ciphertext again.[46] This is the result of the "on-the-fly" encryption that modern encryption software uses.[47] Thus, when one is using encryption software such as TrueCrypt, even after inputting the password, only a tiny percentage of the encrypted hard drive is actually decrypted for use (in memory), because in operating a computer, you do not need to access the majority of the hard drive.[48]

The dangers posed by the analogies and terms popularly used in computer software are not to be underestimated.[49] Although computer users use language like "folders" and "containers," unlike a real folder or container, the contents of an encrypted folder exist *only* in ciphertext, and not plaintext.[50] Thus, if one is presented with an encrypted hard drive, the readable plaintext *does not exist* on

---

[42] *See* TRUECRYPT, *supra* note 20 ("Note that TrueCrypt never saves any decrypted data to a disk . . . .").

[43] *See* LINUX INFORMATION PROJECT, *supra* note 39.

[44] *See* TRUECRYPT, *supra* note 20.

[45] *See* TRUECRYPT, *supra* note 20.

[46] *See* TRUECRYPT, *supra* note 20.

[47] *See* TRUECRYPT, *supra* note 20.

[48] *See* TRUECRYPT, *supra* note 20.

[49] Although beyond the scope of this paper, complex computer interfaces present peculiar challenges to lawyers attempting to analogize new technology to older technology. Should courts analyze new technology on how it *purports* to function to the end-user or how it *actually* works? This has significant implications in areas of the laws where what a defendant knows or believes about something plays a part in the legal analysis, such as the Fourth Amendment. *See* Katz v. United States, 389 U.S. 347 (1967) (Harlan, J., concurring) ("first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"). Would society deem reasonable a person's expectation that technology works as it "pretends" or *purports* to work, or would it only deem reasonable a reliance on how the technology *actually* works? *See also* Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?"* 33 CONN. L. REV. 503, 506 (2001) (noting that it is a "conceptual error" to use a "'lock' and 'key' analogy" in arguing that "encryption triggers Fourth Amendment protection").

[50] *See* TRUECRYPT, *supra* note 20.

the hard drive; only ciphertext exists.[51]

II. THE FIFTH AMENDMENT AS IT PERTAINS TO TESTIMONIAL ACTS

A. *The Supreme Court on Testimonial Acts*

The Fifth Amendment of the Constitution provides that "No person . . . shall be compelled in any criminal case to be a witness against himself . . . ."[52] Although "the public has a right to every man's evidence,"[53] the Fifth Amendment's privilege against self-incrimination ("the privilege") is the "most important"[54] exemption to that duty. The privilege extends not only to answers that support a conviction under a criminal statute, but "likewise embraces [answers] which would furnish a link in the chain of evidence needed to prosecute the claimant for a . . . crime."[55]

However, a court (or other administrative agency or House of Congress) can grant a witness immunity from criminal prosecution in exchange for compelling potentially incriminating testimony.[56] When evaluating a statute that permits a court to grant immunity under the Fifth Amendment, a court must determine "whether the immunity granted under [the] statute is coextensive with the scope of the privilege."[57] The Supreme Court has held that so-called use and derivative use immunity statutes grant immunity coextensive with the Fifth Amendment's privilege against self-crimination.[58]

Absolute immunity is broader than use and derivative use immunity. Specifically, absolute immunity or transactional immunity is a privilege insofar as "one who invokes it cannot subsequently be prosecuted," and thus is a "broader

---

[51] *See* TRUECRYPT, *supra* note 20.

[52] U.S. CONST. amend. V.

[53] Kastigar v. United States, 406 U.S. 441, 443 (1972).

[54] *Id.* at 444.

[55] Hoffman v. United States, 341 U.S. 479, 486 (1951) (reversing conviction where defendant refused to answer questions which by themselves did not implicate him in any federal crimes, but which were designed to establish a connection between the defendant and a fugitive witness).

[56] *See* 18 U.S.C. § 6002 (2006).

[57] *Kastigar*, 406 U.S. at 449. *See* Counselman v. Hitchcock, 142 U.S. 547, 585–86 (1892) (striking down an immunity statute because it did not "supply a complete protection from all the perils against which the constitutional prohibition was designed to guard, and is not a full substitute for that prohibition"). *See also Kastigar*, 406 U.S. at 451-52 (noting that an immunity statute may, but is not constitutionally required to, offer "absolute immunity against future prosecution").

[58] *Kastigar*, 406 U.S. at 453 ("Immunity from the use of compelled testimony, as well as evidence derived directly and indirectly therefrom, affords this protection."). *See* United States v. Hubbell, 530 U.S. 27, 38–39 (2000) (noting that *Kastigar* rejected the notion that "nothing less than full transactional immunity from prosecution for any offense to which compelled testimony relates could suffice" for Fifth Amendment purposes).

protection" than the privilege against self-incrimination.[59] The Supreme Court has held that the grant of immunity should leave a witness "in substantially the same position as if the witness had claimed his privilege in the absence of a . . . grant of immunity."[60] There are no Supreme Court cases directly dealing with encryption at all, or the testimonial nature of the privilege against self-incrimination as it pertains to encrypted or coded documents.

1. *Fisher v. United States*

In 1976, in *Fisher v. United States*, the Supreme Court explored the question of what kinds of acts of production are testimonial.[61] *Fisher* consolidated two cases with similar fact patterns. In both cases the Internal Revenue Service ("IRS") served summons on lawyers Kasmir and Fisher, directing them each to produce documents obtained by their clients from their clients' accountants relating to tax returns.[62] Both attorneys raised various defenses, including the Fifth Amendment's privilege against self-incrimination.[63] The District Court in each case enforced the summons. On appeal the Third Circuit, en banc, affirmed, while the Fifth Circuit reversed.[64] The Supreme Court began its analysis by noting that legal process against a taxpayer's lawyer is not compulsion against the taxpayer himself.[65] Further, even if the taxpayers authored the documents themselves, the Fifth Amendment would not apply because the documents were created voluntarily and the Government had not compelled their creation.[66]

After noting that the documents were not created by compulsion, the Court reached the testimonial nature of the act of production itself. The Court found that "[t]he act of producing evidence in response to a subpoena . . . has communicative aspects of its own, wholly aside from the contents of the papers produced."[67] The Court noted that "[c]ompliance with the subpoena tacitly concedes" that the subpoenaed documents are in fact what had been demanded in the subpoena.[68] However, the Court did not hold that the tax documents were privileged because the testimonial information was a "foregone conclusion."[69] The Court stated that the Government "is in no way relying on the 'truth-tell-

---

[59] *Kastigar*, 406 U.S. at 453.

[60] *Id.* at 457 (quoting Murphy v. Waterfront Comm'n, 378 U.S. 52, 79 (1964)).

[61] Fisher v. United States, 425 U.S. 391 (1976).

[62] *Id.* at 394.

[63] *Id.* at 395 (noting defenses were raised based on accountant-client privilege, attorney-client privilege, the Fourth Amendment, and the Fifth Amendment).

