Florida Law Review

Volume 70 | Issue 4 Article 3

The Skeleton in the Hard Drive: Encryption and the Fifth Amendment

David W. Opderbeck

THE SKELETON IN THE HARD DRIVE: ENCRYPTION AND THE FIFTH AMENDMENT

*David W. Opderbeck**

Abstract

Courts are grappling with the question whether forced decryption of computer files violates the Fifth Amendment privilege against self-incrimination. This Article supplies the background necessary for courts to address this question. It explains how full disk encryption works and discusses the nature of encryption technology from a semantic and information-theory perspective. It also compares how similar questions have been addressed in other areas of the law that have dealt with computer code as speech: the First Amendment and copyright law. This Article argues that disclosure of a password or encryption key is not a testimonial act and therefore is not privileged under the Fifth Amendment.

---

* Professor of Law, Seton Hall University Law School, and Co-Director, Gibbons Institute of Law, Science & Technology. Thanks to Michael Pardo and Ronald Allen for helpful comments on earlier drafts of this Article.

INTRODUCTION

User-controlled encryption is cheap, easy, and ubiquitous. This is good, because encryption provides invaluable benefits for commerce and personal freedom. Without encryption, the Internet and other modern communications networks would lose much of their valuable functionality. But encryption is also a significant problem, because it enables criminals to hide evidence.[1] Contrary to television shows such as "CSI" or "24," forensic investigators cannot crack most off-the-shelf encryption.[2] Many criminals hide skeletons in their hard drives, protected by encryption that can only be unlocked with a skeleton key they alone hold.

Common user-controlled encryption tools are enabled using passwords, biometric identifiers (such as fingerprints), and encryption keys.[3] Courts have just begun to grapple with the question whether the Fifth Amendment protects against the compelled disclosure of these items.[4] Most courts so far have agreed that disclosure of a password or decryption key is a testimonial act.[5] However, with some notable exceptions, most courts have also agreed that the "foregone conclusion" doctrine can justify compelled disclosure.[6]

To address this question, courts must obtain a clear understanding of how encryption works, and, in particular, must understand common forms of "full disk encryption." Courts should also consider the philosophical or normative question of what encryption is and what it does in relation to computer code. Only with this kind of background can courts decide whether disclosure of a password or encryption key is "testimony" or whether the foregone conclusion doctrine can apply.

This Article supplies that necessary background and argues that, under a proper application of Fifth Amendment doctrine, compelled decryption ordinarily is not a testimonial act and therefore is not privileged. Part I of this Article supplies a background in encryption technology. Part II summarizes recent Fifth Amendment cases concerning compelled decryption. Part III looks at encryption and computer code from a semiotics and information theory perspective and examines how computer code is treated under First Amendment and copyright law for

1. For a discussion of some of these tensions, see David W. Opderbeck, *Encryption Policy and Law Enforcement in the Cloud*, 49 CONN. L. REV. 1657, 1662–63 (2017).

2. *See infra* Section I.B.

3. *See infra* Section II.B.

4. *See id.*

5. *See id.*

6. *See id.*

possible analogies to the Fifth Amendment context. Part IV presents this Article's doctrinal arguments under the Fifth Amendment.

I. UNDERSTANDING ENCRYPTION

A. *Encryption Algorithms and Keys*

Encryption is the application of an algorithm to readable information (plaintext) to render the information unintelligible (ciphertext).[7] Decryption is the application of a "key" derived from the encryption algorithm to render the information intelligible once again.[8]

An ancient and simple encryption scheme, the "Caesar Cipher," demonstrates how this process works.[9] The Caesar Cipher involves shifting the letters of the alphabet a set number of positions.[10] A "ROT13" Caesar cipher, for example, rotates the English alphabet 13 places to the right, making the encryption "key" 13.[11] Thus, using the ROT13 cipher, the text "cynl vg ntnva fnz" means "play it again sam" because the letter "r" is 13 places in the alphabet from the letter "e," and so on. This is an example of "symmetric key" encryption, because the same key is used to encrypt and decrypt the data.[12] In asymmetric or "public key" encryption, there are two related keys: a "public" key and a "private" key.[13]

The ROT13 cipher is simple to use because, with twenty-six letters in the Latin alphabet, each letter is the inverse of the letter that is thirteen places away. This simplicity also makes ROT13 easy to crack.[14] Many contemporary forms of computer encryption, however, are essentially impossible to crack, even with the help of large-scale computer power. For example, the Advanced Encryption Standard (AES) approved by the U.S. National Institutes of Standards and Technology (NIST) for use with top secret information, applies 128-bit encryption with 128, 192, or 256

---

7. *See* U.S. DEP'T OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., NIST Special Publication 800-57, RECOMMENDATION FOR KEY MANAGEMENT – PART 1: GENERAL REVISION 3 (July 2012) (defining "ciphertext" and "plaintext"); Eric A. Hibbard, *Encryption: The Basics*, *in* DATA BREACH AND ENCRYPTION HANDBOOK 177, 178 (Lucy Thomson ed., A.B.A. 2011); DAVID SALOMON, DATA PRIVACY AND SECURITY: ENCRYPTION AND INFORMATION HIDING 7 (2003) (noting that "[e]ncrypting a message involves two ingredients, an algorithm and a key").

8. SALOMON, *supra* note 7, at 7.

9. *Id.* The Caesar Cipher is so named because Julius Caesar used it.

10. *Id.*

11. *Id.* at 8.

12. NIST Special Publication 800-57, *supra* note 7, at 28 (defining "Symmetric-key algorithm").

13. *Id.* at 26 (defining "[p]ublic-key (asymmetric) cryptographic algorithm").

14. For a discussion of the ubiquitous use of ROT13 on the early Usenet as a form of insider humor, see the Wikipedia entry for "ROT13." *See What Is ROT13?*, IND. U., https://kb.iu.edu/d/aeol (last visited May 4, 2018).

bit decryption keys and is practically unbreakable with existing computer power.[15]

B. *Full Disk Encryption*

It is easy to copy or "image" the contents of a computer's hard drive or a smart phone's memory. Every state has at least one computer forensics lab capable of producing an exact copy of a hard drive, and regional labs coordinate among multiple states and the federal government.[16] Courts routinely issue search warrants for the seizure of personal computers, laptops, and hard drives based on probable cause that the devices contain contraband (such as child pornography files) or other evidence of criminal activity (such as spreadsheets or other documents detailing financial crimes).[17] The investigation of "computer crime" is now a mainstream law enforcement activity.

Despite the sophistication of law enforcement, however, these forensic laboratories cannot crack robust disk encryption. The use of full disk encryption (FDE), through which the entire contents of a hard drive are encrypted, can render the drive completely opaque to law enforcement. In popular computer lingo, the drive becomes a "brick."[18]

A proper understanding of FDE requires some background in personal computer architecture. Common desktop and laptop computers are comprised of a set of basic components, including hardware, operating system (OS) software, and application software.[19] The hardware

15. *See* NAT'L INST. OF STANDARDS & TECH., FEDERAL INFORMATION SYSTEMS PROCESSING STANDARD 197: ANNOUNCING THE ADVANCED ENCRYPTION STANDARD (AES) (Nov. 26, 2001), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf; ADVANCED ENCRYPTION STANDARD (AES), CNSS POLICY NO. 15, FACT SHEET NO. 1, 2 (June 2003), https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/cnss15fs.pdf (stating that "the design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths"); *New Attack on AES*, SCHNEIER ON SECURITY (July 1, 2009, 11:49 AM), https://www.schneier.com/blog/archives/2009/07/new_attack_on_a.html (noting that a recently published possible method of attacking AES remains "far, far beyond our capabilities of computation").

16. *See, e.g.*, NEW JERSEY REGIONAL COMPUTER FORENSICS LAB, http://www.njrcfl.org/ (last visited June 9, 2014).

17. *See generally* OFFICE OF LEGAL EDUCATION, EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS, SEARCHING AND SEIZING COMPUTERS AND OBTAINING EVIDENCE IN CRIMINAL INVESTIGATIONS 61–63, https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

18. *See Bricked*, URBAN DICTIONARY, http://www.urbandictionary.com/define.php?term=bricked (last visited Apr. 8, 2018).

19. *See generally* IAN WEINAND, COMPUTER ARCHITECTURE FOR BEGINNERS 35 (2016), http://bottomupcs.sourceforge.net/csbu/c1453.html (explaining the functions of a central processing unit); *id.* at 62 (explaining the role of the operation system); *Basic Computer*

components include a motherboard with the microprocessor and random access memory (RAM), input and output devices (such as a keyboard, mouse, and monitor), and long term memory, which typically consists of one or more magnetic hard drives. Application software may include word processors (such as Microsoft Word), spreadsheets (such as Microsoft Excel), presentation tools (such as Microsoft PowerPoint), and a wide variety of other programs that accept user input and produce related content.[20] The computer user employs application programs to produce user-generated content, such as word-processing documents.[21]

The OS, in a sense, sits "between" the computer's hardware and application software layers.[22] The OS coordinates the operations of the computer's various hardware components and allows those components and the application software to "talk" with each other. A computer's OS usually resides on the computer's primary hard drive.[23] Before the OS is accessed, the hard drive must boot up, which requires some degree of coordination among the computer's hardware components before the OS begins to play its coordinating function.[24] This pre-OS coordinating function is performed by software routines that are hard-coded on chips on the motherboard.[25] For IBM-compatible PCs (the kind of machine that runs Microsoft Windows as an OS), these routines are called the BIOS (Basic Input/Output System).[26] When a new primary hard drive is added to a PC, the drive is "formatted" by the system to incorporate a "pre-boot" sector containing BIOS code.[27] After the drive is formatted, whenever the computer is powered up, the BIOS code on the motherboard interacts with the BIOS code on the hard drive and then the OS is accessed.[28] A highly stylized representation of these relationships is as follows:

Architecture, *in* COMPUTER SCIENCE EDUCATION PROJECT, https://www.phy.ornl.gov/csep/ca/node2.html#SECTION00020000000000000000 (last visited Mar. 12, 2018) (explaining the basic computer components).

20. *Basic Computer Architecture*, *supra* note 19.

21. *See generally* DAN GOOKIN, PCS FOR DUMMIES (John Wiley & Sons, Inc., 12th ed. 2005) (describing the general uses and applications of computers).

22. *See* MIROSLAW MALEK, COMPUTER SCI. ENGINEERING, OPERATING SYSTEM 2, https://www.eolss.net/sample-chapters/C15/E6-45-03-01.pdf, (last visited May 4, 2018).

23. *See Boot Device*, COMPUTER HOPE, https://www.computerhope.com/jargon/b/bootdevi.htm (last updated Dec. 20, 2017).

