Harvard Journal of Law & Technology
Volume 32, Number 1 Fall 2018

COMPELLED DECRYPTION AND THE FIFTH AMENDMENT: EXPLORING THE TECHNICAL BOUNDARIES

*Aloni Cohen & Sunoo Park**

TABLE OF CONTENTS

---

* This Article is a joint work to which the authors contributed equally. It was written while both authors were Ph.D. candidates in computer science at MIT. Aloni Cohen is currently a Ph.D. candidate at the MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) and an Affiliate of the Berkman Klein Center for Internet and Society at Harvard University. Sunoo Park received her Ph.D. at MIT (CSAIL) and is now a researcher at the MIT Media Lab, a J.D. candidate at Harvard Law School, and an Affiliate of the Berkman Klein Center for Internet and Society. Both authors' doctoral research specializes in cryptography with a particular interest in the interaction of technology and the law.

The authors are grateful to Daniel J. Weitzner, David Vladeck, Ronald L. Rivest, Jonathan Zittrain, Paul Ohm, Ryan Corbett, and discussants at the Privacy Law Scholars Conference 2018 — particularly Sharon Bradford Franklin and Steven Bellovin — for their advice and support for the writing of this Article. They are also grateful to Philip and Stephen Heymann for sparking their interest in this research project, and to their doctoral advisor Shafi Goldwasser for her ongoing support of their research endeavors.

I. INTRODUCTION

More than seventy five percent of Americans own smartphones today, and that percentage has more than doubled in the last seven years.[1] Passcode- and fingerprint-based encryption are common measures to shield one's device data from prying eyes, whether on a smartphone or on other popular devices such as tablets and laptops. An average user will likely face a short menu of choices during device setup, which offers to protect their phone with a passcode, or with a fingerprint, or not at all.[2] Among the encryption options available, many users may make their choice based largely on convenience, little surmising their decisions' potential implications on their legal rights.

However, the legal ramifications of this choice are significant: in many cases, courts have held that the government may compel *finger-*

1. *Mobile Fact Sheet*, PEW RES. CTR (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile [https://perma.cc/H5FJ-U7TP]. In the words of Chief Justice Roberts, modern cell phones are "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." Riley v. California, 134 S.Ct. 2473, 2484 (2014).

2. Another common option available on Android phones is to require the user to draw a "pattern" on the screen, rather than enter a passcode. *See Lock & Unlock Your Android Device*, GOOGLE: ANDROID HELP, https://support.google.com/android/topic/7651299?hl=en&ref_topic=7340889 [https://perma.cc/MSB9-QJWN]. This Article does not further discuss pattern-based protection, as it is not meaningfully distinguishable from passcode-based protection for the purposes of this Article.

print-based device unlocking in the course of a criminal investigation, but whether the government may compel *password-based* unlocking has been more dependent on the specific circumstances of the case.[3] A legally significant distinction is that unlocking a phone with a fingerprint is a physical, rather than a mental, act.[4]

The extent of an individual's protection against government access to her encrypted data has become rapidly more relevant of late — to both device users and governmental authorities — with the increasing use not only of devices that store large amounts of data, but also of encryption of data stored on and communicated between devices.[5] Over the last decade, digital information storage and encryption have become far more common, and in many settings, ubiquitous. Encryption of digital data has gone from being used only by the technically expert to secure especially sensitive information, to being used routinely (and often, unwittingly) by ordinary people to protect the contents of their computers, tablets, communications, and — especially — smartphones.[6] Naturally, in the course of these developments, encrypted digital information has become an item of increasingly frequent interest to law enforcement during investigations.[7]

---

3. *See infra* Part IV.

4. *See infra* Section IV.E.

5. Encryption by default is an increasingly common feature on popular devices. *See, e.g.*, *iOS Security: iOS 12*, APPLE (Sep. 2018), https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf [https://perma.cc/9FKR-Q7JV] (a detailed technical guide on security in Apple iOS); *How To: Encrypt Your iPhone*, ELEC. FRONTIER FOUND. (last updated Mar. 26, 2018) https://ssd.eff.org/en/module/how-encrypt-your-iphone [https://perma.cc/SYV6-W46A] (providing a brief non-technical guide to iPhone encryption over multiple iOS versions); *Encrypt Your Data*, GOOGLE: NEXUS HELP, https://support.google.com/nexus/answer/2844831?hl=en [https://perma.cc/4S3W-LRA9] (discussing Android smartphones); *Use FileVault To Encrypt the Startup Disk on Your Mac*, APPLE (Dec. 18, 2017), https://support.apple.com/en-us/HT204837 [https://perma.cc/FG5V-UPBW] (discussing Apple computers); Alex Hern, *Apple Defies FBI and Offers Encryption by Default on New Operating System*, GUARDIAN (Oct. 17, 2014, 1:57 PM), https://www.theguardian.com/technology/2014/oct/17/apple-defies-fbi-encryption-mac-osx [https://perma.cc/N9GD-7SYU] (discussing Apple computers). Messaging apps that encrypt communications by default are also increasingly common. *See, e.g.*, *End-to-End Encryption*, WHATSAPP, https://faq.whatsapp.com/en/android/28030015/?category=5245250 [https://perma.cc/P28H-XDBQ]; *Fast, Simple, Secure*., SIGNAL, https://signal.org [https://perma.cc/P2AX-E36H].

6. *See, e.g.*, JAMES A. LEWIS, DENISE E. ZHENG & WILLIAM A. CARTER, CSIS TECH. POL'Y PROGRAM, THE EFFECT OF ENCRYPTION ON LAWFUL ACCESS TO COMMUNICATIONS AND DATA 2–6 (2017) https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/encryption/csis_study_en.pdf [https://perma.cc/PLR5-D5T5].

7. *See, e.g.*, James B. Comey, Director, Fed. Bureau of Investigation, Expectations of Privacy: Balancing Liberty, Security, and Public Safety, Address before Center for the Study of American Democracy Biennial Conference (Apr. 6, 2016), https://www.fbi.gov/news/speeches/expectations-of-privacy-balancing-liberty-security-and-public-safety [https://perma.cc/6SYY-UQB5]; THIRD REPORT OF THE MANHATTAN DISTRICT ATTORNEY'S OFFICE ON SMARTPHONE ENCRYPTION AND PUBLIC SAFETY 1–5, 7, 14–17 (2017), https://www.manhattanda.org/wp-content/themes/dany/files/2017%20Report%20of%20the

The use of encryption has been portrayed by governmental authorities as particularly problematic for law enforcement because, depending on the encryption method used, it may be infeasible for law enforcement to obtain desired data pursuant to a warrant or other authorization, even when its agents have access to an encrypted version of that data — whether a digital copy of an encrypted file or physical possession of a device on which encrypted data is stored.[8] In the context of more traditional physical measures such as safes and bank vaults, the government has the capability, at least in principle, to break in by force in the case of non-compliance by the safe owner (provided that the government knows of the safe's existence and location). In contrast, a "brute force" approach to decryption would, if the encryption were configured appropriately, take far longer than a human lifetime, even using the best technology available today.[9]

The issue of encryption was brought rather dramatically into the public limelight in early 2016, when the FBI sought to access the encrypted phone of one of the culprits of the December 2015 San Bernardino shooting, who was killed during the attack.[10] In order to retrieve the contents of the phone, the FBI wanted Apple to create or to enable installation of bespoke software to circumvent the security protections built into all of its iPhones.[11] Central to the publicity around that case were the government's stirring motive of investigating the nation's deadliest mass shooting in three years and Apple's impassioned public rebuttal of what

---

%20Manhattan%20District%20Attorney%27s%20Office%20on%20Smartphone%20Encryption.pdf [https://perma.cc/XNP8-MV4J] [hereinafter THIRD REPORT].