[64] *Id.*

[65] *Id.* at 397 ("[E]nforcement against a taxpayer's lawyer would not 'compel' the taxpayer to do anything and certainly would not compel him to be a 'witness' against himself.").

[66] *Id.* at 410 n.11.

[67] *Id.* at 410.

[68] *Id.*

[69] *Id.* at 411.

ing' of the taxpayer to prove the existence of or his access to the documents."[70] The production of the documents did not authenticate the documents, because they had been produced by accountants and not the taxpayers being investigated themselves.[71] Although not central to the holding, the Court acknowledged the "'implicit authentication' rationale," whereby a subpoena to a target compels the target to assert the genuineness of the documents produced.[72]

The "foregone conclusion"[73] doctrine first articulated in *Fisher* is central to understanding subsequent applications of *Fisher* and its progeny to cases involving encryption. The Court explains that because the Government was using the subpoena in *Fisher* not "to prove the existence of or access to the documents"[74] but for "surrender,"[75] there is no new information learned that is sufficiently testimonial so as to implicate the Fifth Amendment.

2. *United States v. Doe* ("*Doe I*")

In addition to subpoenaing witnesses to testify before a grand jury or a trial court, the Government can serve a witness with a subpoena *duces tecum*[76] to provide documents to a Grand Jury. A subpoena may compel a witness "to perform an act that may have testimonial aspects and an incriminating effect."[77] In *United States v. Doe* ("*Doe I*"), the Government subpoenaed nearly all of Doe's business documents.[78] The Court noted that "[c]ompliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the [witness] . . . [and the] belief that the papers are those described in the subpoena."[79] The Court also noted that the act of production would relieve the Government of its burden of authentication under the Federal Rules of Evidence, because otherwise the Government would need to authenticate the documents if it obtained them from another source.[80]

3. *Doe v. United States* ("*Doe II*")

After *Doe I*, the Supreme Court heard *Doe v. United States* ("*Doe II*"), an-

---

[70] *Id.*

[71] *Id.*

[72] *Id.* at 413 n.12.

[73] *Id.* at 411.

[74] *Id.*

[75] *Id.* (quoting *In re* Harris, 221 U.S. 274, 279 (1911)).

[76] BLACK'S LAW DICTIONARY 1654 (10th ed. 2014) ("A subpoena ordering the witness to appear in court and to bring specified documents, records, or things.").

[77] United States v. Doe, 465 U.S. 605, 612 (1984) [hereinafter *Doe I*]. Samuel A. Alito, Jr. argued *Doe I* on behalf of the Government, working in the Solicitor General's Office, perhaps serving as the impetus for Alito to write on the topic. *See* Samuel A. Alito, Jr., *Documents and the Privilege Against Self-Incrimination*, 48 U. PITT. L. REV. 27 (1986–87).

[78] *Doe I*, 465 U.S. at 606–07.

[79] *Id.* at 612 (quoting *Fisher*, 425 U.S. at 410).

[80] *Id.* at 614 n.13.

other case implicating the testimonial effect of a compulsory process, specifically an "order compelling a target of a grand jury investigation to authorize foreign banks to disclose records of his accounts."[81] The grand jury target argued that requiring him to sign a consent form for the grand jury permitted the Government to obtain "potentially incriminating account records that would otherwise be unavailable to the grand jury."[82] The Court rejected that argument and held that "an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information."[83] The Court analogized the consent form to a "key to a strongbox" rather than "[t]he expression of the contents of an individual's mind," which would be protected.[84] The Court analogized that it had held as non-testimonial the furnishing of a blood-sample,[85] providing a handwriting exemplar,[86] a voice exemplar,[87] standing in a line-up,[88] and wearing particular clothing.[89]

The Court characterized the consent form that the target was compelled to sign as a "nonfactual statement that facilitates the production of evidence by someone else."[90] The Court was careful to note, however, that "[t]here are very few instances in which a verbal statement, either oral or written, will not convey information or assert facts."[91] In denying the target's assertion of Fifth Amendment privileges, the Court's decision was bound to its facts, noting that

---

[81] Doe v. United States, 487 U.S. 201, 202 (1988) [hereinafter *Doe II*]. Because the banks at issue were foreign banks of the Cayman Islands and Bermuda, the District Court had no means to compel them to produce documents. Moreover, Cayman Islands and Bermuda law at the time prohibited banks from disclosing any documents absent the consent of an accountholder.

[82] *Id.* at 208.

[83] *Id.* at 210.

[84] *Id.* at 210 n.9. *See* Couch v. United States, 409 U.S. 322, 328 (1973) ("It is extortion of information from the accused himself that offends our sense of justice."); United States v. Wade, 388 U.S. 218, 222 (1967) (the privilege prohibits compulsion "to disclose any knowledge he might have" or "to speak his guilt").

[85] Schmerber v. California, 384 U.S. 757, 765 (1966) ("Petitioner's testimonial capacities were in no way implicated" in furnishing a blood sample).

[86] Gilbert v. California, 388 U.S. 262, 266–67 (1967) ("A mere handwriting exemplar . . . is an identifying physical characteristic . . . .").

[87] United States v. Dionisio, 410 U.S. 1, 7 (1973) ("The voice recordings were to be used solely to measure the physical properties of the witnesses' voices, not for the testimonial or communicative content of what was to be said.").

[88] United States v. Wade, 388 U.S. 218, 222 (1967) ("It is compulsion of the accused to exhibit his physical characteristics, not compulsion to disclose any knowledge he might have.").

[89] Holt v. United States, 218 U.S. 245, 252–53 (1910) ("But the prohibition . . . is a prohibition of the use of physical or moral compulsion to extort communications from him, not an exclusion of his body as evidence . . . .").

[90] *Doe II*, 487 U.S. 201, 213 n.11 (1988).

[91] *Id.* at 213.

a form is not "testimonial."[92] The form also did not "admit the authenticity of any records produced by the bank,"[93] which *Doe I* found problematic.[94] The form similarly did not indicate that the target had consented to the production of records, but merely that the form "shall be construed as consent with respect to Cayman Islands and Bermuda bank-secrecy laws."[95] The Court firmly rejected the notion that "the performance of every compelled act carries with it an implied assertion that the act has been performed by the person who was compelled and therefore . . . [is] subject to the privilege,"[96] noting such acts are not "'sufficiently testimonial for purposes of the privilege.'"[97]

4. *United States v. Hubbell*

Never at issue in *Fisher*, *Doe I*, or *Doe II* was the testimonial nature of a Government subpoena to a defendant when the Government's subpoena requires the witness to assemble responses to subpoena that were broadly worded. In *United States v. Hubbell*, a case that arose out of the Whitewater Investigation, the Court reiterated that "'the act of production' itself may implicitly communicate 'statements of fact.'"[98] Moreover, the Court noted once again that production may compel the witness to "admit that the papers existed, were in his possession or control, and were authentic."[99] The Court also noted that the defendant in *Hubbell* was required to answer questions in the Grand Jury about the scope of his compliance with the subpoena.[100] In discussing the Government's subpoena, which had required the defendant to provide voluminous responses to broad requests, the Court stated that "[t]he assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox."[101] The Court rejected the "Government's anemic view" that "the act of production [w]as a mere physical act that [wa]s principally nontestimonial . . . and [could] be entirely divorced from its 'implicit' testimonial aspect so as to constitute a 'legitimate, wholly independent source' (as required by *Kastigar*) for the documents produced sim-

---

[92] *Id.* at 215. ("[T]he form does not acknowledge that an account in a foreign financial institution is in existence or that it is controlled by petitioner. Nor does the form indicate whether documents or any other information relating to petitioner are present at the foreign bank, assuming that such an account does exist . . . [t]he form does not even identify the relevant bank.").