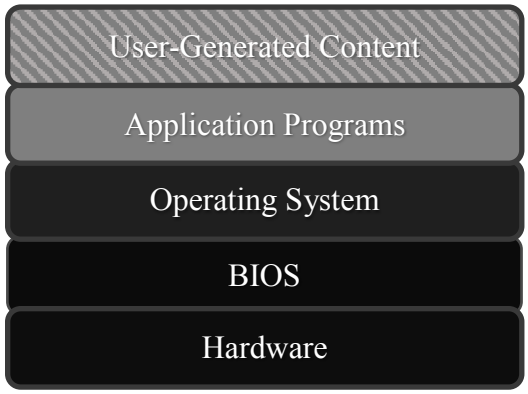
24. *Id.*

25. *See Hard Drive*, COMPUTER HOPE, https://www.computerhope.com/jargon/h/harddriv.htm (last updated Apr. 1, 2018).

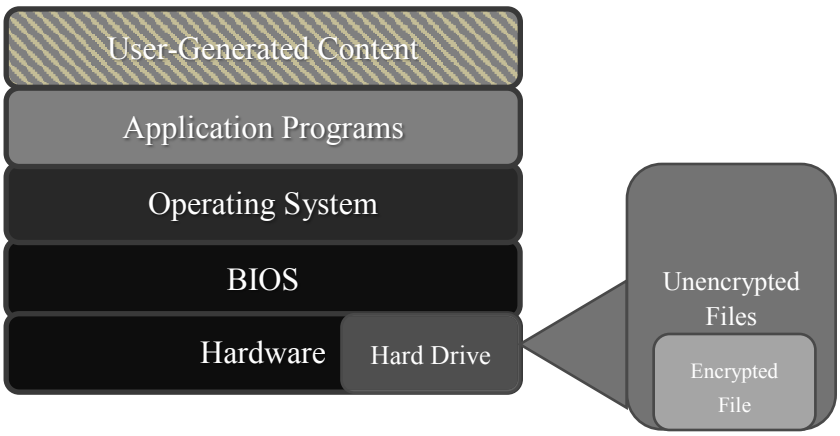
26. *See id.*

27. *See Pre-boot Authentication*, SECUDE, https://web.archive.org/web/20120304234645/http://www.secude.com/media-room/white-papers/full-disk-encryption/pre-boot-authentication/ (last visited May 4, 2018).

28. *Id.*



Basic computer disk encryption involves applying an encryption algorithm to files on the disk so that they are not readable by humans without decryption.[29] For example, a word processing document listing the secret formula for Coke could be encrypted so that only persons with the decryption key could read the information in the file. While encryption of selected files might be adequate for some purposes, a third party could still view non-encrypted files on the hard drive, and also could learn by inspecting the hard drive that it contains encrypted files. The following shows how this sort of encryption relates to the computer architecture:



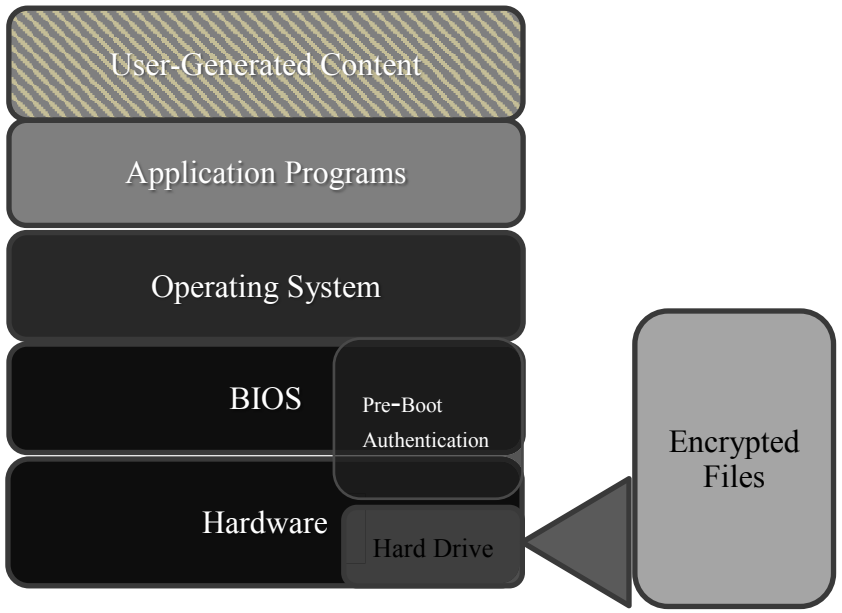
"Full disk encryption" (FDE), in contrast, is a method of securing the entire disk so that all of the disk's contents are encrypted and no one without the necessary password and key can even boot up the disk.[30]

29. *See Troubleshooting Hard Drive Encryption Issues*, DELL KNOWLEDGE BASE, https://www.dell.com/support/article/us/en/19/sln155364/troubleshooting-hard-drive-encryption-issues?lang=en (last modified Mar. 7, 2018).

30. *See id.*

Arguably, FDE obscures the question whether the disk contains any files at all—although, as discussed in Part II below, courts have not yet correctly understood the implications of this technology for Fifth Amendment jurisprudence.

FDE involves the encryption of all files on the hard drive together with a password or biometric lock on the drive's boot sector.[31] The FDE application writes some code to the drive's boot sector that interacts with the BIOS upon start-up.[32] This code requires the entry of a user-generated password in order for the boot sequence to continue.[33] Once the machine boots up, the user-generated password or biometric identifier can be used as a "seed" for a randomly-generated encryption key.[34] The encryption key is employed in connection with an algorithm such as AES to encrypt all the files on the hard drive.[35] While the user is working with a file, the decryption key makes the file readable to the user and encrypts any additional content on the fly.[36] This sort of encryption scheme can be illustrated as follows:



31. Kaspersky Lab Online Courses, KL 108.10: Encryption, *Ch. 2: Full Disk Encryption*, KASPERSKY LAB, slide 2, http://support.kaspersky.com/learning/courses/kl_108.10/unit1_ chapter2.

32. SYMANTEC, WHITE PAPER: HOW DRIVE ENCRYPTION WORKS 1–2 (2012), http://www.symantec.com/content/en/us/enterprise/white_papers/b-how-drive-encryption-works _WP_21275920.pdf (last visited Apr. 1, 2018).

33. *Id.* at 1.

34. Kaspersky Lab Online Courses, KL 108.10: Encryption, *Ch. 2: Full Disk Encryption*, *supra* note 31, at slide 4.

35. *Id.* at slide 2.

36. *Id.* at slide 3.

FDE is a widely available technology. Until very recently, an open source project called "TrueCrypt" was freely available to anyone online.[37] Commercial FDE products such as "DriveCrypt" can be purchased for less than $60, and products such as Sophos SafeGuard work with Microsoft Bitlocker to provide enterprise-level encryption.[38] Even more directly, Microsoft Bitlocker is now integrated with Windows 10, so that FDE is available to any Windows 10 user.[39]

II. THE FIFTH AMENDMENT MEETS ENCRYPTION

A. *Background*

The Fifth Amendment states that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself."[40] This provision does not protect against mere disclosure of private information.[41] Privacy is the domain of the Fourth Amendment and its probable cause, warrant, and related requirements.[42] As the Supreme Court stated in *Fisher v. United States*,[43] "the Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a testimonial communication that is incriminating."[44] The fact that a warrant or subpoena might require a criminal suspect to produce documents that might contain incriminating information therefore does not in itself

37. The TrueCrypt source code was available at http://truecrypt.sourceforge.net/ until the code's developers shocked observers by discontinuing the site. *See TrueCrypt Final Release Repository*, GIBSON RES. CORP., https://www.grc.com/misc/truecrypt/truecrypt.htm (last visited Mar. 16, 2018); *see also* James Lyne, *Open Source Crypto TrueCrypt Disappears with Suspicious Cloud of Mystery*, FORBES (May 29, 2014, 3:16 AM), http://www.forbes.com/sites/jameslyne/2014/05/29/open-source-crypto-truecrypt-disappears-with-suspicious-cloud-of-mystery/; *Tales from the TrueCrypt*, ECONOMIST (June 7, 2014), http://www.economist.com/ news/science-and-technology/21603407-mysterious-useful-piece-software-disappears-mysteriously-tales.

38. *DriveCrypt 1344-Bit – Disk Encryption*, SECURSTAR, http://www.securstar.biz/drivecrypt.html (last visited Mar. 16, 2018); *Sophos SafeGuard Enterprise*, SOPHOS http://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophossafeguardenterprisedsna.pdf?la=en (last visited Mar. 16, 2018); *BitLocker*, MICROSOFT: WINDOWS IT PRO CENTER (Oct. 16, 2017), https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview.

39. *See Bitlocker Frequently Asked Questions (FAQ)*, MICROSOFT: WINDOWS IT PRO CENTER (Oct. 16, 2017), https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-frequently-asked-questions.

40. U.S. CONST. amend. V.

41. Fisher v. United States, 425 U.S. 391, 401 (1976).

42. *Id.*

43. 425 U.S. 391 (1976).

44. *Id.* at 408 (emphasis omitted).

violate the Fifth Amendment's protection against compelled self-incrimination.[45]

The Supreme Court has wrestled with this distinction between "privacy" and "testimony" in a long line of cases going back to *Schmerber v. California*.[46] In *Schmerber*, the defendant was in a car accident and was arrested at a hospital on suspicion of driving under the influence of alcohol.[47] At the direction of a police officer, a physician at the hospital took a blood sample, which was tested for blood alcohol level.[48] The defendant claimed that this non-consensual blood test violated his Fifth Amendment right against self-incrimination.[49] The Court disagreed.[50]

According to the Court, "[t]he distinction which has emerged, often expressed in different ways, is that the privilege is a bar against compelling 'communications' or 'testimony,' but that compulsion which makes a suspect or accused the source of 'real or physical evidence' does not violate it."[51] The *Schmerber* Court acknowledged that "there will be many cases in which such a distinction is not readily drawn. Some tests seemingly directed to obtain 'physical evidence,' for example, lie detector tests measuring changes in body function during interrogation, may actually be directed to eliciting responses which are essentially testimonial."[52] Nevertheless, the Court concluded that "[n]ot even a shadow of testimonial compulsion upon or enforced communication by the accused was involved either in the extraction or in the chemical analysis."[53]

Subsequently, *Fisher* tested the line between privacy and testimony in relation to documentary evidence.[54] In that case, the defendants were accused of tax violations and the documents were subpoenaed from the defendants' accountant or attorney.[55] The defendants argued that compelled production of the documents would amount to an admission that the documents existed and were under their control.[56] The Court rejected this argument.[57] According to the Court,

45. *Id.*
46. 384 U.S. 757 (1966); *id.* at 764.
47. *Id.* at 758.
48. *Id.*
49. *Id.* at 759.
50. *Id.*
51. *Id.* at 764.
52. *Id.*
53. *Id.* at 765.
54. Fisher v. United States, 425 U.S. 391, 421–23 (1976).
55. *Id.* at 394.
56. *Id.* at 410.
57. *Id.* at 410–11.