8. *See, e.g.*, Comey, *supra* note 7; THIRD REPORT, *supra* note 7.

9. *Cf.* CHRISTOF PAAR & JAN PELZL, UNDERSTANDING CRYPTOGRAPHY: A TEXTBOOK FOR STUDENTS AND PRACTITIONERS 7–8 (2010) (explaining the "brute force" approach). This observation has led the FBI to highlight the increasing use of encryption as causing its law enforcement information-gathering capability to "go dark," and the catchphrase "going dark" has since crept into the vernacular of the debate over law enforcement access to encrypted information. *See, e.g.*, Matt Tait, *Decrypting the Going Dark Debate*, LAWFARE (Oct. 17, 2007, 10:00AM) https://www.lawfareblog.com/decrypting-going-dark-debate [https://perma.cc/8LYN-CEU2].

The authors agree with Peter Swire's opinion that the "going dark" analogy can be misleading in the following way: "The idea of 'going dark' is that law enforcement has lost something — they used to be able to see something, and now it is dark. But that is not what has happened. Not so long ago, there were no text messages — in almost all instances, daily communications never created a record of content, because we spoke to someone in our presence, or called someone on a non-wiretapped phone." *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy Before the S. Comm. on the Judiciary*, 114th Cong. 10 (2015) (statement of Peter Swire, Huang Professor of Law and Ethics, Scheller College of Business, Georgia Institute of Technology), https://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Swire%20Testimony.pdf [https://perma.cc/UJ53-RCUZ].

10. Alina Selyukh, *A Year After San Bernardino and Apple-FBI, Where Are We on Encryption?*, NPR (Dec. 3, 2016), https://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption [https://perma.cc/HJL7-Z3DE].

11. *Id.*

it argued was a demand too sweeping to be compatible with responsible security practices and individual privacy rights.[12]

The FBI-Apple conflict has, for better or for worse, become a cornerstone of the public's familiarity with the debate over government access to encrypted data. This Article examines a legally very different scenario, in which the owner of some data, rather than the device manufacturer, is the target of government compulsion.

The focus of this Article is compelled decryption: the decryption of — or provision of the means to decrypt — encrypted data by a person having control thereof, in response to a governmental demand pursuant to a criminal investigation. Specifically, this Article examines the Fifth Amendment protection against compelled self-incrimination, as it applies to governmental orders compelling a target of an investigation to assist in the decryption of specific encrypted data.[13]

Unlike prior work, this Article presents a wide variety of technological variations that could further complicate the compelled decryption doctrine. Each technology presented in the Article challenges a different facet of the doctrine, highlighting the sometimes fragile technological assumptions that courts have made. The type of anticipatory approach to technological changes that this Article takes — including preemptive consideration of the implications that plausible technological variations would have on case analyses — is essential in order to develop robust doctrine that will remain unequivocal and relevant over time. While technical considerations contribute only so much to a real case's eventual outcome, a nuanced understanding of the interplay between technology and legal doctrine is integral to arriving at robust decisions going forward.

This Article begins by establishing the relevant technical and legal foundations. It starts with a brief overview of encryption in Part II, and then describes the relevant legal doctrine including act-of-production testimony and the related foregone conclusion analysis in Part III.

Part IV reviews the patchwork of court decisions regarding compelled decryption, and presents the cases according to a new taxonomy

---

12. *Compare* Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), https://www.apple.com/customer-letter [https://perma.cc/4JZE-Z2E3] *with* Government's Motion to Compel Apple Inc. to Comply With This Court's February 16, 2016 Order Compelling Assistance in Search, In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 5:16-cm-00010-SP (C.D. Cal. Feb. 19, 2016), ECF No. 1; *see also* Arash Khamooshi, *Breaking Down Apple's iPhone Fight With the U.S. Government*, N.Y. TIMES (Mar. 21, 2016) https://www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html [https://perma.cc/9QXA-2NM6].

13. For a discussion of Fourth Amendment issues, which are outside the scope of this article, see generally Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?"*, 33 CONN. L. REV. 503 (2001).

that identifies four archetypal categories that depend on the nature of the compelled act. In "reveal-the-password cases," the target must reveal a password. In "use-a-fingerprint cases," the target must use a fingerprint (e.g., by placing it on a device). In "enter-the-password cases," the target must enter the password into a device. Finally, in "produce-the-decrypted-contents cases," the target must furnish some data in unencrypted form. Each of these types of compelled act aims ultimately to gain the government access to data it seeks, in unencrypted form.

The circumstances under which decryption can be compelled have been broached by various courts as cases have arisen, but the precedent to date does not give rise to a consistent unified theory, and legal scholars are not in agreement about how these cases should be decided. To better focus on technological aspects of compelled decryption, this Article presents the authors' view of the evolving doctrine and omits much of the ongoing legal debate.

Part V turns from the factual variations of past cases and examines a number of technological variations that may, in principle or in practice, present themselves in the future. This Part explains a number of technologies and discusses their interaction with the compelled decryption doctrine. Part V is both technical and legal, concerning both the limits of technology and the foregone conclusion doctrine.

Part VI reflects on the compelled decryption doctrine and the collection of technological variations taken as a whole. Together, they suggest that while the doctrine sometimes turns on non-obvious technological details in surprising ways, with careful consideration of both technology and precedent it can be applied in a consistent manner. Consistency is but one requirement of a desirable doctrine, and is necessary, but not sufficient, to support coherence or desirability in a normative sense. By focusing on consistency, the Article's analysis establishes a baseline and leaves open a number of questions about the desirability of the compelled decryption doctrine more broadly.

Part VII discusses existence, a concept central to the foregone conclusion doctrine as applied to compelled decryption cases to date. The nature of existence of digital data is meaningfully different from the nature of existence of a physical document or object, and this distinction becomes even more nuanced when encryption is involved. The goal of Part VII is to provide a precise but accessible description of encryption technology as it relates to the notion of existence, and it may also serve to accentuate some challenges of applying precedent established in the physical domain to digital information.

***

It is important to consider the significance of analyzing and clarifying the compelled decryption doctrine — and, indeed, encryption law more generally — in the broader context of how past, present, and future cases are treated, and how their treatment may affect the incentives of societal actors and infrastructures over time. A continued lack of clarity regarding how encryption fits under Fifth Amendment protection against self-incrimination will compound the law enforcement challenges presented by cryptography. Security researchers will develop tools that may hinder compelled decryption, whether in response to the lack of clarity of the scope of Fifth Amendment protections, or as a natural side effect of their efforts to develop secure technologies more generally. Some, like the technologies proposed in this Article, may be designed as proofs of concept, to constructively illustrate the potential pitfalls or corner cases that the existing precedent might unsatisfactorily address. Others may be designed and deployed as general-purpose encryption tools or as concerted attempts to hinder law enforcement access to data, whether for criminal purposes or with benign intentions to promote civil liberties and the freedom to conduct ephemeral and private communications. While it may be possible to somewhat curb or make difficult the use of such technologies, it will likely be effectively impossible to eradicate or outlaw their use by the technically knowledgeable and determined.[14] Consolidating the compelled decryption doctrine would lay essential groundwork to begin addressing the reality that alternative technologies exist and will continue to be developed, and discussing where such technologies, in their turn, would fit into the doctrinal framework.