[93] *Id.* at 216 (noting the bank would have to provide authentication of evidence).

[94] *Doe I*, 465 U.S. 605, 614 n.13 (1984).

[95] *Doe II*, 487 U.S. at 216.

[96] *Id.* at 217 n.15.

[97] *Id.* (quoting Fisher v. United States, 425 U.S. 391, 411 (1976)).

[98] *Hubbell*, 530 U.S. at 36.

[99] *Id.* (quoting *Doe I*, 465 U.S. 605, 613 n.11 (1984)).

[100] *Id.* at 37 n.20.

[101] *Id.* at 43 (citing *Doe II*, 487 U.S. 201, 210 n.9 (1988)).

ply fail[ed] to account for those realities."[102]

B. *The Fifth Amendment as Applied by Lower Courts to Encryption*

A number of lower courts have applied the Fifth Amendment's privilege against self-incrimination to the act of compulsory decryption or to compelling a grand jury target or defendant to turn over a password.[103] As the cases below will demonstrate, lower courts have had difficulties with the issue, often reconsidering and overturning their own prior orders when faced with changing facts, or facts that were not well-understood in the first place.

1. *United States v. Burr (In re Willie)*

Arguably the earliest encryption case in American jurisprudence was decided in 1807 by Chief Justice John Marshall (sitting as Circuit Justice) as part of the treason trial of Aaron Burr.[104] In *United States v. Burr*, Burr's secretary, Mr. Willie,[105] was subpoenaed to answer questions about a letter that was written in cipher.[106] The letter, addressed to a Dr. Bollman, was alleged to be from Burr, written under a fictitious name.[107] When asked if he copied the paper or if the letter had been written by Burr, Willie refused to answer.[108] Willie claimed that answering would cause him to incriminate himself; if he admitted to copying the letter, and the letter turned out to contain evidence of treason, then his admission to copying would also serve to incriminate him for misprision of treason.[109] Chief Justice Marshall eventually held that "no witness is compellable to furnish any one [of the many links that compose that chain of testimony which is necessary for conviction] against himself."[110] Nevertheless, the Chief Justice permitted a narrower question to be asked: Whether the witness had "present knowledge of the cipher . . . because his present knowledge would not, it is believed, in a criminal prosecution, justify the inference that his knowledge was acquired previous to this trial, or afford the means of proving that fact."[111] The implication was that past knowledge of the cipher and the letter would tend to incriminate the witness and thus would be protected by the privilege.[112]

---

[102] *Id.; see* Kastigar v. United States, 406 U.S. 441, 449, 453 (1972).

[103] *See, e.g., infra*, Part B.1–8.

[104] United States v. Burr (*In re* Willie), 25 F.Cas. 38 (Marshall, Circuit Justice, C.C. Va. 1807).

[105] The opinion gives "Mr. Willie" and no other name.

[106] *Burr*, 25 F.Cas. at 38.

[107] *Id.*

[108] *Id.*

[109] *Id.* at 38–39. *See* Act of Apr. 30, 1790, 1 Cong. Ch. 9, 1 Stat. 112 (1790); United States v. Wiltberger, 18 U.S. 76, 78 (1820) (holding misprision of treason was the concealment of treason).

[110] *Burr*, 25 F.Cas. at 40.

[111] *Id.*

[112] *Id.* For a discussion of the historical context of the case, *see* R. KENT NEWMYER, THE

2. *United States v. Pearson*

Two hundred years after *Burr*, in *United States v. Pearson*, the Northern District of New York heard the first case regarding use of compulsory process to decrypt encrypted media.[113] The defendant, Abraham Pearson, was charged with a variety of crimes related to child pornography.[114] Under the apparent belief that Pearson had reacquired child pornography content post-indictment, the Government applied for, received, and executed a search warrant of Pearson's home, which he shared with his father,[115] and recovered two computers, an external hard drive, a thumb drive, and more than one hundred "disks" (the order does not indicate what type of disks these were).[116] The Government issued a trial subpoena demanding "any and all passwords, keys, and/log-ins used to encrypt any and all files" on the seized hard drives and other electronic media.[117] The defendant moved to quash the trial subpoena.[118]

The District Court applied a two-part test to determine if the act of production "require[d] incriminating testimony."[119] The District Court asked (1) whether the Government knew "the existence and location of the subpoenaed documents," and (2) whether "production would implicitly authenticate the documents."[120] The District Court concluded that because the Government already possessed the encrypted files and knew that they were encrypted, the Government met the first prong of the test.[121] However, the District Court

---

TREASON TRIAL OF AARON BURR: LAW, POLITICS, AND THE CHARACTER WARS OF THE NEW NATION 33, 100 (2012); AARON BURR, POLITICAL CORRESPONDENCE AND PUBLIC PAPERS OF AARON vol. 2:973-90 (Mary-Jo Kline ed., 1983) (recounting the exact history of the ciphered letter, its alteration, its dubious attribution to Aaron Burr, and reprinting a copy of the plaintext version).

[113] United States v. Pearson, No. 1:04-CR-340, 2006 U.S. Dist. LEXIS 32982 (N.D.N.Y. May 24, 2006) *aff'd*, 570 F.3d 480 (2d Cir. 2009). The Second Circuit did not hear an appeal regarding the encryption issue. A May 24, 2006 Memorandum Decision and Order reserved a ruling on Pearson's motion to quash the subpoena, but subsequently denied the motion orally. *See* Court Docket Minute Entry at 18, United States v. Pearson, No. 1:04-CR-340, 2006 U.S. Dist. LEXIS 32982 (N.D.N.Y. June 5, 2006) (Bloomberg Law).

[114] *Pearson*, 2006 U.S. Dist. LEXIS 32982, at *5–6.

[115] Although unrelated to the Fifth Amendment issue of encryption, Abraham Pearson's father, Elijah Pearson, subsequently asserted he was representing his son (though he had made no appearance to the District Court), and asserted that the search violated an attorney-client privilege. *See id.* at *14–15.

[116] *Id.* at *9.

[117] *Id.* at *51–52.

[118] *Id.* at *52.