> It is doubtful that implicitly admitting the existence and possession of the papers rises to the level of testimony within the protection of the Fifth Amendment. The papers belong to the accountant, were prepared by him, and are the kind usually prepared by an accountant working on the tax returns of his client. Surely the Government is in no way relying on the "truth-telling" of the taxpayer to prove the existence of or his access to the documents. . . .[58]

The Court then introduced what has become known as the "foregone conclusion" doctrine:

> The existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers. Under these circumstances by enforcement of the summons "no constitutional rights are touched. The question is not of testimony but of surrender."[59]

The *Fisher* Court listed many kinds of potentially incriminating physical evidence a criminal suspect could be compelled to produce without implicating the Fifth Amendment right against self-incrimination, including blood samples, handwriting exemplars, voice exemplars, and trying on items of clothing.[60] Each of these examples involved the compulsion of some act that was not itself considered testimonial. Other examples of compelled conduct have included compelling the suspect to submit to "fingerprinting, photographing, or measurements, to write or speak for identification, to appear in court, to stand, to assume a stance, to walk, or to make a particular gesture."[61]

It is unclear from the *Fisher* Court's "foregone conclusion" statement whether a given act is inherently non-testimonial or an *exception* to the Fifth Amendment privilege. This confusion is evident in the forced decryption cases discussed in Section II.B below. The confusion is heightened by two Supreme Court cases subsequent to *Fisher* that also

58. *Id.* at 411 (quoting *In re* Harris, 221 U.S. 274 (1911)).

59. *Id.*

60. *Id.* at 408 (citing Schmerber v. California, 384 U.S. 757, 763–64 (1966) (refusing to extend the protection of the Fifth Amendment privilege to blood samples)); United States v. Wade, 388 U.S. 218, 222–23 (1967) (refusing to extend the protection of the Fifth Amendment privilege to voice exemplars); Gilbert v. California, 388 U.S. 263, 265–67 (1967) (refusing to extend the protection of the Fifth Amendment privilege to handwriting exemplars); Holt v. United States, 218 U.S. 245 (1910) (refusing to extend the protection of the Fifth Amendment privilege to clothing).

61. *Schmerber*, 384 U.S. at 764.

factor into the "act of production"/"foregone conclusion" analysis: *Doe v. United States*[62] and *United States v. Hubbell*.[63]

In *Doe*, the principles discussed in *Schmerber* and *Fisher* were applied to a proposed order requiring a criminal defendant to sign a consent form authorizing foreign banks to produce his banking records.[64] The government suspected the defendant had deposited unreported income in foreign banks.[65] The defendant argued that signing the consent forms would constitute a "testimonial communication" because it would comprise "a declarative statement of consent made by Doe to the foreign banks."[66] Justice Blackmun, writing for the Court, disagreed.[67]

According to Justice Blackmun, "in order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a 'witness' against himself."[68] The primary purpose of the Fifth Amendment, Justice Blackmun noted, was to prevent the "inquisitorial method of putting the accused upon his oath and compelling him to answer questions designed to uncover uncharged offenses, without evidence from another source."[69] The consent forms at issue did not identify any specific account, state whether any documents were in existence at any particular bank, or include any admission about the authenticity of any records produced by any bank.[70]

The sole dissenter, Justice Stevens, argued that "[i]f John Doe can be compelled to use his mind to assist the Government in developing its case, I think he will be forced 'to be a witness against himself.'"[71] Justice Stevens argued that a witness "may in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe-by word or deed."[72]

In the Court's next effort to distinguish between compelled testimony and compelled production of physical evidence, *United States v. Hubbell*, Justice Stevens wrote the majority opinion.[73] *Hubbell* involved the famous (or infamous) "Whitewater" investigation and prosecutions of

62. 487 U.S. 201 (1988).
63. 530 U.S. 27 (2000); *id.* at 36; *Doe*, 487 U.S. at 209.
64. *Id.* at 203.
65. *Id.* at 202.
66. *Id.* at 208.
67. *Id.* at 219.
68. *Id.* at 210.
69. *Id.* at 212.
70. *Id.* at 215–16.
71. *Id.* at 220 (Stevens, J., dissenting).
72. *Id.* at 219.
73. United States v. Hubbell, 530 U.S. 27, 29 (2000).

Webster Hubbell.[74] Hubbell was serving a sentence for tax evasion and mail fraud resulting from a plea agreement with the Whitewater Special Prosecutor when he was served with a subpoena *duces tecum* for documents before a grand jury investigating further alleged fraud involving Whitewater.[75] Hubbell was ordered by the trial court to produce the documents under the federal grand jury immunity statute.[76] He produced the documents in response to this order, and was subsequently indicted on further tax and mail fraud charges.[77] The trial court dismissed the indictment because it believed the indictment was based on information in the documents in violation of the immunity statute.[78] After an appeal and a somewhat complicated conditional plea agreement, the immunity issue was heard by the Supreme Court.[79]

Justice Stevens noted that "there is a significant difference between the use of compulsion to extort communications from a defendant and compelling a person to engage in conduct that may be incriminating."[80] He further acknowledged that "a person may be required to produce specific documents even though they contain incriminating assertions of fact or belief because the creation of those documents was not 'compelled' within the meaning of the privilege."[81] Nevertheless, Justice Stevens stated, the "act of production" itself could constitute a testimonial admission that "the papers existed, were in [the defendant's] possession or control, and were authentic."[82] According to Justice Stevens,

> [i]t was unquestionably necessary for respondent to make extensive use of 'the contents of his own mind' in identifying the hundreds of documents responsive to the requests in the subpoena. . . . The 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.[83]

Justice Stevens also rejected the government's argument that the "foregone conclusion" analysis in *Fisher* saved the government's case against Hubbell. According to Justice Stevens,

74. *Id.* at 30.
75. *Id.* at 30–31.
76. *Id.* (citing 18 U.S.C. § 6002–6003).
77. *Id.* at 31.
78. *Id.* at 31–32.
79. *Id.* at 34.
80. *Id.* at 34–35.
81. *Id.* at 35–36.
82. *Id.* at 36.
83. *Id.* at 43.

> [w]hatever the scope of this 'foregone conclusion' rationale, the facts of this case plainly fall outside of it. While in *Fisher* the Government already knew that the documents were in the attorneys' possession and could independently confirm their existence and authenticity through the accountants who created them, here the Government has not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent.[84]

He therefore held that the indictment would violate the statutory grant of immunity and must be dismissed.[85]

Under the distinction between testimonial and non-testimonial acts of production, then, (1) the provision of *physical* acts or samples, such as standing in a lineup or giving a blood sample; and (2) the mere production of documents generally are not considered testimonial, while acts that convey *information about* the nature, location, or authenticity of documents or materials could be testimonial. Justice Stevens' dicta concerning the strongbox key and combination in his dissent in *Doe*, echoed in his majority opinion in *Hubbell* as applied to the foregone conclusion doctrine, has been featured in the contemporary debate over compelled disclosure of passwords tied to encryption keys. As the summary in the next Section suggests, courts are struggling to apply these concepts in the domain of computer files and digital encryption.

B. *Recent Cases Involving Compelled Decryption*

A handful of recent cases address how these principles should apply to encrypted hard drives. As noted above, many of these cases assume that the production of a password protecting encryption is a testimonial act, but construe the "foregone conclusion" doctrine as an exception to the Fifth Amendment privilege. However, in an important—but incorrectly decided—case, the Eleventh Circuit has held that the foregone conclusion doctrine may not apply when the contents of a hard drive are both unknown and encrypted.[86] Three other cases involve encryption that is accessed by biometric identification (in those cases, a fingerprint), with differing results.[87]

---

84. *Id.* at 44–45.

85. *Id.* at 45–46.

86. *See In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1344–46 (11th Cir. 2012).

87. *See* State v. Diamond, 890 N.W.2d 143, 150–51 (Minn. Ct. App. 2017), *aff'd*, 905 N.W.2d 870 (Minn. 2018); State v. Stahl, 206 So. 3d 124, 134–35 (Fla. Dist. Ct. App. 2016); Commonwealth v. Baust, 89 Va. Cir. 267, 2014 WL 10355635, at *4 (Va. Cir. Ct. 2014).

1. Compelled Production of Passwords Controlling Encryption

In one of the earliest reported cases on this issue, *United States v. Fricosu*,[88] FBI agents had seized a number of computers, pursuant to valid search warrants, at the home where defendant resided.[89] Of three laptop computers seized, one was encrypted with a program called PGP Desktop.[90] During a recorded conversation with her husband, a co-defendant who was incarcerated, Ms. Fricosu seemed to admit that the encrypted laptop contained a file or files relevant to the investigation.[91] The government then sought a writ under the All Writs Act compelling defendant to produce the contents of the encrypted hard dive.[92]

Based on the recorded telephone conversation, the court concluded that "[t]here is little question here but that the government knows of the existence and location of the computer's files. The fact that it does not know the specific content of any specific documents is not a barrier to production."[93] The court further found that that "the government has met its burden to show by a preponderance of the evidence that the Toshiba Satellite M305 laptop computer belongs to Ms. Fricosu, or, in the alternative, that she was its sole or primary user, who, in any event, can access the encrypted contents of that laptop computer."[94] It was also significant to the court that the government offered Ms. Friscosu immunity.[95] The court therefore found that an order requiring production of the laptop hard drive's decrypted contents would not violate the Fifth Amendment.[96] The order entered by the court compelled the defendant to perform the steps necessary to decrypt the computer's contents and prohibited the government from using those contents against Ms. Friscosu.[97]

In contrast, the Eleventh Circuit suggested in *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*,[98] that the foregone

88. 841 F. Supp. 2d 1232 (D. Colo. 2012).

89. *Id.* at 1234.

90. *Id.* PGP Desktop is a form of FDE offered by Symantec. *See Easy-to-Use Decryption Software*, SYMANTEC, https://www.symantec.com/products-solutions/products/buy.jsp%3Fpcid%3Dpcat_info_risk_comp%26pvid%3Ddesktop_home_1%26om_sem_cid%3Dbiz_sem_nam_us_Google_SMB_Store_PGP_Desktop_Home%26mktsrc%3Dpaidsearch%26om_sem_kw%3Dpgp%2Bhome (last visited Apr. 14, 2018) (describing the PGP Desktop Home product and showing the price per license).

91. *Fricosu*, 841 F. Supp. 2d at 1235.