Furthermore, a continued lack of clarity on the scope of self-incrimination doctrine in the context of compelled decryption will lead to unpredictable and inconsistent results. While this may be true in any emerging area of law, the complexity of the technology involved in compelled decryption cases will exacerbate this outcome. The rapid pace of ongoing technological change may additionally lead to sustained unpredictability and inconsistency over a long period, especially if the nature of technological change is not taken explicitly into account as the doctrine develops. Moreover, the often emotionally charged nature of compelled decryption cases — frequently involving child pornography[15] — has the potential to exert undue pressure on law enforcement to find any way to access the encrypted files, without affording the leisure

14. For example, a technologically knowledgeable and determined person with access to today's publicly available literature on cryptography could, even if no such technologies were available to be obtained from external sources, simply write a computer program to implement those technologies herself. Indeed, if she were sufficiently technologically knowledgeable, determined, and creative, she could figure out how to create such technologies even without the help of the existing cryptography literature.

15. *See generally* cases cited *infra* Part IV.

to consider the larger legal and technological context, including wider possible repercussions for more commonplace applications of encryption and related technologies.

Encryption is a well-established technology that is widely used, often in contexts where it provides substantial societal benefit; it has become a vital part of the infrastructure underlying commerce, communications, data protection, and security.[16] For example, encryption is used billions of times a day, often unwittingly, for everyday tasks such as online shopping, or indeed, visiting any website whose address begins with https://.[17] The information protected by encryption pertains to countless individuals, organizations, and technological systems, and pervades the private and public sectors. The implications of compelled decryption doctrine need to be considered not only in the immediate context of criminal cases involving encrypted data, but also in the broader environment of encryption as a multi-purpose technology that has the potential to reap great societal benefit if we can strike the right balance so that it is not unduly fettered.

II. BRIEF BACKGROUND ON ENCRYPTION

An encryption algorithm is a procedure that, given a piece of information[18] (sometimes called a "plaintext") and a password (sometimes called a "secret key"),[19] produces an encryption (sometimes called a "ciphertext").[20] A decryption algorithm is a procedure that, given an en-

16. *See, e.g.*, Bruce Schneier, *Why We Encrypt*, SCHNEIER ON SECURITY (June 23, 2015), https://www.schneier.com/blog/archives/2015/06/why_we_encrypt.html [https://perma.cc/B2QR-59CA]; Andi Wilson Thompson, *The Human Rights Benefits of Encryption*, NEW AM. (Mar. 2, 2015), https://www.newamerica.org/oti/blog/the-human-rights-benefits-of-encryption [https://perma.cc/V59C-NRDC].

17. *See generally HTTPS Encryption on the Web*, GOOGLE: TRANSPARENCY REPORT https://transparencyreport.google.com/https/overview?hl=en [https://perma.cc/N4M4-CAC8].

18. In general, encryption can be applied to any piece of digital information. Typically, in practice, it is applied either to specific files or folders on a computer, or to an entire disk drive. Most encryption cases considered in this Article feature disk encryption rather than file encryption. File encryption may introduce interesting complexities into compelled decryption cases — for example, if any specific knowledge of encrypted contents is helpful to the government's case, then focusing on specific files may be to its benefit. This Article does not examine such possibilities in further detail.

19. Technically, the terms "password" and "secret key" are not synonymous, though for the purposes of this Article they may be treated as synonymous except where (rarely) otherwise indicated. For more discussion, see *infra* note 21.

20. This terminology can be found in any standard cryptography textbook. *See, e.g.*, JONATHAN KATZ & YEHUDA LINDELL, INTRODUCTION TO MODERN CRYPTOGRAPHY 52 (Douglas R. Stinson ed., CRC Press 2d ed., 2015). A curious reader seeking a less technical introduction to the concepts of encryption and decryption may be interested in ELLA DEON LACKEY, RED HAT CERTIFICATE SYSTEM COMMON CRITERIA CERTIFICATION 8.1, ch. 1 (2012), https://access.redhat.com/documentation/en-US/Red_Hat_Certificate_System_

cryption and a password,[21] produces the original piece of information (i.e., the plaintext).[22]

Encryptions in the absence of the correct password reveal no information about the underlying plaintext.[23] In particular, it is infeasible to determine whether a ciphertext is an encryption of meaningful information, or of meaningless information.[24] In many cases, it may even be unclear whether a piece of data is indeed an encryption of something, or if it is just an unstructured random-looking file that cannot be decrypted to any plaintext at all (even a meaningless one).

It is important that the password be very difficult to guess:[25] otherwise, by simply trying several guesses of the password, it would be possible to decrypt with a reasonable chance of success. One way to make the password very hard to guess is to choose it at random from a very large number of possibilities. Roughly speaking, the larger the number of possible passwords, the stronger the security provided by encryption. For example, if the password is a thirty-character alphanumeric string,[26] then the number of possible passwords is:

$$(26 + 26 + 10)^{30} =$$
$$591{,}222{,}134{,}364{,}399{,}413{,}463{,}902{,}591{,}994{,}678{,}504{,}204{,}696{,}392{,}694{,}759{,}424.$$

Common_Criteria_Certification/8.1/html/Deploy_and_Install_Guide/Introduction_to_Public_Key_Cryptography.html#Introduction_to_Public_Key_Cryptography-Encryption_and_Decryption [https://perma.cc/WT5V-64FH].

21. This Article consistently assumes that the key used for encryption is the same as that used for decryption. This is not true of all encryption schemes, but it is true of the category of encryption schemes pertinent to this Article: that is, encryption schemes that are used for device encryption. The category of encryption schemes where the encryption and decryption keys are the same is called "symmetric-key" or "secret-key" encryption schemes. In contrast, in "public-key" encryption schemes, the keys used for encryption and decryption are distinct, and only the decryption key needs to be kept secret.

22. *See, e.g.*, KATZ & LINDELL, *supra* note 20, at 52; LACKEY, *supra* note 20, at ch. 1.

23. This requirement of "revealing no information" is, in the cryptography literature, expressed as a precise mathematical definition. Intuitively, the requirement says that for an observer who is given a ciphertext without the corresponding secret key, the chance that the observer will correctly guess the underlying plaintext is no better than if the observer were guessing a plaintext totally at random. The formal version of the requirement is beyond the scope of this Article, but interested readers with some technical background may wish to search for "semantic security" in any standard cryptography textbook. *See generally* KATZ & LINDELL, *supra* note 20, at 43–103.

24. For instance, a file containing only zeros.

25. For a more detailed discussion of the problems created by easy-to-guess passwords, see generally ROSS J. ANDERSON, SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED 31–52 (2d ed. 2008).