[119] *Id.* at *57 (citing *In re* Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d 87, 93 (1992)). The test was an application of the foregone conclusion doctrine. *See supra* Part II.A.1.

[120] *Id.* (citing *In re* Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d 87, 93 (1992)).

[121] *Id.* at *58.

found that the Government had not satisfied the second prong because it could not "authenticate the files by evidence *other* than the production of the password."[122] Since Pearson asserted that some of the encrypted files were prepared by his father and attorney Elijah Pearson, if the Government compelled the password from Pearson, the production "would provide a link in the chain of ownership and control of any incriminating encrypted files."[123] Despite this finding, the District Court denied Pearson's motion during an evidentiary hearing.[124]

3. In re *Boucher I* and *II*

In In re *Boucher* (*Boucher I*),[125] the Government stopped defendant Boucher at a border checkpoint and searched his laptop computer, finding thousands of images of child pornography.[126] After waiving his *Miranda* rights, Boucher admitted that he downloaded pornographic files to a desktop computer at home and transferred those files to his laptop, unknowingly downloading child pornography in the process.[127] An officer asked Boucher to show him where the pornographic files were located.[128] Boucher showed the officer files on "drive Z" whereupon the officer searched drive Z, and found more images of apparent child pornography.[129] After seizing Boucher's laptop, the laptop was shut down.[130] However, upon shutting down the computer, the officers inadvertently engaged the laptop's encryption software, called "Pretty Good Privacy."[131] As a result, law enforcement was unable to access the computer's files before trial. When the Government subpoenaed Boucher, Boucher moved to quash the subpoena, asserting his Fifth Amendment right.[132] The magistrate judge denied the Government's motion, holding that by entering his password, Boucher "would be disclosing the fact that he knows the password and has control over the files

---

[122] *Id.* at *62.

[123] *Id.* at *61.

[124] Unfortunately, there is no record of why the District Court ultimately denied Pearson's motion. *See* Minute Entry, United States v. Pearson, *supra* note 113, at 19. The transcript of the evidentiary record remains sealed. Sealed Document at 19, United States v. Pearson, No. 1:04-cr-00340 (N.D.N.Y. June 5, 2006), ECF No. 126. Presumably, the Government must have been able to demonstrate that it was able to independently authenticate and link the encrypted files to Pearson.

[125] *In re* Boucher, 2007 WL 4246473 (D. Vt. Nov 29, 2007) [hereinafter *Boucher I*].

[126] *Id.* at *1.

[127] *Id.*

[128] *Id.* at *1–2.

[129] *Id.* at *2.

[130] *Id.*

[131] *Id.*; *see generally* OPEN PGP ALLIANCE, http://www.openpgp.org/about_openpgp/history.shtml (last visited Feb. 21, 2015).

[132] *Boucher I*, 2007 WL 4246473, at *3.

on drive Z."[133]

The Government appealed the magistrate judge's decision.[134] In *Boucher II*, the District Court held that Boucher did not have any act of production privilege under the foregone conclusion doctrine because the law enforcement agents had already viewed the child pornography on drive Z.[135] Thus, Boucher's act of production was not needed to authenticate the evidence because Boucher previously had admitted to law enforcement agents that he had possession of the computer.[136] Because the Government had viewed the material and knew it was there, the Government could independently authenticate the evidence without the need for the subpoena.[137]

4. *United States v. Kirschner*

Thomas Kirschner was indicted for three counts of receipt of child pornography in December 2009.[138] Post-indictment, the Government served a subpoena to find additional evidence of new crimes, ordering Kirschner "to provide all passwords used or associated with the . . . computer . . . and any files."[139] Kirschner asserted, among other things, that the subpoena violated his Fifth Amendment right against self-incrimination.[140]

The District Court issued a brief order granting Kirschner's motion to quash the subpoena on the Fifth Amendment grounds.[141] Examining *Hubbell*, the District Court concluded that "forcing the Defendant to reveal the password for the computer communicates that factual assertion to the government, and thus, is testimonial . . . ."[142] The District Court noted that even if the Government provided Kirschner with act-of-production immunity as to the password, that would "not suffice to protect Defendant's invocation of his Fifth Amendment privilege," because the password is not merely "producing specific documents—it is about producing specific testimony asserting a fact."[143]

5. In re *Grand Jury Subpoena (Bumgardner)*

In 2012, the Eleventh Circuit Court of Appeals decided whether a subpoena ordering a grand jury target to decrypt and produce the contents of encrypted hard drives violated the Fifth Amendment.[144] Ultimately, the Eleventh Circuit

---

[133] *Id.*

[134] *In re* Boucher, 2009 WL 424718 (D. Vt. Feb. 19, 2009) [hereinafter *Boucher II*].

[135] *Id.* at *5–6. *See supra* Part II.A.1.

[136] *Id.*

[137] *Id.* at *4.

[138] United States v. Kirschner, 823 F. Supp. 2d 665, 666 (E.D. Mich. 2010).

[139] *Id.*

[140] *Id.* at 666–68.

[141] Id. at 669.

[142] *Id.*; *see supra* Part II.A.4.

[143] Kirschner, 823 F. Supp. 2d at 669.

[144] *In re* Grand Jury Subpoena Dated Mar. 25, 2011, 670 F.3d 1335, 1337 n.1 (11th Cir.

held that the "decryption and production of the hard drives' contents would trigger Fifth Amendment protection because it would be testimonial, and that such protection would extend to the Government's use of the drives' contents."[145]

Upon request by the U.S. Attorney, the District Court granted act of production immunity but not derivative use immunity.[146] Bumgardner asserted his privilege against self-incrimination because he was not granted derivative use immunity, and the District Court for the Northern District of Florida held him in civil contempt.[147] The Government had subpoenaed the "'unencrypted contents' of the digital media, and 'any and all containers or folders thereon.'"[148] Bumgardner argued that by decrypting the hard drives, "he would be testifying that he, as opposed to some other person, placed the contents on the hard drive, encrypted the contents, and could retrieve and examine them whenever he wished."[149] Importantly, the Eleventh Circuit noted that at the District Court, the Government was unable to prove that there was any data on the encrypted drives.[150] The Eleventh Circuit saw that the crux of the dispute was not whether the encrypted media was testimonial, but whether the act of production, or decryption, would be testimonial.[151]

The Eleventh Circuit analyzed *Fisher* and *Hubbell*,[152] and adopted the reasoning of the Ninth and D.C. Circuits that "[w]here the location, existence, and authenticity of the purported evidence is known with reasonable particularity," the foregone conclusion doctrine applies.[153] The Eleventh Circuit explained that the production of evidence is testimonial "when that act conveys some explicit or implicit statement of fact that certain materials exist, are in the subpoenaed individual's possession or control, or are authentic."[154] Reiterating the Supreme Court's statements in *Curcio v. United States*,[155] the Eleventh Circuit held that

---

2012) [hereinafter *Bumgardner*]. Notably, Matthew Bumgardner was "Doe" in the 11th Circuit case. Amended Complaint at 5, Bumgardner v. United States, No. 11-cv-00338 (N.D. Fla. Aug. 24, 2011). "Doe" had been released from custody immediately after oral argument. *Bumgardner*, 670 F.3d at 1341 n.12.