92. *Id.*

93. *Id.* at 1237.

94. *Id.*

95. *Id.* at 1238.

96. *Id.* at 1237.

97. *Id.*

98. 670 F.3d 1335 (11th Cir. 2012).

conclusion doctrine cannot apply unless the government knows of specific files subject to the warrant or other process that are stored on the subject device.[99] Central to the court's decision in that case was the court's belief that the government did not know whether any files resided on the encrypted portion of the defendant's hard drive.[100] The court noted that the encryption software used by the defendant fills up free space on the encrypted portion of a drive with random characters.[101] According to the court, "because the TrueCrypt [encryption] program displays 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."[102] The court concluded that, because "random characters are not files," the government had not shown "that the drives *actually* contain any files, nor has it shown which of the estimated twenty million files the drives are capable of holding may prove useful."[103]

The Eleventh Circuit's approach did not prevail in one of the most comprehensive opinions on forced encryption in the federal and state case law, *Commonwealth v. Gelfgatt*.[104] In that case, the Massachusetts Supreme Judicial Court held, in a 5–2 opinion, that the foregone conclusion doctrine can apply to passwords that protect encryption keys.[105] Defendant Gelfgatt, an attorney, was charged with crimes involving mortgage fraud.[106] Pursuant to a search warrant, state police seized four computers from Gelfgatt's residence that were encrypted with DriveCrypt Plus full disk encryption software.[107] During his interrogation, Gelfgatt admitted that the computers were encrypted and that he held the passwords needed to decrypt the computers, but refused to turn over the passwords.[108] The Commonwealth moved for an order to compel decryption, which was denied by the lower courts.[109]

---

99. *Id.* at 1344–46.

100. *Id.* at 1346 ("Nothing in the record before us reveals that the Government knows whether any files exist and are located on the hard drives . . . .").

101. *Id.* at 1340 n.11.

102. *Id.* at 1347.

103. *Id.*; *cf.* SEC v. Huang, 2015 WL 5611644, at *2 (E.D. Pa. 2015) (following *In re Grand Jury*).

104. 11 N.E.3d 605 (Mass. 2014); *id.* at 619. The author of this Article filed an amicus brief in this case in support of the Commonwealth, joined by The Massachusetts Chiefs of Police Association and NW3C (The National White Collar Crime Center). *See* Brief of Amicus Curiae Professor David W. Opderbeck, Supported by the Massachusetts Chiefs of Police Association, Inc. and NW3C, Inc., *Gelfgatt*, 11 N.E.3d 605 (Mass. 2014).

105. *Id.* at 617.

106. *Id.* at 609.

107. *Id.* at 610.

108. *Id.* at 610–11.

109. *Id.* at 611.

The Massachusetts Supreme Court assumed, without much analysis, that the disclosure of a password is a testimonial communication.[110] The court stated that "[b]y such action, the defendant implicitly would be acknowledging that he has ownership and control of the computers and their contents," which differs from giving a physical evidence such as a blood sample or handwriting exemplar.[111] However, the court held that the foregone conclusion exception applied because there was clear evidence that Gelfgatt had been involved in some of the allegedly fraudulent mortgage transactions and had acknowledged that he kept encrypted files relating to these transactions.[112]

Justice Lenk, joined by Justice Duffy, filed a dissenting opinion.[113] Justice Lenk relied heavily on the Eleventh Circuit's decision in *In re Grand Jury Subpoena* for the argument that the government must show a degree of particularity about particular files or documents that is "significantly greater than what is required to show probable cause."[114] Therefore, Justice Lenk concluded, "the 'reasonable particularity' standard requires much more than government knowledge that a defendant owns or has access to a particular computer."[115] In Justice Lenk's view, the Commonwealth could not satisfy this standard.

Like the majority in *Gelfgatt*, the Third Circuit also recently has questioned the Eleventh Circuit's approach.[116] In *United States v. Apple Macpro Computer*,[117] the defendant was suspected of accessing child pornography over the internet.[118] A state search warrant was issued for the defendant's residence, and the police seized an Apple iPhone 5S, an Apple iPhone 6 Plus, an Apple Mac Pro Computer, and two attached external hard drives, all of which were encrypted.[119] U.S. Department of Homeland Security Agents then obtained a federal search warrant to examine these devices.[120] The defendant voluntarily provided a password for the iPhone 5S, but refused to provide passwords to decrypt the Mac Pro or hard drives.[121] The defendant also provided the passcode to unlock

110. *Id.* at 614.
111. *Id.* at 615.
112. *Id.*
113. *Id*. at 617 (Lenk, J., dissenting).
114. *Id.* at 620–22.
115. *Id.* at 622.
116. *See* United States v. Apple Macpro Comput., 851 F.3d 238, 248 (3d Cir. 2017).
117. 851 F.3d 238 (3d Cir. 2017).
118. *Id.* at 242.
119. *Id.*
120. *Id.*
121. *Id.*

the iPhone 6 Plus, but refused to provide a passcode for an application on that phone that contained encrypted files.[122]

Government forensic analysts discovered the Mac Pro password without the defendant's assistance and found on the internal hard drive one child pornography image as well as logs showing that the computer had been used to access known child pornography sites and to download thousands of known child pornography files.[123] Investigators also interviewed the defendant's sister, who stated that the defendant had shown her child pornography images from the encrypted external hard drives.[124] Based on this information, the government obtained an order under the All Writs Act requiring the defendant to produce the devices and hard drives in a fully unencrypted state.[125]

The magistrate judge denied the defendant's motion to quash the All Writs Act order.[126] The defendant subsequently appeared for a forensic examination at the Delaware County Police Department.[127] He produced the iPhone 6 Plus with all files decrypted, which included photographs of his four-year-old niece's genitals.[128] He claimed he could not remember the correct passwords to unlock the external hard drives and subsequently was held in contempt for failing to produce those drives in a decrypted state.[129]

The Third Circuit affirmed the denial of the motion to quash.[130] The Third Circuit noted that the Eleventh Circuit's decision in *In re Grand Jury Subpoena* would not require a different result because the evidence was sufficient to show that files existed on the encrypted devices and that the defendant could access those devices.[131] In a footnote, the Third Circuit also noted that the Government's knowledge of files on the encrypted devices might not reflect the proper inquiry under the foregone conclusion exception.[132] Instead, the court suggested, "a very sound argument can be made that the foregone conclusion doctrine properly focuses on whether the Government already knows the testimony that is implicit in the act of production" and that the relevant testimony is that

122. *Id.* at 243.
123. *Id.* at 242.
124. *Id.* at 248.
125. *Id.* at 243.
126. *Id.*
127. *Id.*
128. *Id.*
129. *Id.*
130. *Id.*
131. *Id.* at 248.
132. *Id.* at 248 n.7.

the defendant knows the passwords to decrypt the devices.[133] If the surrounding evidence shows that this testimony is a foregone conclusion, the exception might apply even absent any showing of what files the device might contain.[134]

2. Compelled Production of Biometric Identification Controlling Encryption

Other courts have distinguished passwords and biometric identification to unlock encrypted devices. In *Commonwealth v. Baust*,[135] a Virginia trial court held that production of a passcode to a cell phone is a testimonial act and that the foregone conclusion doctrine does not apply because the subject of the testimony is not about the existence and authenticity of documents on the phone, but rather is about the password itself.[136] The court noted: "[I]f the password was a foregone conclusion, the Commonwealth would not need to compel Defendant to produce it because they would already know it."[137] In contrast, the court held, "[t]he fingerprint, like a key . . . does not require the witness to divulge anything through his mental processes," and therefore the biometric identification could be compelled.[138]

Other courts have disagreed with this distinction. In *State v. Stahl*,[139] for example, a Florida appellate court questioned Justice Stevens's distinction in *Doe* between a key and a combination, and noted that surrendering a key to a strongbox or stating the combination to a strongbox lock has the same effect.[140] The court further questioned "the continuing viability of any distinction as technology advances" and suggested that the use of a passcode on a smart phone should not result in greater constitutional protection than the use of a "fingerprint as the passcode."[141] The court held that the foregone conclusion doctrine should apply if the State establishes three elements: (1) "it knows with reasonable particularity that the passcode exists"; (2) the passcode "is within the accused's possession or control"; and (3) the passcode "is

133. *Id.* The relevant testimony, according to the Third Circuit, could simply be "I, John Doe, know the password for these devices." *Id.*

134. *Id.*

135. 89 Va. Cir. 267, 2014 WL 10355635 (Va. Cir. Ct. 2014).

136. *Id.* at *4.

137. *Id.*

138. *Id.*; *cf.* State v. Diamond, 890 N.W.2d 143, 149–51 (Minn. Ct. App. 2017) (upholding order to produce fingerprint to unlock cellphone and distinguishing testimonial act of producing a password from non-testimonial act of supplying a fingerprint key), *aff'd*, 905 N.W.2d 870 (Minn. 2018).

139. 206 So. 3d 124 (Fla. Dist. Ct. App. 2016).

140. *Id.* at 134–35.

141. *Id.* at 135.

authentic."[142] The element of authenticity, the court suggested, would invariably be satisfied, because "[i]f the doctrines are to continue to be applied to passcodes, decryption keys, and the like, we must recognize that the technology is self-authenticating [because] no other means of authentication may exist."[143] Therefore, the court noted, "[i]f the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic."[144] In short, the court concluded, "[t]his is a case of surrender and not testimony."[145]

III. ENCRYPTION, SPEECH, AND TESTIMONY

A. *What Is "Testimony?"*

As discussed in Part II, the cases that have addressed compelled disclosure of encryption keys under the Fifth Amendment circle around the question whether an encryption key or password is a form of speech or communication. Case law does not explore the line between speech or communication and *actions* that are not speech or communication with any degree of philosophical depth, and commentators continue to dispute the distinction.[146]

Some scholars have sought to circumvent the question by grounding the Fifth Amendment right against self-incrimination in a right of privacy.[147] As Ronald Allen and Kristin Mace have noted, however, privacy based justifications "cannot explain why the privilege applies or when it does," since the government otherwise has a "right to every man's evidence," even if that evidence incriminates a family member or is embarrassing even if not incriminating.[148] In contrast, privacy questions are directly addressed by the Fourth Amendment's search and seizure limitations.[149]

The Fifth Amendment's privilege against self-incrimination, although involving underlying privacy interests, seems to concern a particular kind

142. *Id.* at 136.

143. *Id.*

144. *Id.*

145. *Id.* at 137; *see* Efren Lemus, Comment, *When Fingerprints Are Key: Reinstating Privacy to the Privilege Against Self-Incrimination in Light of Fingerprint Encryption of Smartphones*, 70 SMU L. REV. 533, 539–44 (2017).