26. Alphanumeric means consisting of the letters A–Z, a–z, and digits 0–9.

It would take a prohibitively long time for any publicly known computing technology to try decrypting with that many different passwords.[27]

Employing analogies to explain these complex, technical processes poses significant challenges. It is common to analogize data encrypted under a secret key to a document in a safe locked with a physical key.[28] Such analogies are valuable, and indeed arguably essential to explain certain aspects of encryption without getting deeply involved in the technical details.

However, analogies also have the potential to mislead when applied across disciplines. As discussed in Part III, a more appropriate analogy from the legal standpoint would be to a safe with a combination lock, because in both the combination safe and in encryption the "key" is some piece of information rather than a physical object. The distinction

---

27. Today, many smartphones, including the iPhone, use encryption to protect their data. To decrypt, a user must enter a short password usually consisting of 4 or 6 numbers (sometimes also called a passcode). This may raise a natural question: How does such a short password provide any meaningful security? An answer to this question is outlined below for the curious reader.

In the computer security community, a password and a secret key are not quite synonymous. *See* NIELS FERGUSON, BRUCE SCHNEIER & TADAYOSHIU KOHNO, CRYPTOGRAPHY ENGINEERING: DESIGN PRINCIPLES AND PRACTICAL APPLICATIONS 304–05 (2010). Devices that use passwords to decrypt often have a procedure for transforming the short password entered by the user into a much longer secret key using some additional secret information stored on the device itself. *See id.* An alternative, subtly different possibility is that the secret key is not a function of the password or biometric information, but rather, a trusted secure hardware component contains an independent secret key and releases it only when the correct password or biometric is presented. *Id.* at 306–07*; see also iOS Security*, APPLE (Aug. 2018), https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf [https://perma.cc/9FKR-Q7JV] (explaining of Apple's Touch ID system). Such techniques allow users to memorize short passwords while using encryption algorithms that require long, hard-to-guess secret keys.

By itself, the password provides scant security. There are 10,000 possible four-digit passwords: a human could try all 10,000 in a day or two, a computer in a matter of moments. To increase the level of security offered, devices unlocked by short passwords often employ additional measures that make trying many passwords impossible. Common measures include erasing all the device's contents after repeated incorrect passwords are entered or introducing a delay of minutes or hours between password attempts.

Combined with the security of the underlying encryption algorithm, these security measures are often effective. In fact, they were central to the famous dispute between FBI and Apple regarding the decryption of the iPhone used by one of the perpetrators of the December 2015 San Bernardino shooting. When law enforcement talks of its inability to read the contents of encrypted communications or devices, it is typically referring to a combination of the prohibitive computational cost of trying out all possible secret keys to find the right one and the prohibitive difficulty of finding an alternative workaround that would not require trying all possible secret keys (such workarounds are not always possible or within a feasible monetary cost, and typically have to be designed on a case-by-case basis even when they are possible). *See, e.g.*, U.S. DEP'T OF JUSTICE, OFF. OF THE INSPECTOR GEN., A SPECIAL INQUIRY REGARDING THE ACCURACY OF FBI STATEMENTS CONCERNING ITS CAPABILITIES TO EXPLOIT AN IPHONE SEIZED DURING THE SAN BERNARDINO TERROR ATTACK INVESTIGATION (Mar. 2018), https://oig.justice.gov/reports/2018/o1803.pdf [https://perma.cc/RGS4-EPNY].

28. *See, e.g.*, United States v. Hubbell, 530 U.S. 27, 43 (2000); Doe v. United States (*Doe I*), 487 U.S. 201, 210 n.9 (1988).

between something known and something possessed is fundamental to the Fifth Amendment self-incrimination doctrine.[29] Yet to many with a technical, rather than legal, background, the analogies of a key and combination lock may seem entirely equivalent.

Analogies also obscure certain details of a technical rather than legal nature, as they cannot capture every subtlety of the technical reality. For example, the same analogy to a physical safe obscures the idea that it may be impossible to tell whether a piece of data is an encryption of something or is simply random-looking, meaningless data. Capturing this possibility in the physical analogy requires some creativity and complicates the analogy: one can imagine what appears externally to be a locked wooden chest, but is instead a solid block of wood carved to look like a chest — and so could not possibly contain anything at all.

This Article is full of analogies made by authors with technical backgrounds, but who have studied the legal context in detail. The authors have done their best to choose these analogies carefully, endeavoring to provide illustrations of how legal doctrines interplay with technological features without obfuscating critical details.

III. THE FIFTH AMENDMENT AND THE NATURE OF TESTIMONY

The Fifth Amendment to the U.S. Constitution states that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself . . . ."[30]

Modern Supreme Court precedent[31] has established that to be afforded Fifth Amendment protection, an act must be compelled, incriminating, and also testimonial.[32] While a suspect (or witness) cannot be compelled to provide oral or written testimony against herself, a court may compel her to provide inculpatory evidence that is not testimonial.[33]

---

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

30. U.S. CONST. amend. V. The protections offered by the Fifth Amendment are not absolute. The government may compel a defendant to testify by granting immunity pursuant to 18 U.S.C § 6002. *See* Andrew T. Winkler, *Password Protection and Self-Incrimination: Applying the Fifth Amendment Privilege in the Technological Era*, 39 RUTGERS COMPUT. & TECH. L.J. 194, 212 (2013). Such a grant of immunity must protect the defendant against use and derivative use of the immunized testimony. *Id.* at 208. The scope of derivative use is quite broad, and thus could significantly hinder further prosecution of the immunized individual. A grant of immunity is unnecessary where no Fifth Amendment privilege exists. While the extent of the protection offered by immunity in compelled decryption cases merits increased attention, this Article is concerned with the privilege itself. As such, the complexities raised by immunity are not discussed further.

31. This Part gives a pragmatic overview of how the Fifth Amendment is applied by courts to modern cases.

32. *See, e.g.*, *Fisher*, 425 U.S. at 408 ("[T]he 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.").

33. *Id.*

This Fifth Amendment right extends only to natural persons and not corporations or other legal persons.[34]

A. The Nature of Testimony

While testimony is a type of evidence, not all evidence is testimonial. Thus, a suspect may be compelled to herself be physical evidence, or be the source of physical evidence that may be incriminating, including: "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."[35] A suspect may also be compelled by subpoena to produce physical evidence, or even documents whose contents may incriminate her, provided that the *creation* of the documents was not compelled by the government.[36]

Doe v. United States (Doe I) is illustrative.[37] To further a criminal investigation, the government sought to compel Doe to sign a directive authorizing a bank to release his personal records.[38] The directive was worded so that signing it did not entail Doe's admission that the records existed.[39] Instead, the directive simply authorized the bank to release any documents of a given description, without any assertions regarding the existence of such documents.[40] The Supreme Court ruled that compelling Doe to sign the directive did not violate the Fifth Amendment, holding that the directive itself was not testimonial in nature.[41] "In order to be 'testimonial,' an accused's oral or written communication, or act, must itself, explicitly or implicitly, relate a factual assertion or disclose information."[42] Even if the information to be released from the bank would be incriminating, the signature could be compelled because the form and the signature did not communicate any "factual assertions" to the government.[43]

Understanding the meaning of "testimonial" is key to understanding the Fifth Amendment. According to *Doe I*, a testimonial act must "explicitly or implicitly[] relate a factual assertion or disclose infor-

34. Curcio v. United States, 354 U.S. 118, 122 (1957) ("It is settled that a corporation is not protected by the constitutional privilege against self-incrimination.").