[145] *Bumgardner*, 670 F.3d at 1341.

[146] *Id.* at 1338.

[147] *Id.*

[148] *Id.* at 1339.

[149] *Id.* at 1339–40.

[150] *Id.* at 1340 n.11 (noting "blank space appears as random characters" (i.e., like all other encrypted data) when encrypted data is forensically examined).

[151] *Id.* at 1342.

[152] *Id.* at 1342–45. *See supra* Parts II.A.1, 4.

[153] *Bumgardner*, 670 F.3d at 1344 n.20.

[154] *Id.* at 1345.

[155] Curcio v. United States, 354 U.S. 118, 128 (1957) (reversing conviction of contempt when union leader refused to disclose location of the union's books and records the Court held "forcing the custodian to testify orally as to the whereabouts of nonproduced records

the "touchstone" of the process to determine whether an act of production is testimonial is "whether the government compels the individual to use 'the contents of his own mind' to explicitly or implicitly communicate some statement of fact."[156]

The Eleventh Circuit held that the decryption and production of the encrypted media was a testimonial act, because it used the contents of the target's mind, and was not a mere physical transfer.[157] Further, the Government did not have a foregone conclusion as to what files, if any, existed on the encrypted media.[158] "We are unpersuaded," the Eleventh Circuit wrote, "by the Government's . . . key/analogy in arguing that . . . [the decryption was] nothing more than a physical, nontestimonial transfer."[159] In concluding that there was not a valid foregone conclusion argument, the Eleventh Circuit engaged in a fact-intensive examination of the forensic testimony, recognizing that the fact that digital media is encrypted does not itself indicate that the media contains data.[160] The Eleventh Circuit specifically pointed to *Boucher*, noting that the case did not turn on the Government knowing "what was contained [in the files, but rather that] it was crucial that the Government knew that there existed a file" in the first place.[161] Unlike *Boucher*, the Government in *Bumgardner* did not know whether or not the files it sought existed on the encrypted media.[162] In reversing the civil contempt charge, the Eleventh Circuit concluded that Bumgardner's invocation of his privilege against self-incrimination was proper in light of an immunity offer that would not sufficiently protect him from future prosecution.[163]

6. *United States v. Fricosu*

Ramona Fricosu, and her ex-husband, Scott Whatcott, were indicted on several counts of bank fraud, wire fraud, money laundering, and making false statements.[164] During a search pursuant to a warrant for Fricosu's home, agents

---

requires him to disclose the contents of his own mind. He might be compelled to convict himself out of his own mouth.").

[156] *Bumgardner*, 670 F.3d at 1345 (quoting *Curcio*, 354 U.S. at 128).

[157] *Id.* at 1349.

[158] *Id.* at 1346.

[159] *Id.*

[160] *Id.* at 1347 (analogizing encrypted media to a vault that is "capable of storing mountains of incriminating documents, that alone does not mean that it contains incriminating documents, or anything at all"). *See also id.* at 1349 n.27 (rejecting the analogy to *Fricosu* because there the Government had independent corroborating evidence that the material it sought was contained on the media).

[161] *Bumgardner*, 670 F.3d at 1348–49 (citing *Boucher II*, 2009 WL 424718, at *3).

[162] *Id.* at 1349.

[163] *Id.* at 1350–53.

[164] Indictment, United States v. Whatcott, No. 10-cr-00509 (D. Colo. Sept. 30, 2010).

recovered six computers, one of which was encrypted with "PGP Desktop."[165] Importantly, when agents started the encrypted machine, they were able to view an encryption screen, which identified the computer as "RS.WORKGROUP.Ramona."[166] The day after the search, Whatcott called Fricosu from a state prison where he was being held on state charges.[167] During their conversation, Fricosu indicated that FBI Agents would be seeking evidence on her laptop, but that they should be thwarted by her passwords, which her lawyer had indicated she was not obligated to give to the FBI.[168] Subsequent to this recorded conversation, the Government sought a warrant to search the laptop and a writ pursuant to the All Writs Act[169] to compel Fricosu to "produce the unencrypted contents of the computer."[170] Fricosu resisted the subpoena.[171]

The District Court looked to *Boucher I* and *Boucher II*, as well as *Fisher*, *Doe I*, *Doe II*, and *Hubbell*[172] Based on the foregone conclusion doctrine, the District Court concluded that the Government "knows of the existence and location of the computer's files," and then found by a preponderance of the evidence that the laptop belonged to Fricosu, or at least that she "was its sole or primary user."[173] Although unstated, in order to reach the foregone conclusion doctrine, the court necessarily must have concluded that the act of production was testimonial: If the court had concluded that the act of production was not testimonial, then it would not have been able to reach the foregone conclusion analysis.[174]

7. In re *The Decryption of a Seized Data Storage System (Feldman)*

In *Feldman*,the Government again attempted to compel a criminal defendant to "provid[e] federal law enforcement agents [with] a decrypted version of the contents of his [lawfully seized] encrypted data storage system."[175] Agents had

---

[165] United States v. Fricosu, 841 F. Supp. 2d 1232, 1234 (D. Colo. 2012). Note that "PGP Desktop" is a variant of "Pretty Good Privacy." *See* OPEN PGP ALLIANCE, *supra* note 131. *See also* SINGH, *supra* note 20.

[166] *Fricosu*, 841 F. Supp. 2d at 1234.

[167] *Id.* at 1235.

[168] *Id.*

[169] 28 U.S.C. § 1651 (2006).

[170] *Fricosu*, 841 F. Supp. 2d at 1235.

[171] *Id.*

[172] *Id.* at 1236–37; *see supra* Parts II.A.1–4, II.B.3.

[173] *Fricosu*, 841 F. Supp. 2d at 1237 (noting the evidence was "uncontroverted" since Fricosu acknowledged in the recorded phone conversation that she owned or had the laptop, the contents of which required her password, and the laptop was found in her bedroom and identified with her name).

[174] *See supra* Part II.A.1.