146. *See, e.g.*, Ronald J. Allen & M. Kristin Mace, *The Self-Incrimination Clause Explained and Its Future Predicted*, 94 J. CRIM. L. & CRIMINOLOGY 243, 259 (2004) (noting that "[t]he Court has failed to provide a definition of 'testimony' that can explain its own cases").

147. *See id.* at 261.

148. *Id.* at 261–62 (quoting Kastigar v. United States, 406 U.S. 441, 443 (1972)).

149. *See* William J. Stuntz, *Self-Incrimination and Excuse*, 88 COLUM. L. REV. 1227, 1236 (1988).

of speech-act. Other scholars, along with most of the case law, therefore have focused on what comprises "testimony."[150]

Allen and Mace suggest the Supreme Court views "testimony" as an act of substantive cognition—"the product of cognition that results in holding or asserting propositions with truth-value."[151] They suggest that "[c]ognition 'involves the acquisition, storage, retrieval, and use of knowledge.'"[152] They apply their definition to the example of a suspect who is compelled to submit a polygraph examination while the examiner points to locations on a map where a murder victim's body might be buried, such that the suspect's physiological responses reveal the likely location of the body.[153] As Allen and Mace note, "there is perhaps universal agreement" that this evidence should be inadmissible under the Fifth Amendment to implicate the suspect in the murder, even though the suspect has not verbally spoken.[154] They suggest that their definition of "testimony" explains this intuition because the polygraph test records biometric responses that convey knowledge held by the suspect.[155]

Allen and Mace recognize that the foregone conclusion doctrine poses problems for this definition.[156] The act of producing a document involves cognition, and it seems unclear under their theory why any exception should be made for the Fifth Amendment testimonial protection of such an act just because the location and existence of the document is a foregone conclusion. They suggest the difference could arise from the *degree* of cognition required.[157] If the witness must exercise relatively minimal cognitive "efforts," such as when a relatively narrow subpoena describes as specific set of documents, there is less offense than when the witness must expend greater cognitive efforts to identify, locate, and gather documents potentially responsive to a broader subpoena.[158]

It is unclear, however, what Allen and Mace mean by cognitive "efforts" or whether such a concept has any scientific or philosophical purchase. Could we measure, say, the number of neuronal connections

150. One scholar who avoided the question of defining "testimony" without adopting a privacy-based rationale was William Stuntz. *See id.* at 1228. Stuntz argued that Fifth Amendment privilege is justified because it excuses witness from the temptation to commit perjury. *See generally id.* at 1228–29. This is a fascinating rationale for the privilege generally, but it does not seek to address, given the privilege exists, whether or when a foregone conclusion doctrine should apply to limit the privilege.

151. Allen & Mace, *supra* note 146, at 266.

152. *Id.* at 267 (quoting MARGARET W. MATLIN, COGNITION 2 (3d ed. 1994)).

153. *Id.* at 248–49.

154. *Id.* at 249.

155. *Id.* at 269.

156. *Id.* at 287–89.

157. *Id.* at 288–89.

158. *Id.*

used to respond to a narrow subpoena versus a broad subpoena? The notion of measuring neuronal questions, of course, is not realistic, but the point is that cognitive "effort" seems impossible to quantify. Moreover, even if some measure of cognitive "efforts" were possible, why would it matter to a definition of "testimony?" Relatively little cognitive effort, presumably, is expended in the response to a simple question such as, "Did you kill the victim—yes or no?" But a witness could not be compelled to answer such a question.

In his article *Testimony*, Michael Pardo discusses when a communicative act might comprise "testimony" based on the speaker's intent to convey knowledge.[159] Pardo's main concern in that paper is epistemology, or what counts as knowledge.[160] In the category of "natural testimony," Pardo notes, (1) "the speaker must intend a listener or an audience to believe that the speaker has competence, authority, or credentials to assert the proposition," and (2) "the content of the communicative act must be what conveys information to the hearer."[161] However, the actual hearer need not be the intended hearer, as in the case of a journal entry or diary later read by a third party.[162] It is enough that the speaker intends to convey the requisite authority to some specific audience and that the communicative act conveys information to whomever ultimately is the hearer.[163]

Pardo's article explores various "epistemic 'pathways'" through which natural testimony can generate knowledge, as well as "epistemic 'dead ends'" through which natural testimony sometimes fails to generate knowledge.[164] He suggests that the rules concerning formal, in-court testimony draw fruitfully on this epistemic account of testimony and seeks to clarify the problematic question of hearsay as well as various constitutional rules concerning testimony.[165] Concerning the Fifth Amendment, Pardo argues that the Court's distinction between "testimonial" and other acts first drawn in *Schmerber* fits his framework for what comprises "testimony."[166] An act can satisfy both of Pardo's two conditions whether it is in the form of a verbal statement or action.[167]

But the act of production doctrine cases, Pardo claims, "have analytically confused and misapplied certain aspects of the concept of

159. Michael S. Pardo, *Testimony*, 82 TUL. L. REV. 119, 120–21 (2007).
160. *See id.* at 125–32.
161. *Id.* at 130–31.
162. *Id.* at 131–32.
163. *Id.* at 131.
164. *Id.* at 139–44.
165. *Id.* at 144, 148, 164–65.
166. *Id.* at 178, 188.
167. *See id.* at 188.

testimony."[168] He is particularly critical of the Court's assumption under the foregone conclusion doctrine that the government's prior knowledge of the testimony's contents should matter.[169] Pardo concedes that "[i]f a speaker knows that the hearer already knows a proposition or has the same or superior evidence compared with the speaker, the speaker is not testifying to that proposition by asserting it" and further that there is no "testimony" when "a hearer who already knows the proposition or believes she has the same or superior evidence."[170] Therefore, under Pardo's definition, if the information is a foregone conclusion to the government, the act of production is not "testimony" vis-à-vis the government. However, Pardo argues, the government is not the only audience for the information. A judge or jury, for whom the information is not a foregone conclusion, is also an audience, and in many ways a more important one.[171] Pardo concludes: "[A]n act of production ought to be deemed testimonial for purposes of the Self-Incrimination Clause when, under the particular circumstances of the case, the act implicitly communicates information, and it is within the scope of the right when the content of the implicit communication was compelled and is incriminating."[172]

There are two problems with Pardo's treatment of this question. First, the distinction he draws between "the government" and a judge or jury as audiences for the communication is not so clear as he suggests. The "government," (i.e., the prosecution) acts on behalf of the State (i.e., the political community of *the people*), and the judge and jury *also* act on behalf of the state. The "audience," then, is always the state. The differences between the prosecutor, judge, and jury arise from their different *functions* within the machinery of the state. If some information presents itself as a "foregone conclusion" to the prosecution—that is, if some information is not natural "testimony" to the prosecution—it also *ipso facto* is a foregone conclusion and not formal "testimony" to the judge and jury. The prosecution, judge, and jury play different roles in the system and have different duties from each other. Both the judge and jury in their own ways serve as checks to protect accused citizens against the excessive zeal of prosecutors in an adversarial system, and the jury also serves as a check on judges. Nevertheless, as Judge Jack Weinstein

168. *Id.* at 184.
169. *See id.* at 186.
170. *Id.*
171. *Id.*
172. *Id.* at 188.

has noted, "[i]n a sense, the jury was, and remains, the direct voice of the sovereign, in a collaborative effort with the judge."[173]

Second, the question of what comprises the "content" of a "communicative act" is precisely what is at issue in an act of production. On this point the act of production and foregone conclusion doctrines attempt to demarcate between actions that are sufficiently information-laden to be considered "testimony" and those that are not.

Consider the compelled blood alcohol test in *Schmerber*.[174] The fact that the blood tested was the suspect's own blood, and the fact of the suspect's blood alcohol content level, is not anything the suspect intends to convey, and indeed the *suspect* does not "convey" it at all, unless the suspect is identical with the chemical information in his blood. There is no intent involved at all, unless the blood itself has some quality of agency or intentionality identical to the suspect's own agency and intentionality. The authority supporting the factual claims that a test was performed on this suspect's blood giving a particular blood alcohol level is the authority of the lab technicians who will testify about how the blood was drawn and what tests were conducted. The suspect is not required to testify about the authenticity of the blood sample or the results of the blood test.

The same is true for the production of papers or things known to be in a suspect's possession. The authority for authenticating that these papers were turned over by the suspect in response to a subpoena or warrant is inherent in the subpoena or warrant itself and in the fact that the papers were turned over. The suspect is not required to testify about the authenticity of the documents or the meaning of their contents. The authority for these facts resides in other information about the state of the world and the actions of other agents, not in any intention or communication of the suspect.

In a subsequent article, *The Epistemology of Testimony*, Pardo refines his discussion of these questions.[175] In that article, Pardo suggests that whether something is considered "testimony" depends on whether the defendant is serving as an "epistemic authority" for a proposition.[176] For example, in the case of a blood sample to determine blood type, Pardo suggests, the defendant is not serving as an epistemic authority as to

173. United States v. Khan, 325 F. Supp. 2d 218, 230 (E.D.N.Y. 2004); *cf.* Douglas A. Berman, *Making the Framers' Case, and a Modern Case, for Jury Involvement in Habeas Adjudication*, 71 OHIO ST. L.J. 887, 888 (2010).

174. Schmerber v. California, 384 U.S. 757, 758 (1966).

175. Michael S. Pardo, *Self-Incrimination and the Epistemology of Testimony*, 30 CARDOZO L. REV. 1023 (2008).

176. *Id.* at 1040.

blood type, so this kind of sample is not "testimony."[177] He suggests that "[o]ne does not have to posit distinct material and non-physical realms to see an epistemic difference between words and blood."[178]

This notion of "epistemic authority" is helpful, but in the age of DNA evidence, the line between "words and blood" might be fuzzier than Pardo suggests. Interestingly for the purpose of this paper, the Sixth, Seventh, and Ninth Circuits have held that *Schmerber* applies to blood tests to extract genetic information stored in a national database.[179] A person's DNA conveys far more information than a blood alcohol test, including, for example, the ability to place a person at a crime scene based on DNA samples from hair, blood, skin, semen, and the like left at the scene. A person's DNA also can communicate more definitive information in many ways than documents or things in that person's possession. DNA evidence can offer stronger "smoking gun" evidence than a smoking gun itself. If a person provides a sample of her blood (or, more likely, a mouth swab), implicitly acknowledging it is *her* blood, and the blood (or swab) contains genetic information highly specific to that individual, where does the epistemic authority lie? It seems impossible to stretch the concept of "testimony" to include DNA evidence, again unless we wish to reduce a person's agency, intentionality, and speech to his or her genetic code. Genes do not testify; people testify. This is why notions of epistemic authority must be tied to the concept of what comprises a communicative act. As Pardo suggests, in "testimony," a speaker makes "an *assertion*."[180] The concept of an "assertion" involves an intent to convey *information*.