35. Schmerber v. California, 384 U.S. 757, 764 (1966).

36. United States v. Hubbell, 530 U.S. 27, 35 (2000) ("[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.").

37. 487 U.S. 201 (1988).

38. *Id.* at 203.

39. *Id.* at 204.

40. *Id.*

41. *Id.* at 219.

42. *Id.* at 209–10.

43. *Id.* at 215.

mation."[44] Justice Stevens' dissent in that same case presents a completely different formulation:

> A defendant can be compelled to produce material evidence that is incriminating . . . . But can he be compelled to use his mind to assist the prosecution in convicting him of a crime? I think not. He 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.[45]

Similarly, the *Fisher* court held that that case did not involve testimonial self-incrimination because "[s]urely the Government [was] in no way relying on the 'truthtelling' of the taxpayer to prove the existence of or his access to the documents."[46]

Another definition, which perhaps lies somewhere between the notions of "disclos[ing] information" and "us[ing] his mind to assist", is that testimony encompasses statements or acts by an individual that "disclose the contents of his own mind."[47] This conception, and the phrase "contents of the mind" in particular, predominates in the cases examined in this work. These competing conceptions of testimony are discussed further in Section V.G.

B. Act-of-Production Testimony

Even if a piece of evidence is not itself testimonial, it has long been recognized that the very *act of producing* the evidence may communicate information auxiliary to the evidence itself, thereby making the act testimonial.[48] If so, the act of production may warrant Fifth Amendment protection, depending on the circumstances.[49]

Fisher provides an oft-cited example: "Compliance with the subpoena [for a taxpayer's financial records] tacitly concedes the existence

---

44. *Id.* at 209–10.

45. *Id.* at 219 (Stevens, J., dissenting). The majority suggests that they "do not disagree" with this excerpt. *Id.* at 210 n.9; *see also* United States v. Hubbell, 530 U.S. 27, 43 (2000) (Stevens, J.) ("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."). Justice Stevens' distinction between a key and a combination is revisited later in the Article when discussing encryption, as the compulsion to open a strongbox bears certain resemblance to the compulsion to reveal the contents of an encrypted computer.

46. Fisher v. United States, 425 U.S. 391, 411 (1976).

47. Curcio v. United States, 354 U.S. 118, 128 (1957).

48. *Fisher*, 425 U.S. at 410.

49. *Id.*

of the papers demanded and their possession or control by the taxpayer. It also would indicate the taxpayer's belief that the papers are those described in the subpoena."[50] The three pieces of testimony communicated by the accused's act of production identified in *Fisher* are the existence, possession or control, and authenticity of the produced evidence.[51]

It may be possible for the government to compel an act even if it communicates implicit testimony. If all of the testimony implicit in an act of production is a *foregone conclusion*, then the act may still be compelled.[52] For example, a handwriting exemplar from a defendant implicitly communicates that the defendant is able to write; but because the ability to write is "a near truism" the exemplar can be compelled, even if it is incriminating.[53] The situation in *Fisher* was similar: "The existence and location of the papers [were] a foregone conclusion and the taxpayer add[ed] little or nothing to the sum total of the Government's information by conceding that he in fact ha[d] the papers."[54] Notably, the government does not have to know the contents of documents or papers to compel their production.[55]

Fisher thus established a two-pronged test to determine whether the production of some evidence may be compelled. First, would the act of production implicitly communicate information (e.g., the existence or authenticity of the produced evidence or the defendant's possession thereof)? If not, the production may be compelled.[56] Second, is the information implicitly communicated a foregone conclusion? If so, the act

---

50. *Id.*

51. *Id.*

52. *See id.* at 411. A current prevailing standard for establishing a foregone conclusion is "reasonable particularity." *See, e.g.*, *In re* Grand Jury Subpoena Dated March 25, 2011 (*Doe II*), 670 F.3d 1335, 1344 n.20 (11th Cir. 2012). This was established by various Circuit Courts of Appeals and has not yet been addressed by the Supreme Court. *See* United States v. Hubbell, 530 U.S. 27, 33 (2000) (noting the D.C. Circuit's "reasonable particularity" standard but declining to explicitly adopt it); *In re* Grand Jury Subpoena Dated April 18, 2003, 383 F.3d 905, 910 (9th Cir. 2004) (adopting the "reasonable particularity" standard); *see also* Vivek Mohan & John Villasenor, *Decrypting the Fifth Amendment*: *The Limits of Self-Incrimination in the Digital Era,* 15 U. PA. J. CONST. L. HEIGHT. SCRUTINY 11, 20 (2012) (asserting that the Supreme Court has not explicitly adopted or rejected the "reasonable Particularity" standard). The precise meaning of reasonable particularity for foregone conclusion is an interesting question for further study. Too stringent a standard could unduly burden the government compelling an act of production, while too loose a standard might allow the government to bootstrap weak evidence into stronger evidence. *See* Brief of Amicus Curiae Professor Orin Kerr in Support of Neither Party, Commonwealth v. Jones, No. SJC-12564 (Mass. filed Oct. 11, 2018), 2018 WL 5269423 (arguing that a court should require the government to show by "clear and convincing evidence" that an individual knows the password to a phone before compelling her to enter it).

53. *Fisher*, 425 U.S. at 411.

54. *Id.*

55. *See, e.g.*, *In re* Grand Jury Subpoena Dated Oct. 29, 1992, 1 F.3d 87, 93 (2d Cir. 1993) (concluding that compulsion only required existence and location being "forgone conclusions").

56. *Fisher*, 425 U.S. at 411.

of production may be compelled.[57] Otherwise, the act falls under the protection of the Fifth Amendment and may not be compelled.[58]

United States v. Hubbell is one notable case in which the testimonial aspects of act of production were deemed to merit Fifth Amendment protection.[59] While under investigation for tax evasion and related crimes, Hubbell was served with a subpoena to appear and produce all documents in his possession which fell into eleven broad categories, including "any and all documents reflecting, referring, or relating to any direct or indirect sources of money" from a period of three years.[60] Identifying and sorting the documents falling under the subpoena required Hubbell to examine a multitude of documents, eventually resulting in the production of 13,120 pages of material.[61] The court ruled that the act of production in *Hubbell* was testimonial because the "breadth of the description" of the requested documents made their "collection and production . . . tantamount to answering a series of interrogatories asking a witness to disclose the existence and location of particular documents fitting certain broad descriptions."[62]

Turning to the foregone conclusion aspect of the *Fisher* test, the *Hubbell* court held that the facts in this case "plainly [fell] outside of" the scope of the "'foregone conclusion' rationale."[63] In *Fisher*, the government "knew that the documents were in the attorneys' possession and could independently confirm their existence and authenticity"; in *Hubbell,* however, the government failed to demonstrate any "prior knowledge of either the existence or the whereabouts of the . . . documents ultimately produced by the respondent."[64] In light of the strong testimonial aspect of Hubbell's act of production, along with the very broad nature of the subpoena (specifically, the Independent Counsel acknowledged that he could not satisfy the "reasonable particularity" standard prescribed by the Court of Appeals), [65] the Court held that the Fifth Amendment protected the act of production in *Hubbell*.[66]

57. *Id.*
58. *See id.*
59. United States v. Hubbell, 530 U.S. 27, 28–29 (2000).
60. *Id.* at 41.
61. *Id.* at 42.
62. *Id.* at 41.
63. *Id.* at 44.
64. *Id.* at 44–45.
65. *Id.* at 30.
66. *See id.* at 46.