[175] *In re* The Decryption of a Seized Data Storage System, 2013 BL 116993, at *1 (No. 2:13-mj-00449) (E.D. Wis. Apr. 19, 2013) [hereinafter *Feldman I*].

seized sixteen devices, five of which had no data, two of which were not decrypted, and nine that were encrypted.[176] The agents found evidence that someone received, stored, or distributed child pornography via the file-sharing program "e-Mule."[177] Upon examination of the unencrypted computers, forensic examiners determined that some of the child pornography files had been downloaded to devices corresponding to the encrypted hard drives.[178]

The magistrate judge began by looking to *Fisher* and *Hubbell*, and then analyzed various cases, including *Bumgardner*, before holding that the Seventh Circuit would agree with the Eleventh Circuit that the compulsory decryption would be a testimonial act.[179] Despite noting that this case was distinguishable from *Bumgardner* because the "government has shown that the encrypted devices contain data,"[180] the Government, "unlike in *Boucher* and *Fricosu*," has not proven "access and control."[181] Thus, noting it was a "close call," the magistrate judge concluded that the Government did not know with "reasonable particularity [. . .] that Feldman *ha[d] personal access to and control over* the encrypted storage devices."[182]

As an apt demonstration of the fact-bound nature of these kinds of inquiries, the District Court granted a government motion for reconsideration one month later.[183] The Government had been able to decrypt a small portion of an encrypted hard drive, revealing child pornography, and importantly, "detailed personal financial records and documents belonging to Feldman," and "dozens of personal photographs of Feldman."[184] The Court held that "Feldman's access to and control over the encrypted storage devices was a 'forgone conclusion.'"[185] Ultimately, the Government dismissed the original application, even after its victory (perhaps to foreclose an appeal), because it had "successfully decrypted

---

[176] *Id.* (noting the encryptions programs "appeared to be the sort that would lock or damage data if too many incorrect password guesses were made.").

[177] *Feldman I* at *2; *see generally* EMULE, http://www.emule-project.net/home/perl/general.cgi?l=1 (last visited Feb. 21, 2015) (eMule is a free peer-to-peer file sharing client that connects to multiple file sharing networks).

[178] *Id.* at *2–3.

[179] *Id.* at *2–4 n.6; *Hubbell*, 530 U.S. 27; *Fisher*, 425 U.S. 391 *Bumgardner,* 670 F.3d 1335;

[180] *Feldman I* at *4.

[181] *Id.* at *5.

[182] *Id.*

[183] *In re* The Decryption of a Seized Data Storage Sys., No. 2:13-mj-00449-WEC, 2013 BL 153162 (E.D. Wis. May 21, 2013) (*Feldman II*).

[184] *Id.* at *2.

[185] *Id.* (observing the devices were found in Feldman's residence, where he lived alone; the unencrypted computer's login screen had one username, Feldman's first name; and the recently decrypted portion of the hard drive had financial documents and photos clearly belonging to the defendant).

two of Feldman's hard drives."[186]

8. *Commonwealth v. Gelfgatt*

In *Commonwealth v. Gelfgatt*,[187] the Supreme Judicial Court of Massachusetts applied the "foregone conclusion" doctrine and held that compelling a defendant to enter an encryption key to seized computers was not testimonial.[188] Gelfgatt, an attorney, allegedly engaged in a complex mortgage fraud scheme, during which he used computers to conduct title searches and write documents.[189] After arresting Gelfgatt, law enforcement agents seized two desktop computers, a laptop computer, and a netbook, among other digital media.[190] All four computers were encrypted with "DriveCrypt Plus" software.[191] During questioning, Gelfgatt acknowledged that he owned multiple encrypted home computers, but that he would not divulge the passwords.[192]

The trial judge denied the Government's motion to compel Gelfgatt to enter his password to begin the decryption process on his computers.[193] The SJC granted direct review, and began by analyzing *Fisher*, *Hubbell* and the "foregone conclusion doctrine."[194] The Court engaged in a thorough analysis of the facts surrounding the case, noting that Gelfgatt admitted to State police Troopers that his computers were encrypted, and although he was able to decrypt the computers, the police were "not going to get to *any* of [his] computers."[195] Thus, the Court concluded, "motion to compel decryption does not violate the defendant's rights under the Fifth Amendment because the defendant is only telling the government what it already knows."[196] The majority never addressed the reasonable particularity standard adopted by other federal courts.[197] Nor did

---

[186] Motion to Dismiss Application at *1, *In re* The Decryption of a Seized Data Storage Sys., No. 2:13-mj-00449 (E.D. Wis. Aug. 16, 2013).

[187] Commonwealth v. Gelfgatt, 468 Mass. 512, 11 N.E.3d 605 (2014).

[188] *Id.* at 514, 11 N.E.3d at 608.

[189] *Id.* at 609, 11 N.E.3d at 514–15.

[190] *Id.* at 610, 11 N.E.3d at 516.

[191] *Id.*; *see SecurStar, Encryption Software Solutions–Products–DriveCrypt Plus Pack*, SECURSTAR, http://www.securstar.com/products_drivecryptpp.php (last visited Feb. 21, 2015).

[192] *Id.* at 610, 11 N.E.3d at 517.

[193] *Id.* at 611, 11 N.E.3d at 517–18.

[194] *Id.* at 614, 11 N.E.3d at 522.

[195] *Id.* at 615, 11 N.E.3d at 524.

[196] *Id.* at 616, 11 N.E.3d at 524.

[197] Interesting, and unmentioned by the majority, the dissenters in *Gelfgatt* noted that the Government intended "to introduce evidence of the encryption itself as evidence of "consciousness of guilt."" *Id.* at 619, 11 N.E.3d at 529 n.6 (Lenk, J., dissenting). The dissent noted that encryption was "a common business practice," and that many professional rules governing attorneys, including interim guidance from the Supreme Judicial Court itself, advised attorneys to encrypt data. *Id.*

it address arguments of attorney-client privilege.[198]

C. *Literature Review*

As with many emerging areas of the law, particularly those involving complex technology, there are few timely articles analyzing the Fifth Amendment as it specifically applies to the testimonial nature of ordering decryption or production of decrypted data. This brief literature review will examine articles written on the issue.Due to the fast-paced nature of this area of the law, some articles examine only a few of the cases discussed above.[199]

In *The Weak Protection of Strong Encryption: Passwords, Privacy, and Fifth Amendment Privilege*, Nathan K. McGregor examined the *Pearson* and *Boucher* cases.[200] McGregor argued that unlike the comparison of encryption to "translation" or a "safe," the analogy to a "shredder" is much more precise.[201] He explained that encryption is like a shredded document, unreadable and unreconstructable.[202] McGregor, however, ultimately makes a policy argument that, because the Supreme Court gives no Fifth Amendment protection to "diaries and datebooks" or other "private papers," protecting encrypted "invidious material as child pornography—surely contravenes public policy."[203]

In *The Right to Remain Encrypted: The Self-Incrimination Doctrine in the Digital Age*, Nicholas Soares examined *Fricosu*, *Boucher*, and *Bumgardner*.[204] In analyzing these three cases, Soares, overstates the nature of the tension between *Fricosu* and *Bumgardner*, believing the District Court in *Fricosu* erred in believing that there was sufficient evidence to authenticate the defendant as the sole owner of the laptop in question.[205] However, this significantly overstates *Fricosu*'s arguments: a District Court in the first instance felt there were sufficient facts on the record to demonstrate ownership of the specific laptop.[206] Soares also characterizes *Boucher I* and *Boucher II* as "reach[ing] *different* results by applying the *same doctrine* to the *same facts*."[207] This also appears to misstate the facts of the case, because in *Boucher I* the Government subpoenaed the password, while in *Boucher II* the Government merely subpoenaed the

---

[198] *Id.* at 627, 11 N.E.3d at 541 (Lenk, J., dissenting).