The example of genetic information in relation to "testimony" is particularly apt to the discussion of decryption keys because DNA, like encryption keys and passwords, is a kind of "code." The question about the connection between "information" and "communication" is basic to information theory, which underlies modern computing technology. The following Section shows how information theory clarifies the foregone conclusion doctrine in relation to encryption keys and passwords. It further explores this difficult question as it has arisen in two other areas of law: the First Amendment and copyright law. Part IV then extends these insights to argue that neither encryption code nor passwords that

177. *Id.*

178. *Id.* at 1041.

179. United States. v. Reynard, 473 F.3d 1008, 1021 (9th Cir. 2007); United States. v. Bean, 214 F. App'x 568, 571 (6th Cir. 2007); United States v. Hook, 471 F.3d 766, 774 (7th Cir. 2006) (stating that "the information that is extracted from the blood, DNA, is another form of physical, genetic identification of an individual not unlike a photograph or fingerprint and is thus also not protected by the Fifth Amendment").

180. *Id.* at 1037.

protect encryption are forms of "speech" that could comprise testimonial acts.

B. *Encryption, Semiotics, and Information Theory*

It should be clear from the discussion of the Caesar Cipher in Part I above that the key "13" communicates nothing at all about the substance of the text "cynl vg ntnva fnz." Arguably, the number 13 in this context has no semantic content. The number 13 does not even say, "This message is encoded with a ROT13 cipher." A person who wants to use the number 13 as a key would already have to know (or guess) that this is a ROT13-encoded message. The number itself is nothing but the key that converts "cynl vg ntnva fnz" into the readable English message "play it again sam." On the other hand, arguably, to a person with at least some background in encryption—such as a user of an Internet bulletin board in which ROT13 is frequently employed—the number 13 itself *could* communicate that a certain kind of encryption is being used.[181]

In this regard, a subtle but very important distinction must be drawn between "language" and "information." *Language* refers to the syntax and grammar used to signify things or states of affairs. Philosophers have long recognized that there is a basic distinction between a "sign" (language) and something that is "signified" (information).[182] As the great philosopher and theologian Augustine of Hippo argued: "[A] sign is something which, offering itself to the senses, conveys something other to the intellect."[183] *Information*, in contrast, can be defined as the content of states of affairs embodied in "well formed, meaningful and truthful data."[184] That is, *information* is the content of states of affairs, which must be expressed in *language* to be understood by humans.[185] *Information* is the actual content of that which is signified, and *language* is the means by which signs pointing to the signified are constructed.

This dynamic raises interesting questions in metaphysics. Does the thing signified by a sign possess an actual existence? Is "information" in some sense a fundamental element of the cosmos, along with energy and matter? In Platonic and other metaphysically realist philosophy, echoed in the quote from Augustine above, there is an actual ideal realm to which

181. For a discussion of the use of ROT13 in early Internet Usenet groups see ROT13 on Wikipedia. *See ROT13*, WIKIPEDIA https://en.wikipedia.org/wiki/ROT13 (last visited Mar. 14, 2018).

182. *See Medieval Semiotics*, STANFORD ENCYCLOPEDIA OF PHILOSOPHY, § 1–2.1 (last edited on May 11, 2011), http://plato.stanford.edu/entries/semiotics-medieval/.

183. *Id.* at § 2.1 (quoting Augustine, De Doctrina Christiana, II.1.) (emphasis added).

184. *See Semantic Conceptions of Information*, STANFORD ENCYCLOPEDIA OF PHILOSOPHY, § 3.2.3 (last edited on Jan. 7, 2015), http://plato.stanford.edu/entries/information-semantic/.

185. *See id.*

signs refer and which provides the universal "form" of particular things in the world.[186] Much contemporary semantic theory, including much of the application of semantics to computer science and artificial intelligence, assumes that the sign and the signified are closely related—that, in some sense, the sign constructs the signified without any external referent such as the Platonic realm of "forms" or the Augustinian mind of God.[187]

Aside from these rich metaphysical questions, the close relation between sign and signified in computer code means that code is essentially arbitrary.[188] But if computer code is arbitrary, how can we (or the machine) know what is signified? As Kumiko Tanaka-Ishii notes, "[o]ne of the basic ways is to take an operational approach and judge the equivalence from input and output sets."[189] Since in computing terms "output" is a function of the machine, we could say that computer code is what it does. In this sense, computer code is not the message itself, even though code does cause computer machines to output messages.

At the same time, since the code is not the message, code that outputs a message can be disaggregated, compressed, or otherwise manipulated without destroying the message. This remarkable fact underlies all historic forms of cryptography as well as modern telecommunications technology.[190] A message in English—say, "Watson, come here, I need you"—can be converted into an information equivalent, such as electromagnetic waves or digital 0's and 1's, and this information equivalent can be compressed, chopped up, and transmitted or stored. The information equivalent can then be retrieved and run through a receiver that reproduces the original language.[191]

When this happens, no new "information" is being created. The state of affairs that the "information" encodes or that which is signified—the fact that Edison desires Watson to come to the lab—remains the same. In fact, modern information theory involves laws of the conservation of information, akin to the laws of the conservation of matter in physics. The

186. *See, e.g.*, KUMIKO TANAKA-ISHII, SEMIOTICS OF PROGRAMMING 54 (Cambridge Univ. Press 2010).

187. *See id.* The metaphysical belief that signs—"code"—construct reality is the instinct behind most kinds of Internet exceptionalism. *See* David W. Opderbeck, *Deconstructing Jefferson's Candle: Towards a Critical Realist Approach to Cultural Environmentalism and Information Policy*, 49 JURIMETRICS 203, 210, 239 (2009).

188. *See* TANAKA-ISHII, *supra* note 186, at 67.

189. *Id.*

190. *See Information*, STANFORD ENCYCLOPEDIA OF PHILOSOPHY, § 2.1, (Oct. 26, 2012), https://plato.stanford.edu/entries/information/.

191. *See id.*

notion of signal "loss," such as parts of a radio transmission or cell phone call that "drop out," relates to this conservation law.[192]

These semantic concepts from information theory do not sit entirely comfortably with the "linguistic turn" in contemporary analytic philosophy. The semantic concept of information assumes a sort of metaphysic in which "information" comprises a fundamental reality. This reflects the influence of logical positivism on early information theorists and cyberneticists such as Claude Shannon and Norbert Weiner.[193] The problem of language, however, was a key reason for the collapse of logical positivism.[194] The "sign" rarely, if ever, corresponds directly to the "signified" without context. For this reason, some philosophers of language, particularly those attracted to "speech-act theory," distinguish the act of speaking (the "illocutionary act") from the desired state of affairs the speaker intends to produce (the "perlocutionary act"). The focus shifts from the *speech* itself to *action*.[195]

The shift from speech to action has not been lost on legal theory, particularly in relation to statutory interpretation. In his book *Legal and Political Hermeneutics*, first published in 1837, Francis Lieber used the example of a "housekeeper" who gives some money to a "domestic" and tells the domestic to "fetch some soupmeat."[196] Lieber noted that this simple, everyday command includes within it at least eight other unstated commands (such as "fetch the meat for the use of the family and not for himself") that the domestic must incorporate into his interpretation of the primary command based on context and experience.[197]

The act of providing the password and decryption key necessary to unlock full disk encryption on a computer hard drive resides at the nexus between the positivistic-cybernetic information theories that underlie computer technology and the act-based theories of language that inform contemporary debates in the philosophy of language. This is why the problem in legal doctrine seems so vexing: is typing or speaking a password, or triggering the application of a coded decryption key, a form

192. *See* Claude Shannon, *A Mathematical Theory of Communication*, 27 BELL SYSTEM TECH. J. 379, 379 (1948).

193. For a discussion of logical positivism, see THE COLUMBIA HISTORY OF WESTERN PHILOSOPHY at 621–24 (Richard H. Popkin ed., Columbia Univ. Press 1999). For Weiner's germinal work, see NORBERT WIENER, CYBERNETICS, OR THE CONTROL AND COMMUNICATION IN THE ANIMAL AND THE MACHINE (M.I.T. Press 2d ed. 1961). For a discussion of Weiner's life, see FLO CONWAY & JIM SIEGELMAN, DARK HERO OF THE INFORMATION AGE: IN SEARCH OF NORBERT WIENER THE FATHER OF CYBERNETICS (Basic Books 2009).

194. *See, e.g.*, THE COLUMBIA HISTORY OF WESTERN PHILOSOPHY, *supra* note 193, at 624.

195. *See id.*

196. FRANCIS LIEBER, LEGAL AND POLITICAL HERMENEUTICS 28 (F.H. Thomas 3d ed. 1880).

197. *Id.* at 28–29. This example is discussed in a collection of materials on statutory interpretation in ESKRIDGE, FRICKEY AND GARRETT, CASES AND MATERIALS ON LEGISLATION: STATUTES AND THE CREATION OF PUBLIC POLICY 694–95 (West 4th ed. 2007).

of "speech" that could be testimonial and legally privileged, or is it a form of "action," like handing over a physical key, that in itself would not be considered testimonial speech? In the distinction between "privacy" and "testimony," the courts must confront a basic, almost mystical question at the intersection of semantic theory, philosophy of information, and computer science.

Indeed, as the next two Sections suggest, this problem is not entirely unique to the Fifth Amendment context—it is a basic problem for the law in the information age. Courts have also wrestled with the question whether certain kinds of performative acts or instructions, including the operation of computer code, are protected under the First Amendment or are subject to statutory copyright protection. The First Amendment and copyright cases provide some additional context for our discussion of whether forced decryption should be considered "testimonial" under the Fifth Amendment.

C. *"Speech" in the First Amendment Context*

Not all conduct that arguably contains some expressive content is considered protected "speech" under the First Amendment. In *Spence v. State of Washington*,[198] the Court addressed whether the modification (with a peace symbol) and upside-down display of an American flag in violation of a state flag desecration statute was a form of protected speech.[199] In concluding that this conduct was protected speech, the court considered four factors: (1) whether the act is "sufficiently imbued with elements of communication"; (2) whether the "context in which a symbol is used . . . give[s] meaning to the symbol"; (3) whether "[a]n intent to convey a particularized message" is present; and (4) whether "in the surrounding circumstances the likelihood was great that the message would be understood by those who viewed it."[200]

As might be expected, slippery guidelines such as these have been notoriously difficult to apply. For example, in *City of Dallas v. Stanglin*,[201] the Court considered whether a city ordinance that created "teenage" dance halls limited to persons between the ages of 14 and 18 violated the expressional association rights of those persons to associate with persons of other age groups. [202] The Court declined to extend First Amendment protection to "recreational dancing."[203] According to Justice Rehnquist, "[i]t is possible to find some kernel of expression in almost

198. 418 U.S. 405 (1974).
199. *Id.* at 406.
200. *Id.* at 409–11.
201. 490 U.S. 19 (1989).
202. *Id.* at 20.
203. *Id.* at 25.

every activity a person undertakes—for example, walking down the street or meeting one's friends at a shopping mall—but such a kernel is not sufficient to bring the activity within the protection of the First Amendment."[204]

The nexus between an ordinary function not considered "speech," such as walking to a shopping mall, and protected expression is particularly interesting in the context of computer code. The Supreme Court has never decided whether, or to what extent, computer code is a form of "speech" protected by the First Amendment, although some important federal appellate cases hold that computer code is a form of protected speech.