IV. ENCRYPTION AND SELF-INCRIMINATION: REVIEW OF CASES

This Part reviews several compelled decryption cases, which tend to follow the same general structure: the government seizes a digital storage medium (e.g., a computer) that it has reason to believe contains encrypted information relevant to an investigation,[67] and attempts to compel a suspect (e.g., with a subpoena) to help it access these encrypted contents. The defendant then invokes her Fifth Amendment protection against compelled self-incrimination, and a judge is called upon to decide what the government may compel from the suspect.

The cases are presented in terms of four archetypal categories distinguished by what specifically the government seeks to compel the target to do: (1) to reveal the password, (2) to use a fingerprint, (3) to produce the decrypted contents, or (4) to enter the password. Though each of these approaches to compelling decryption raises distinct Fifth Amendment issues, the existing literature has not disentangled the last two categories.[68]

Not all cases fit neatly into that taxonomy. As discussed further in Section IV.F, which category best fits a case is largely a product of law enforcement's discretion when drafting a subpoena, warrant, or motion, and some cases may fit multiple categories. Even so, distinguishing the compelled acts and the corresponding implicit testimony helps to clarify the precedent. Taken as a whole, the collection of cases establishes that passwords themselves generally cannot be compelled, that unlocking a device with a fingerprint generally can be compelled, and that whether the government can compel the entering of a password or the production of the decrypted contents rests on a case-by-case analysis of the testimony that the act of decryption may implicitly communicate (in the manner of *Fisher* and *Hubbell*).

Neither courts nor legal scholars are in agreement about how compelled decryption cases should be decided. To better focus on technological aspects of compelled decryption, this Article presents the authors' understanding of the evolving doctrine and omits much of the ongoing legal debate.

---

67. In general, the legality of the seizure itself may be a pertinent question in the context of the Fourth Amendment, *see supra* note 13 and accompanying text; however, as the discussion explicitly focuses on the Fifth Amendment, it assumes the search was legal.

68. *See, e.g.*, Dan Terzian, *The Micro-Hornbook on the Fifth Amendment and Encryption*, 104 GEO L.J. ONLINE 168, 170–74 (2016) (asking, under the heading "Forcing the Production of the Decrypted Phone?" whether "the government can force you to enter the password, which decrypts your phone").

A. Reveal-the-Password Cases

On December 10, 2009, Thomas Kirschner was indicted for three counts of receipt of child pornography.[69] The government seized his computer, which appeared to contain encrypted files, and issued a grand jury subpoena requiring Kirschner "to provide all passwords used or associated with the . . . computer . . . and any files."[70] Kirschner moved to quash the subpoena on Fifth Amendment grounds.[71]

The court granted the motion to quash, holding that requiring Kirschner to provide his password would be testimonial, since "the government is not seeking documents or objects," but rather "seeking testimony . . . requiring [Kirschner] to divulge through his mental processes his password — that will be used to incriminate him."[72] This reasoning relied on analogizing a password decrypting a computer to a combination unlocking a safe, citing Justice Stevens' dissent in *Doe I*, which stated that a defendant may be "forced to surrender a key to a strongbox" but not "to reveal the combination to his wall safe — by word or deed."[73]

United States v. Kirschner's holding that passwords are clearly testimony is bolstered by subsequent cases, including *In re Grand Jury Subpoena to Sebastien Boucher (Boucher I)*,[74] *Commonwealth v. Baust*,[75] and *SEC v. Huang*.[76] The prevalence of cases in which the government seeks to compel decryption in ways other than compelling the disclosure of the password additionally indicates the commonly accepted testimonial nature of passwords.[77]

However, there are at least three cases that disagree with *Kirschner.* In *United States v. Pearson*,[78] an earlier compelled decryption case, the government issued a subpoena for "all passwords, keys and/or log-ins

---

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

70. *Id.*

71. *Id.*

72. *Id.* at 669.

73. *Id.* (citing Doe v. United States (*Doe I*), 487 U.S. 201, 219 (1988) (Stevens, J., dissenting)). For further discussion on Stevens' dissent, *see supra* note 45.

74. No. 2:06-mj-91, 2007 WL 4246473, at *6 (D. Vt. 2007) ("Since the government is trying to compel the production of the password itself, the foregone conclusion doctrine cannot apply. The password is not a physical thing . . . . It is pure testimonial production rather than physical evidence having testimonial aspects."), *rev'd on other grounds by In re* Grand Jury Subpoena to Sebastien Boucher (*Boucher II*), no. 2:06-mj-91, 2009 WL 424718 (D. Vt. 2009).

75. 89 Va. Cir. 267, 271 (2014) ("Unlike a document or tangible thing, such as an unencrypted copy of the footage itself, if the password was a foregone conclusion, the Commonwealth would not need to compel Defendant to produce it because they would already know it.").

76. No. 15-269, 2015 WL 5611644, at *2 (E.D. Pa. 2015) ("Here, the SEC seeks to compel production of the passcodes which require intrusion into the knowledge of Defendants and no one else.").

77. *See generally* Terzian, *supra* note 68.

78. 2006 U.S. Dist. LEXIS 32982 (N.D.N.Y 2006).

used to encrypt any and all files" by the defendant.[79] A District Court in New York did not have occasion to address the question — central to *Kirschner* — of whether the password is itself testimony.[80] Instead, the court's analysis resembled that of *United States v. Doe* (*Doe II*),[81] discussed in the next Section, which focused on the possible testimonial communications about the encrypted files.[82]

State v. Stahl[83] is a more recent case in which the State of Florida sought to compel the defendant, Stahl, to reveal the password to unlock his iPhone.[84] The Florida Court of Appeals rejected the reasoning of *Kirschner*, on the basis that that requiring Stahl to produce his password did not compel him "to communicate information that had *testimonial significance*."[85] The court implicitly conceded that compelling Stahl to reveal his password to the State would communicate the contents of Stahl's mind, but that it would have no other "value or significance," and was therefore not testimonial for the purpose of the Fifth Amendment protection.[86] The *Stahl* court rejected the notion that the Fifth Amendment protects all the contents of the accused's mind, and instead described a doctrine under which only those contents that are significant are to be protected.[87] After rejecting the reasoning of *Kirschner*, *Stahl* continued with a foregone conclusion analysis, concluding that since the password existed, was known to the defendant, and was authentic, it could be compelled.[88] *Stahl*'s interpretation diverged starkly from the interpretation of *Fisher*, *Hubbell*, and *Doe I* that is common throughout the other cases discussed in this Article. *Stahl*'s testimonial significance test would significantly alter the scope of the Fifth Amendment, and go against a preponderance of precedent.[89]

---

79. *Id.* at *3.