[199] *See supra* Part II.B.

[200] Nathan K. McGregor, Note, *The Weak Protection of Strong Encryption: Passwords, Privacy, and Fifth Amendment Privilege*, 12 VAND. J. ENT. & TECH. L. 581 (2010).

[201] *Id.* at 602–03.

[202] *Id.*

[203] *Id.* at 607.

[204] Nicholas Soares, Note, *The Right to Remain Encrypted: The Self-Incrimination Doctrine in the Digital Age*, 49 AM. CRIM. L. REV. 2001 (2013).

[205] *Id.* at 2010–11; *see* United States v. Fricosu, 841 F. Supp. 2d 1232, 1235 (D. Colo. 2012).

[206] *Fricosu*, 841 F. Supp. 2d at 1235 (noting the conversation about the recently seized laptop between Fricosu and incarcerated co-defendant occurred the day after the seizure).

[207] Soares, *supra* note 204, at 2009–10.

unencrypted copy of the seized encrypted hard drive after Boucher had already confessed to Government agents that the laptop was in his sole possession.[208] Because the Government changed tactics and subpoenaed a copy of the unencrypted media rather than the password itself, it could properly rely on the foregone conclusion, because it could independently authenticate the Defendant's possession of the laptop (through the Defendant's confession), and therefore, the act of production added nothing to the Government's case as such.

Chet Kaufman, Assistant Federal Public Defender and the lead defense counsel in *Bumgardner*, has published a thorough article analyzing mostly the *Bumgardner* case.[209] Kaufman explores the limits of the foregone conclusion doctrine, particularly as the Eleventh Circuit adopted the "reasonable particularity" standard of the District of Columbia and Ninth Circuits.[210] Kaufman also analyzes the limits of the doctrine, particularly as it pertains to collective business entities.[211]

III. ORDERS TO DECRYPT ENCRYPTED MEDIA VIOLATE THE FIFTH AMENDMENT BECAUSE THE ACT OF PRODUCTION IS TESTIMONIAL

A. *The Act of Producing a Password or Unencrypted Copy of Encrypted Media is Testimonial for Purposes of the Fifth Amendment*

The best framework to analyze encryption and the Fifth Amendment is to examine how the encryption system in a given case actually works, rather than creating inapt analogies between encryption and older technology. Because every case has different facts involving different types of encryption, a fact-based inquiry of the technology best allows courts to understand how the underlying technology interacts with the Fifth Amendment. Ultimately, the Eleventh Circuit in *Bumgardner* correctly sketched the bounds of the Fifth Amendment as it applies to compulsory orders to produce unencrypted media or provide passwords.[212]

Encryption is often involved in criminal offenses concerning the possession of contraband, such as child pornography on a computer, or some other electronic evidence important for the Government's case.[213] Often, child pornography cases begin by an online investigation, where the real identity of the alleged child pornography possessor is unknown.[214] Thus, even when the Government eventually traces the data coming into the computer network inside a person's home, it still lacks an important link in proving its case: tracing

---

[208] *In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *4 (D. Vt. Feb. 19, 2009).

[209] Chet Kaufman, *Encrypting Data May Give Rise to a Limited Constitution Defense*, 37 CHAMPION 36 (Aug. 2013).

[210] *Id.* at 37–38.

[211] *Id.* at 39–40.

[212] *See supra* Part II.B.5.

[213] *See supra* Part II.B.2–4, 7.

[214] *See supra* Part II.B.2–4, 7.

the child pornography from the home network to an individual defendant.[215] This task is especially difficult in a household with several residents and with no other evidence of child pornography, except for encrypted data on the computers and hard drives.[216] In such situations, the Government faces two hurdles. First, the prosecution may need the actual child pornography to prove its case.[217] Second, it has to establish that the individual defendant possessed the child pornography.[218] Commonly, defendants might admit in a post-*Miranda*[219] interview that they possessed child pornography or even show some of it to an agent.[220] Such admissions give the Government one critical piece of evidence: a direct link between the contraband and the defendant. The compelling of a password or compulsory decryption is another way of tying the defendant to the data. Without it, a defendant may be able to claim, "Yes, you found child pornography on a hard drive, but you cannot prove that the hard drive was mine." Because a password comes from a defendant's mind, its revelation is testimonial; thus, an order to compel decryption compels a testimonial act.[221]

Courts and commentators that attempt to analogize to older technology often "miss the metaphor" because there is no historical analogue that matches encryption in the constitutionally relevant ways. Many analogies to older technology simply do not replicate how electronic encryption actually works.[222] Although metaphors are useful in analogizing new technology to older, more familiar one, if the metaphor is stretched too far, it loses its usefulness to courts and commentators.[223]

Encryption is not a language or a translation, because, generally, more than one person knows a language. The fact that only an individual defendant can "speak" the "language" of encryption has testimonial significance, because it allows the Government to prove sole control of the encrypted media. Merely knowing such a unique "language" could permit the Government to prove knowledge of contents of the encrypted media. This is obviously not the case with a spoken language: if a person can read Spanish, the Government cannot prove that that person knows the contents of every Spanish-language text. Even

---

[215] *See supra* Part II.B.2–4, 7.

[216] *See supra* Part II.B.2–4, 7.

[217] *See supra* Part II.B.2–4, 7.

[218] *See supra* Part II.B.2–4, 7.

[219] Miranda v. Arizona, 384 U.S. 436 (1966) (holding arresting officers must give defendants warnings about their constitutional right against self-incrimination and defendants have to voluntarily waive this right before they can give statements that are admissible in court).

[220] *See supra* Part II.B.3.

[221] *See* Curcio v. United States, 354 U.S. 118, 128 (1957).

[222] *See supra* Part I.A.2 for a discussion of modern cryptology.

[223] *In re* Grand Jury Subpoena Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012) ("The Government attempts to avoid the analogy by arguing that it does not seek the combination or the key, but rather the contents. This argument badly misses the mark.").

though defendants do not "know" the language, they are the sole possessors of the password or have the sole ability to "read" and "translate" the language. These acts are testimonial because only the defendants can make the language understandable to other people. By doing so, the defendants can help authenticate their sole possession of encrypted media.

The "strongbox" or "key" metaphor also is inappropriate. Although software manufacturers may describe their products as "locking" data or describe passwords as a "key," that is not how the technology actually works.[224] The Supreme Court has long recognized that "being forced to surrender the key to a strongbox" is constitutional.[225] Encryption does not simply put a physical barrier in front of readable information, but renders the plaintext into ciphertext, making it unreadable.

A "combination" metaphor to a safe more accurately captures a password's testimonial nature, because a combination is something that is in one's mind. However, it also fails to represent how the data is actually stored. Generally, a letter in a safe is readable by humans. The safe metaphor might lead one to incorrectly believe that the plaintext version of encrypted data exists behind the safe's door. But in a modern cryptosystem, encrypted data exists only as ciphertext until accessed.