In *Junger v. Daley*,[205] for example, the Sixth Circuit held that export control restrictions on encryption software potentially could violate the First Amendment.[206] The court did not decide the merits, however, because the restrictions changed while the case was pending.[207] And in *Universal City Studios v. Corley*,[208] an important early case challenging the anti-circumvention provisions of the Digital Millennium Copyright Act, the Second Circuit held that computer code is a form of protected speech.[209] According to the Second Circuit, "[c]ommunication does not lose constitutional protection as 'speech' simply because it is expressed in the language of computer code."[210] The court noted that "[i]f someone chose to write a novel entirely in computer object code by using strings of 1's and 0's for each letter of each word, the resulting work would be no different for constitutional purposes than if it had been written in English."[211]

The categories of being a "witness" against oneself under the Fifth Amendment and "speech" under the First Amendment obviously are not coextensive. Many "speech" acts for First Amendment purposes would not entail being a "witness" against one's self (or, in the language of the modern case law, would not be "testimonial"). But if the relevant analogy is the lockbox key versus the lockbox combination, *Junger* and *Corley* seem potentially relevant. If computer code is merely functional and not expressive, it seems more like the lockbox key, whereas if computer code is expressive, it seems more like the combination.

---

204. *Id.*
205. 209 F.3d 481 (6th Cir. 2000).
206. *Id.* at 482.
207. *Id.* at 485.
208. 273 F.3d 429 (2d Cir. 2001).
209. *Id.* at 449.
210. *Id.* at 445.
211. *Id.* at 445–46. For further discussion of the relationship between source code, speech, and encryption, see Allen Cook Barr, Note, *Guardians of Your Galaxy S7: Encryption Backdoors and the First Amendment*, 101 MINN. L. REV. 301 (2016).

D. *"Expression" in Copyright Law*

Copyright law is another analogous area for our discussion of speech, testimony, and computer code. Copyright protects original works that are fixed in a tangible medium of expression.[212] U.S. copyright law has long recognized that computer code, including both human-readable source code and machine-readable object code, are "literary works" subject to copyright protection.[213] However, copyright extends only to original expression and not to any "idea, procedure, process, system, method of operation, concept, principle, or discovery."[214] The *function* of a computer program therefore is not susceptible to copyright protection.

The copyrightability of object code is particularly interesting for purposes of this Article. Computers operate using a binary language of 0's and 1's, called object code.[215] The 0's and 1's represent states in a circuit: 0 is "off" and 1 is "on."[216] Human beings generally cannot write or interpret object code.[217] Instead, human programmers employ a coding language, which produces source code. For example, some lines of source code instructing the system to produce a printout when the user responds affirmatively to a query might read:

<display>"Do you wish to print"
If <input> = "yes" then <print>

A program called a "complier" would translate this source code into object code, a sequence of 0's and 1's that would cause the computer to perform the specified functions.[218]

If object code is compiled by computers and is not readable by humans, how can it comprise copyrightable subject matter? An early case involving player-pianos, *White-Smith Music Publishing Co. v. Apollo Co.*,[219] laid the foundation for later doctrine.[220] The issue in *White-Smith*

212. 17 U.S.C. § 102(a) (2012).

213. *See, e.g.*, NATIONAL COMMISSION ON NEW TECHNOLOGICAL USES OF COPYRIGHTED WORKS, FINAL REPORT 1, 16 (1978) [hereinafter CONTU Report]; Apple Comput., Inc. v. Franklin Comput. Corp., 714 F.2d 1240, 1247–49 (3d Cir. 1983), *superseded by statute*, The Semiconductor Chip Protection Act of 1984, *as recognized in* Brooktree Corp. v. Advanced Micro Devices, Inc., 977 F.2d 1555 (Fed. Cir. 1992).

214. 17 U.S.C. § 102(b) (2012).

215. *See Apple Comput., Inc.*, 714 F.2d at 1243.

216. *Id.*

217. *Id.*

218. *Id.* This description still generally holds for many kinds of programming, but as discussed below, it can be misleading in modern programming environments.

219. 209 U.S. 1 (1908).

220. *See generally id.* at 1, *superseded by statute*, 17 U.S.C. § 102(b) (2012), *as recognized in Apple Comput., Inc.*, 714 F.2d at 1240.

was whether a player-piano roll was an infringing "copy" of the protected musical score.[221] Player-pianos employed cylinders of paper with perforations that caused the device's internal levers to play certain notes.[222] The master "recording" of perforations was created when a person played the notes on a piano rigged to make the corresponding perforations in a blank roll.[223] Human beings generally could not "write" or read these perforations.[224]

In *White-Smith*, Justice Day held that the rolls were not infringing "copies" under the 1907 Copyright Act.[225] In a concurrence, Justice Holmes questioned why a machine-readable reproduction should not be considered a "copy," but agreed that the question should be addressed to the legislature.[226] The significance of the case for contemporary copyright doctrine is that the 1909 Copyright Act clarified that "mechanical reproductions" of music are protected "copies." Then, the 1976 Copyright Act further clarified that a "copy" can include any "material object . . . in which a work is fixed . . . and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." Finally, the 1980 amendment based on the CONTU Report included computer programs within the definition of "copy."[227]

For copyright purposes, then, human expression that is rendered by machines into a format readable only by machines remains protectable expression both in its human-readable and machine-only-readable form. This seems to extend the First Amendment principles regarding computer software discussed in Section III.B above. Even when there is an intermediate step of machine "translation," the resulting information can be considered "expression," at least for the purpose of copyright law. By analogy, using a password to unlock a decryption key so that a disk's contents can be human-readable might represent a form of "testimonial" speech even though the mechanical process of "translation"—decryption—happens within the machine.

An interesting wrinkle in the copyright discussion of computer code is that the early cases describing how programming works—from source

221. *Id.* at 13–14.

222. *Id.*

223. *Id.* at 10.

224. *See id.* at 9–10, 18 (noting that the perforated musical rolls used by player pianos are created via "mechanical construction," and that such rolls cannot be read as musical compositions).

225. *Id.* at 18.

226. *Id.* at 20 (Holmes, J., concurring).

227. 17 U.S.C. § 101 (2012) (defining "copy" and "computer program"); Copyright Act of 1909, Pub. L. No. 60-349, 35 Stat. 1075, 1075–76 (1909) (extending Copyright protection to "mechanical reproductions" of music).

code, to a complier, to object code—are no longer entirely accurate.[228] For some kinds of coding languages, the source code is not usually compiled into object code, but instead is executed by an "interpreter."[229] A common example is JavaScript, which is employed on many webpages and is interpreted and run by web browsers.[230] Also, some programming environments, such as Microsoft Visual Basic, enable programmers to select and assemble pre-coded modules through a graphical user interface (GUI) instead of writing lines of source code.[231] In these kinds of environments, there is perhaps an even closer link between the human-readable and machine-readable iterations of the work.

IV. ENCRYPTION, THE SIGN, AND THE SIGNIFIED: WHY DISCLOSURE OF PASSWORDS OR DECRYPTION KEYS IS NOT TESTIMONIAL

These analogies from First Amendment and copyright law highlight the difficulty of classifying computer code in semiotic terms. In these domains, computer code can be a form of protected expression because it is a kind of language. Like any other language, computer code is viewed in First Amendment and copyright law through a somewhat naïve semiotic lens as a kind of sign that points relatively straightforwardly to some intelligible human signification. But the more computer code moves towards basic functionality, the less likely it is to be protected by law.

In this light, the apparent relevance of First Amendment cases, such as *Junger* and *Corley*, to the Fifth Amendment context dims.[232] In those cases, the speaker of computer code is the person who writes the code.[233] An end user of encryption software does not write any code. The password that unlocks a device using full disk encryption is not itself computer code, but triggers the *application* of computer code when the decryption key is applied to the encrypted data in relation to the encryption algorithm.

---

228. *See* Ed Felten, *Source Code and Object Code*, PRINCETON CTR. FOR INFO. TECH. POL'Y: FREEDOM TO TINKER (Sept. 4, 2002), https://freedom-to-tinker.com/2002/09/04/source-code-and-object-code/.

229. *Id.*

230. *See Overview of JavaScript*, http://web.stanford.edu/class/cs98si/slides/overview.html (last visited Feb. 27, 2018).

231. *See* Margaret Rouse, Visual Basic (VB), TECHTARGET http://searchwindevelopment.techtarget.com/definition/Visual-Basic (last visited Feb. 27, 2018); Derek Banas, *Visual Basic Tutorial 2017*, YOUTUBE (Nov. 30, 2016), https://www.youtube.com/ watch?v=3FkWddODLno.

232. *See supra* Section III.C.

233. *See, e.g.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429, 436–37 (2d Cir. 2001); Junger v. Daley, 209 F.3d 481, 483–84 (6th Cir. 2000).

Similarly, copyright protects only original expression, not ideas, processes, methods, or systems of operation.[234] This makes the issue of infringement interesting in computer software copyright cases. By definition, computer programs are designed to cause computers to perform some function. What aspect of computer code could be "expression" rather than an idea, process, method, or system of operation? In an infringement claim involving computer software, the court usually will seek to define various levels of "abstraction," from lines of code to structure and logic to general function, in order to filter out elements that are unprotectable before comparing the protectable elements with the allegedly infringing program.[235] As may be imagined, this is at best an imprecise exercise.

It is unlikely that an encryption key, algorithm, or related password could be considered protectable "expression" under any kind of abstraction-filtration-comparison analysis. The algorithm is a mathematical function, which can only be expressed in a particular way, and therefore is equivalent to the idea itself and is unprotectable under the "merger" doctrine.[236] The form of the key is dictated by the function of the algorithm.

Things get interesting here, because a strong encryption algorithm must be capable of generating very large numbers of unique keys; otherwise, any given collection of encrypted data would be subject to brute force attack employing a defined set of keys. It is possible that, with a large number of possible variations, the merger doctrine might not eliminate copyright entirely. It is doubtful, however, that any person could be considered the "author" of a randomly generated key for copyright purposes.