80. *Id.* at *54, n.6 ("By proceeding directly to the 'act of production' argument, Defendant essentially concedes that the password itself carries no Fifth Amendment privilege.").

81. 670 F.3d 1335 (11th Cir. 2012).

82. *Compare Pearson*, 2006 U.S. Dist. LEXIS 32982, at *58–*62, *with Doe II*, 670 F.3d at 1341.

83. 206 So. 3d 124 (Fla. App. Ct. 2016).

84. *Id.* at 124.

85. *Id.* at 136 (emphasis added). While disagreeing with *United States v. Kirschner*, 823 F. Supp. 2d 665 (E.D. Mich. 2010), *Stahl* stopped short of directly contradicting it, suggesting in a footnote that there may be facts in that case that warrant the opposite conclusion. *Stahl*, 206 So. 3d at 134, n.11.

86. *Stahl*, 206 So. 3d at 134.

87. *Id.* at 133–34 (finding that "the contents of the accused's mind must be 'extensive[ly] use[d]' in creating the response, or must 'relat[e] him to the offense'" (citations omitted) (alterations in original) (quoting *Hubbell*, 530 U.S. 27, 27 (2000); Doe v. United States (*Doe I*), 487 U.S. 201, 213 (1988)). Compelling Stahl's password would, the court argues, do neither. *Id.* at 133–34.

88. *Id.* at 136.

89. A very recent Florida appellate case disagreed with *Stahl* in its holding that password disclosure *is* protected under the Fifth Amendment, and quashed a trial court order (which was based on reasoning following *Stahl*) compelling disclosure of two passwords. G.A.Q.L. v.

Finally, the Superior Court of Pennsylvania in *Commonwealth v. Davis*[90] entirely ignored the issue of a password's pure testimonial nature, and applied the foregone conclusion analysis from *Stahl* without further justification.[91]

B. Produce-the-Decrypted-Contents Cases

Rather than seeking a password, the government can seek to compel the defendant to directly furnish the decrypted contents of the device. This is analogous to issuing a subpoena for documents stored in a strongbox, rather than the combination that unlocks the box. In such cases, courts have directly adapted the act-of-production and foregone conclusion doctrine from *Fisher* and *Hubbell*.

The facts in *Doe II* are straightforward. In October 2010, after a months-long investigation, police applied for and were granted a warrant to search a hotel room booked by the defendant, Doe, who was suspected of distributing child pornography.[92] Law enforcement seized two laptop computers and five hard drives totaling about five terabytes of storage.[93] Portions of the various drives were encrypted, and forensic examiners at the FBI were unable to recover any meaningful data from these portions.[94] A grand jury subpoena issued requiring "Doe to produce the 'unencrypted contents' of the digital media, and 'any and all containers or folders thereon.'"[95] Doe refused and, in a subsequent hearing, a lower court rejected Doe's Fifth Amendment arguments and held

State, No. 4D18-1811, 2018 WL 5291918, at *2–*3 (Fla. Dist. App. Ct. Oct. 24, 2018). The majority in *G.A.Q.L.*, however, erred in applying the *Doe II* foregone-conclusion test verbatim to *G.A.Q.L.* and thereby analyzing what testimony would be implicit in the act of producing the decrypted contents that the requested passwords would unlock. *See id.* at *3–*5. In *Doe II* (discussed further in Section VI.B), the government in fact sought to compel the defendant to produce the decrypted contents, and accordingly, the court's analysis focuses on the testimonial communication inherent in *that act of producing decrypted contents*. *In re* Grand Jury Subpoena Dated March 25, 2011 (*Doe II*), 670 F.3d 1335, 1337 (11th Cir. 2012). In contrast, the State of Florida in *G.A.Q.L.* sought to compel *disclosure of passwords*, a different act. No. 4D18-1811, 2018 WL 5291918, at *1. The *reasoning* underlying *Doe II* is relevant to *G.A.Q.L.*, but applying the *Doe II* test verbatim to *G.A.Q.L.* results in analyzing the testimony inherent in an act which the state did not even try to compel. The concurrence, which more closely follows the *Fisher* reasoning as understood in this Article, argued that the majority's analysis erred in analyzing password disclosure as an act of production at all, rather than as plain oral testimony. *Id.* at *5–*6 (Kuntz, J., concurring in result).

90. 176 A.3d 869 (Pa. Super. Ct. 2017).

91. *Id.* at 876.

92. *Doe II*, 670 F.3d 1335, 1339 (11th Cir. 2012).

93. *Id.*

94. *Id.*

95. *Id.*

Doe in civil contempt.[96] Doe appealed the contempt judgment to the Eleventh Circuit.[97]

The government argued that the subpoena only required Doe to produce "pre-existing and voluntarily created files."[98] Because the creation of the files was voluntary, the government argued, their contents were not protected by the Fifth Amendment.[99] While the Eleventh Circuit agreed that the contents of the files would not constitute testimony, it rejected the government's argument that this was the only potential consideration.[100]

The Eleventh Circuit adopted the act-of-production framework of *Fisher* and *Hubbell*, stating that "the decryption and production would be tantamount to testimony by Doe of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; and of his capability to decrypt the files."[101] The court rejected the government's argument that producing the files would be a purely "physical nontestimonial transfer," writing that "[r]equiring Doe to use a decryption password is most certainly more akin to requiring the production of a combination because both demand the use of the contents of the mind, and the production is accompanied by the implied factual statements noted above that could prove to be incriminatory."[102]

The Eleventh Circuit then turned to the second half of the *Fisher* test: were the testimonial aspects of decryption and production already known to the government? No. The court determined that the government was unable to demonstrate knowledge of Doe's capability to decrypt the encrypted portions of the drives.[103] Moreover, even the existence of any files whatsoever on those portions was not a foregone conclusion.[104] According to the court, the government did not know if there were any files on the drive whatsoever.[105] In support, the court highlighted a key exchange from the district court's hearing.

---

96. *Id.* at 1338.

97. *Id.*

98. *Id.* at 1342.

99. *Id.*

100. *Id.*

101. *Id.* at 1346. The ruling suggests that there may be an additional reason to consider production of decrypted drives as testimonial. "[T]he decryption and production of the hard drives would require the use of the contents of Doe's mind and could not be fairly characterized as a physical act that would be nontestimonial in nature." *Id.*

102. *Id.*

103. *Id.* ("Nothing in the record before us reveals that the Government knows . . . that Doe is even capable of accessing the encrypted portions of the drives.")

104. *Id.* at 1347 ("The Government has not shown, however, that the drives *actually* contain any files . . . .").

105. The court goes to some lengths to emphasize that it is the existence of files, not their contents or names, that is important, writing that "[t]o be clear, the Government does not have

> Although they were unable to find any files, [forensic examiner] McCrohan testified that they believed that data existed on the still-encrypted parts of the hard drive. In support of this belief, the Government introduced an exhibit with nonsensical characters and numbers, which it argued revealed the encrypted form of data that it seeks.
>
> In his testimony on cross-examination by Doe, however, McCrohan conceded that, although encrypted, it was possible that the hard drives contain nothing. Doe asked McCrohan, "So if a forensic examiner were to look at an external hard drive and just see encryption, does the possibility exist that there actually is nothing on there other than encryption? In other words, if the volume was mounted, all you would see is blank. Does that possibility exist?" McCrohan responded: "Well, you would see random characters, but you wouldn't know necessarily whether it was blank."[106]

The court therefore concluded that the existence of any files was not a foregone conclusion.