The "shredder" metaphor comes closer. Shredding a document "transforms" it into an unreadable form; however, the person who does the shredding is no more able to transform it *back* to a readable form than the Government. Perhaps one can imagine a shredder that shreds in a certain pattern only known to the person doing the shredding, enabling him to easily reconstruct the document, but like a language only one person knows, this carries the metaphor too far.

B. *The Foregone Conclusion Doctrine Will Defeat Fifth Amendment Claims If the Government Can Independently Prove Location, Existence and Authenticity of the Evidence with Reasonable Particularity*

A defendant's ability to invoke the Fifth Amendment in the context of a compulsory order to decrypt will depend on the foregone conclusion doctrine and events that in all likelihood long preceded the subpoena or warrant. The foregone conclusion doctrine will permit the Government to compel a defendant when the Government can otherwise prove that the hard drive and its data was the sole property of the defendant.[226] If a defendant confesses to possession of the drive, that may suffice.[227] If the Government can view some portion of

---

[224] *See supra* Part I.A.2.

[225] United States v. Hubbell, 530 U.S. 27, 43 (2000) (citing Doe v. United States, 487 U.S. 201, 210 n.9 (1988)).

[226] *Bumgardner* at 1343 n.19.

[227] *In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *4 (D. Vt. Feb. 19, 2009).

the hard drive and determine that the files belonged to one individual, that too may suffice.[228]

The "reasonable particularity" standard adopted by the Eleventh Circuit in *Bumgardner* has not been endorsed by the Supreme Court, but has been adopted by two other circuits.[229] Before *Hubbell* had gone up to the Supreme Court, the D.C. Circuit had used the "reasonable particularity" standard,[230] but the Supreme Court did not comment on it at all when it heard the case.[231] The Eleventh Circuit succinctly described the standard in *Bumgardner*: "[w]here the location, existence, and authenticity of the purported evidence is known with reasonable particularity, the contents of the individual's mind are not used against him, and therefore no Fifth Amendment protection is available."[232]

In *Boucher*, the defendant made statements to law enforcement that he owned the hard drive; he then entered his password, and showed child pornography on the hard drive to law enforcement.[233] Thus, the Government possessed sufficient evidence that Boucher owned and exercised sole control over the hard drive and its content, and thus the testimonial nature of the act of production (of the decryption) was a foregone conclusion.[234] *Fricosu* follows similar logic, although the Government learned that the defendant was the sole owner not through a confession but through a recorded phone call in prison.[235] *Feldman* is also in accord with that understanding of the foregone conclusion doctrine.[236] Because the Government was able to partially decrypt (though by what methods is unclear from the publically available docket) the hard drive and determine that it contained the defendant's personal information, the district court held that it was a foregone conclusion that the computer belonged to the defendant.[237]

The foregone conclusion doctrine also explains the results when courts have ruled in favor on defendants. In *Pearson*, the district court ruled for the defendant until it was able to hold an evidentiary hearing because there was an open factual question as to whether the defendant was the sole user of the comput-

---

[228] *Id.*

[229] *See* United States v. Ponds, 454 F.3d 313, 320–21 (D.C. Cir. 2006); *In re* Grand Jury Subpoena, Dated April 18, 2003, 383 F.3d 905, 910 (9th Cir. 2004).

[230] United States v. Hubbell, 167 F.3d 552, 579–80 (D.C. Cir. 1999).

[231] *Ponds* at 320–21 (noting that the Supreme Court in *Hubbell* did not adopt the lower court (D.C. Circuit's) "reasonable particularity" standard when it affirmed).

[232] *In re* Grand Jury Subpoena Dated March 25, 2011, 670 F.3d 1335, 1344 (11th Cir. 2012).

[233] *In re* Boucher, 2007 WL 4246473, *1–2 (D. Vt. Nov. 29, 2007).

[234] *In re* Boucher, 2009 WL 424718, at *4 (D. Vt. Feb. 19, 2009).

[235] United States v. Fricosu, 841 F. Supp. 2d 1232, 1235 (D. Colo. 2012).

[236] *In re* The Decryption of a Seized Data Storage Sys., No. 2:13-mj-00449-WEC, 2013 BL 153162, at *2 (E.D. Wis. May 21, 2013).

[237] *Id. at* *3.

er.[238] Similarly in *Bumgardner*, the Eleventh Circuit's ruling hinged on the fact that the Government was unable to prove that there was any content on the encrypted hard drives.[239]

Ultimately, whether or not the foregone conclusion doctrine applies in the context of encryption is a fact-bound determination. Can the Government point to a specific file or set of data it is looking for? Can it trace evidence directly to the encrypted hard drive and not merely to a computer network? Can it pinpoint the exact hard drive location of the files it wants? Can the Government prove sole ownership and control of the hard drive? If it can partially decrypt the hard drive, dose the decrypted data demonstrate sole ownership, or does it suggest that there is more evidence to be found? During hearings on motions to suppress, these questions can only be answered by careful forensic searches, proven with clear testimony from qualified experts, such that judges and litigants can understand the underlying technology.

IV. CONCLUSION

When dealing with encryption and the Fifth Amendment, courts and commentators should be hesitant to analogize encryption to older technology, and instead should engage in a fact-specific inquiry that focuses on exactly what type of encryption is being used, the testimonial nature of the act of production of a password or decrypted material, and what the government can prove it already knows about the material it is seeking. Inapt analogies and inexact information yield "bad" law. Prosecutors and defense counsel should ensure that experts who understand the issues of encryption testify to a judge in a cogent and coherent way that puts the testimonial issue squarely before a court.

When the Government has already seen the material it seeks with sufficient particularity, the foregone conclusion doctrine may apply. If the Government knows little or nothing about the encrypted material, or does not even know whether or not any material actually exists on an encrypted hard drive or device, using the contents of a defendant's mind to get evidence violates the Fifth Amendment's prohibition against compulsory testimony against oneself. Whether or not a Circuit Court has adopted the "reasonable particularity" standard of the Ninth, Eleventh, and D.C. Circuits[240] may determine how much independent evidence the Government will need to prove in order to satisfy the foregone conclusion. Ultimately, whether or not the Fifth Amendment applies to a particular compulsory process involving encryption will be a fact-bound question.

---

[238] United States v. Pearson, No. 1:04-CR-340, 2006 U.S. Dist. LEXIS 32982 at *61–62 (N.D.N.Y. May 24, 2006).

[239] *In re* Grand Jury Subpoena Dated March 25, 2011, 670 F.3d 1335, 1349 (11th Cir. 2012).

[240] *See* United States v. Ponds, 454 F.3d 313, 320–21 (D.C. Cir. 2006); *In re* Grand Jury Subpoena, Dated April 18, 2003, 383 F.3d 905, 910 (9th Cir. 2004).