Like the First Amendment analogy, the copyright analogy demonstrates the difficulty of determining *what kind* of communication inheres in computer code, and more particularly, in encryption algorithms, keys, and associated passwords. As with the First Amendment analysis, the immediate functionality of this form of expression suggests that it would not be legally protected under copyright law. The random nature of machine-generated keys further argues against copyrightability. There is an undefined point at which computer code is no longer a sign that *points to* something signified, similar to language or "speech," but instead is a kind of "thing" in itself, similar to a tool, device, or key.

234. 17 U.S.C. § 102(b) (2012).

235. *See, e.g.*, Comput. Assoc's Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 706 (2d Cir. 1992).

236. *See, e.g.*, Kregos v. Associated Press, 937 F.2d 700, 705 (2d Cir. 1991) (stating that "expression is not protected in those instances where there is only one or so few ways of expressing an idea that protection of the expression would effectively accord protection to the idea itself").

This demonstrates that disclosure of an encryption algorithm or decryption key itself should not be viewed as testimonial "speech" under the Fifth Amendment. In semantic terms, handing over passwords and decryption keys is like handing over a physical key, even though speaking or typing a code accomplishes the act of "handing over." If the content of some computer code could itself convey a message that might incriminate a person, the Fifth Amendment privilege should apply. But this is unlikely and does not apply at all to encryption algorithms or decryption keys. This kind of code does not convey any message. It has no semantic content and is entirely functional. The forced disclosure of a decryption key, then, should not in itself implicate the Fifth Amendment.

But what about the forced disclosure of a biometric identifier or password that is tied to full disk encryption? Biometric identifiers such as fingerprints seem closest to the kinds of acts of production the *Fisher* Court said are not testimonial, including "traditional" blood samples.[237] Passwords seem different because they are "words," or at least strings of characters. As with fingerprints, however, the pass-"words" or character strings tied to full disk encryption convey no semantic content. They are entirely functional. Disclosing the password is very much like the physical act of handing over the lockbox key; the decryption key is very much like the teeth on the lockbox key, which fit into the mechanical locking mechanism, and the encryption algorithm is very much like the mechanical locking mechanism on the strongbox lock.

This semantic analysis suggests that the "foregone conclusion" doctrine should be viewed in this context not as an "exception" to the Fifth Amendment privilege, but as a tool that helps clarify what kinds of technological acts fall on the side of "function" rather than "testimonial communication." The cases that have ordered disclosure of passwords or encryption keys have found or assumed the action was testimonial but applied the foregone conclusion doctrine as an exception.[238] The results in those cases were correct, but a more careful review of how passwords and biometric identifiers function in relation to encryption could strengthen the analysis.

In a few cases, courts have refused to apply the foregone conclusion doctrine to forced decryption based on the Eleventh Circuit's reasoning in *In re Subpoena Duces Tecum Dated March 25, 2011*.[239] Other courts should reject the Eleventh Circuit's reasoning because, as the discussion of full disk encryption in Part I above demonstrates, that court made a fundamental mistake concerning the nature of encrypted computer

237. *See* Fisher v. United States, 425 U.S. 391, 408 (1976).

238. *See supra* Section II.B.

239. *See, e.g.*, SEC v. Huang, No. 15-269, 2015 WL 5611644, at *3–4 (E.D. Pa. Sept. 23, 2015) (relying on *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012) in declining to apply the foregone conclusion doctrine).

"files." The Eleventh Circuit panel's failure to understand basic computer technology fatally undermines its legal analysis of both the non-testimonial nature of computer encryption keys or passwords and the "foregone conclusion" rule.

The Eleventh Circuit seemed to suggest that a computer "file" must contain semantically meaningful information—that the 0's and 1's must signify some meaningful concept.[240] A "file," however, is not a component of a "language." A file is merely a kind of container, which may or may not hold documents encoded with some semantic meaning, and a computer "file" is simply any specific set of data stored on a computer.[241] Therefore, the "random characters" placed on the hard drive by the TrueCrypt software *were* computer "files," contrary to the court's conclusion. Production of the encryption key or password would merely have allowed the government to decrypt those files that were more than random strings of characters, or at least to determine that none of the computer files contained meaningful information.[242]

The Eleventh Circuit's misunderstanding of computer technology was compounded by its misplaced reliance on Justice Stevens' opinion in *Hubbell*.[243] Justice Stevens' concern in *Hubbell* related to the requirement that the defendant comb through large numbers of documents and identify specific documents that might respond to the subpoena, when the government had no prior reason to believe that the documents might exist or be under the defendant's control.[244] In forced decryption cases, in contrast, the government already knows the *hard drive* or other computer storage device exists and is under the suspect's control; that the hard drive or storage device is encrypted; and that the suspect possesses the password or key necessary for decryption. If the underlying concern is that the search warrant, subpoena, or other process used to obtain the hard drive or storage device was overly broad, that issue properly falls under

240. *See In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d. at 1346.

241. *See File*, MERRIAM-WEBSTER DICTIONARY, http://www.merriam-webster.com/dictionary/file ("c (1) : a collection of related data records (as for a computer) (2) : a complete collection of data (such as text or a program) treated by a computer as a unit especially for purposes of input and output"); *File*, OXFORD DICTIONARY, http://oxforddictionaries.com/definition/english/file ("1.2 *Computing* A collection of data, programs, etc. stored in a computer's memory or on a storage device under a single identifying name"); *File*, FREE DICTIONARY, http://www.thefreedictionary.com/file ("3. a collection of related computer data or program records stored by name").

242. *See* Dan Terzian, *Forced Decryption as a Foregone Conclusion*, 6 CALIF. L. REV. CIR. 27, 35 (2015) (noting that "contrary to [the Eleventh Circuit's] conclusion, the government always knows that an encrypted hard drive has unencrypted files").

243. *See In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d at 1342, 1347.

244. *See* United States v. Hubbell, 530 U.S. 27, 44–45 (2000).

the Fourth Amendment privacy domain. Disclosure of the password or decryption key only reveals facts about the suspect's control over those functional items, not about what the encrypted storage media does or does not contain.

Consider the following example: a suspect in a tax fraud case admits that an *unlocked* filing cabinet in his office contains "files" that belong to him. The government obtains a grand jury subpoena requiring the suspect to turn over the file cabinet. The suspect argues that he should not be required to turn over the filing cabinet because this would comprise a testimonial admission concerning his control over the documents in the files. Under *Fisher*, this scenario clearly falls under the foregone conclusion exception.[245]

But what if the suspect argues that he should not be required to turn over the filing cabinet because all the files are empty—they are nothing but manila folders that contain no writing and no documents of any kind? This should utterly undermine, not support, any Fifth Amendment argument. If the defendant's argument is truthful, he would be required to hand over some physical objects—a filing cabinet and some manila folders. Production of these physical items would not be considered testimonial under the Supreme Court's jurisprudence, and the suspect's possession and control of the items would be a foregone conclusion. The suspect might have an objection to the subpoena based on scope, burden, or relevance, but these are not Fifth Amendment privileges.

Assume further that the government believes the suspect is lying about the folders being empty. The government believes, correctly, that the folders contain records relating to the alleged tax fraud. Should the subpoena be quashed because both the existence and content of the documents could be incriminating given the suspect's lie about the file cabinet's contents? This would be an obviously incorrect, indeed bizarre, result. In response to a subpoena to produce files, a suspect would only need to claim the files are "empty" to be relieved of any obligation of production. The foregone conclusion exception would be gutted if it could be avoided through a simple lie.

Imagine instead that the suspect produces the physical file cabinet, which is filled with manila folders containing sheets of paper covered with seemingly random characters. The suspect admits that he employs a crude encryption system that uses a cardboard "mask" with cut outs in a pattern. When placed over the pages filled with seemingly random character strings, the mask will reveal only the letters intended to be read as part of a message. But the suspect claims that some or all of the files in this cabinet really contain only random characters, without any messages that could be revealed by the mask. In fact, this is part of the

245. *See* Fisher v. United States, 425 U.S. 391, 407–08 (1976).

genius of his filing system, because an unwanted inquirer would need to expend an enormous amount of time trying to discover which, if any, of the files contain pages with messages. It seems clear that the foregone conclusion doctrine would apply under these circumstances. There is no doubt that the file cabinet exists, that it contains files, that the files contain documents that may or may not convey meaningful semantic content, and that all of this is under the custody and control of the suspect. Turning over the files is an act of production, not of testimony.

In the example that opened this string of hypotheticals, we specified that the suspect's file cabinet was *unlocked*. If the cabinet was locked, should that change the analysis of any of the hypotheticals under the foregone conclusion exception? In addition to the cabinet itself, the government must obtain the physical key or lock combination (depending on the kind of lock) from the suspect. The issue here is not what, if anything, the file cabinet contains, but rather whether the suspect possesses or knows the key or combination. Since the suspect admitted that he uses the cabinet to store "files," regardless of what those "files" might contain, the suspect's possession and control of the key or combination is a foregone conclusion. This suggests that the Third Circuit's comment in *Apple Macpro Computer* was apt: the relevant testimony would be "'I, John Doe, [have the key or] know the [combination] for [this filing cabinet].'"[246] Even more directly, if the suspect turned over the key or combination, this would comprise an act of surrender, not of testimony. Although both the teeth on the key and the characters in the combination function as types of code, neither are signs that signify any meaning beyond their function. The same is true of passwords and biometric identifiers that access decryption keys.

CONCLUSION

Encryption is an ancient technology that has become widely available and enormously powerful in the computer age. It is both necessary to contemporary life and dangerous. While encryption enables free commerce and free speech, it also allows criminals an uncrackable safe haven—a kind of digital Tortuga for online piracy.[247] Courts now regularly must decide whether compelled disclosure of passwords or decryption keys violates the Fifth Amendment privilege against self-incrimination. Neither a password, nor a biometric identifier that activates a decryption algorithm, nor the algorithm itself, comprises testimonial speech. Handing over a password, biometric identifier, or decryption key is akin to handing over a physical key, which is not

246. United States v. Apple Macpro Comput., 851 F.3d 238, 248 n.7 (3d Cir. 2017).

247. Tortuga is a Caribbean Island made famous as a pirate stronghold in the Pirates of the Caribbean movies. *See Tortuga*, FANDOM: POTC WIKI, http://pirates.wikia.com/wiki/Tortuga (last visited Mar. 12, 2018).

ordinarily a testimonial act under the Supreme Court's Fifth Amendment jurisprudence. The foregone conclusion doctrine should be employed in these cases not as an exception to the Fifth Amendment privilege, but to clarify that compelled decryption is an act of production and not a testimonial act. Courts that have held otherwise have not properly understood what encryption is or what it does.