---

to . . . know[] specific file names," and clarifying that when the government does not know a specific file name, "it . . . must show with . . . reasonable particularity that it . . . is aware . . . that (1) the file exists in some specified location, (2) the file is possessed by the target . . . and (3) the file is authentic . . . . Thus . . . it still must . . . establish that a file . . . whatever its label, does . . . exist." *Id.* at 1353, n.28; *see also* United States v. Apple MacPro Computer, 851 F.3d 238, 248, n.7 (3d Cir. 2017) (applying *Doe II*).

Some others have interpreted the 11th Circuit as requiring the government to have knowledge of the contents of the encrypted drive. The alternative interpretation, is that the Eleventh Circuit held that the government could not compel decryption because it did not know the *contents* of the hard drive. *See, e.g.*, Orin Kerr *The Fifth Amendment Limits on Forced Decryption and Applying the 'Foregone Conclusion' Doctrine*, WASH. POST (Jun. 7, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/06/07/the-fifth-amendment-limits-on-forced-decryption-and-applying-the-foregone-conclusion-doctrine/ [https://perma.cc/MK6C-BK5C] ("[According to the Eleventh Circuit, the foregone conclusion doctrine] did not apply because the government did not know with 'reasonable particularity' what materials would be found on the computer were the files decrypted."). The authors' interpretation is that the Eleventh Circuit held that the government could not compel decryption because it had not established whether the drive was even encrypted (and thus contained "encrypted files"), without making a statement about the importance, if any, that knowledge of contents would have had, had it somehow been known that the drive was indeed encrypted. *Doe II*, 670 F.3d at 1349 ("[T]he Government has failed to show any basis . . . for its belief that encrypted files exist on the drives . . . .").

106. *Doe II*, 670 F.3d at 1340. See *infra* Part V and Part VII for further discussion of the issues raised by McCrohan's testimony.

Because production of the decrypted files would communicate Doe's knowledge of their existence, the Fifth Amendment precluded compulsion thereof.[107] The court reversed Doe's contempt judgment.[108]

Summarizing, the Eleventh Circuit applied the *Fisher* test in *Doe II*. First, the court held that that "[r]equiring Doe to use a decryption password [was] . . . akin to requiring the production of a combination" because both used the contents of the mind and both were accompanied by a number of possibly incriminatory "implied factual statements."[109] Then it examined whether these implied factual statements were a foregone conclusion, concluding that they were not.[110]

Courts have applied this type of reasoning relatively consistently in cases in which the government seeks to compel production of decrypted contents of an encrypted storage medium, including *In re Grand Jury Subpoena to Sebastien Boucher (Boucher II)*,[111] *In re The Decryption of a Seized Data Storage System (Feldman)*,[112] and *United States v. Fricosu*.[113] In each of these three cases, the court skipped straight to the foregone conclusion examination, focusing on the existence and location of the files in question (but not their contents), and on the defendant's ability to access the encrypted devices.[114] *Boucher II* also briefly raised the

---

107. *Id.* at 1349 ("The Fifth Amendment protects Doe's refusal to decrypt . . . because the act of decryption and production would be testimonial . . . .").

108. *Id.* at 1353.

109. *Id.* at 1346.

110. *See id.* at 1349 ("[T]he Government cannot show that the 'foregone conclusion' doctrine applies.").

111. *In re* Grand Jury Subpoena to Sebastien Boucher (*Boucher II*), No. 2:06-mj-91, 2009 WL 424718, at *1, *2 (D. Vt. Feb. 19, 2009). On appeal, the government stated that "it [did] not in fact seek the password for the encrypted hard drive, but require[d] Boucher to produce the contents of his encrypted hard drive in an unencrypted format by opening the drive before the grand jury." *Id.* at *1. With the new subpoena, the government ultimately prevailed. *See also infra* note 74.

112. *In re* The Decryption of a Seized Data Storage System (*Feldman*), No. 13-M-449, 2013 U.S. Dist. LEXIS 202353, at *1 (E.D. Wis. Apr. 19, 2013). The eventual court order required Feldman, "without being observed by law enforcement agents or by counsel for the United States of America, [to] enter the appropriate password or passwords into forensic copies of the above-identified storage devices so as to decrypt those devices." *Id.* at *4. Thus, it can reasonably be viewed as either a produce-the-decrypted-contents case or an enter-the-password case, though the former is a slightly better fit. *See also infra* Section VI.B.

113. United States v. Fricosu, 841 F. Supp. 2d 1235, 1237 (D. Colo. 2012). Note that in both *Feldman*, 2013 U.S. Dist. LEXIS 202353, at *4, and *Fricosu*, 841 F. Supp. 2d at 1238, the government applied for an order compelling decryption under the All Writs Act, rather than a grand jury subpoena.

114. *See, e.g.*, *Doe II*, 670 F.3d at 1349 n.28 ("[T]he Government does not have to show that it knows specific file names."); *Fricosu*, 841 F. Supp. 2d at 1236 ("The fact that it does not know the specific content of any specific documents is not a barrier to production."); *cf. Boucher II*, 2009 WL 424718, at *3 (noting the government's knowledge of the contents of encrypted drives was used to establish that the existence of files was a foregone conclusion); *Feldman*, 2013 U.S. Dist. LEXIS 202353, at *3 (similarly).

issue of authenticity, taking the government at its word that "it [would] not use [Boucher's] act of production as evidence of authentication."[115]

In *Boucher II*, *Feldman*, and *Fricosu*, the court found that any information potentially revealed by the act of producing the decrypted contents of the drive or computer in question was already known to the government and thus granted the government's order to compel.[116]

C. Enter-the-Password Cases

The next category of cases involves instances where the government seeks to compel a defendant to enter the password directly into an encrypted device. To avoid learning the password, the government promises not to view the password being used. Act-of-production testimony and foregone conclusion analysis play important roles in these types of cases. However, the testimony implicit in enter-the-password cases is not the same as that in produce-the-decrypted-contents cases.

In 2010, the Commonwealth of Massachusetts charged an attorney named Leon Gelfgatt with forgery and attempted larceny.[117] The previous year, the Commonwealth alleged, Gelfgatt forged and filed at the registry of deeds documents assigning seventeen outstanding home mortgages to two sham companies, intending to divert funds meant to pay off the home mortgage loan to himself.[118] The Commonwealth believed that Gelfgatt "relied heavily on the use of computers to conceal his identity and perpetrate his alleged scheme."[119]

On December 17, 2009, Gelfgatt was arrested.[120] His residence and vehicle were searched and four encrypted computers were seized.[121] During post-arrest questioning, Gelfgatt "acknowledged that he was able to perform decryption" of the computers.[122]

Though knowledge of the contents can be used to support the knowledge of the existence of contents, *Boucher II* and *Feldman* do not indicate the necessity of knowledge of the contents, only sufficiency.

115. *Boucher II*, 2009 WL 424718, at *4. This may raise the following question: if it is acceptable to take the government at its word that it will not make use of some act-of-production testimony, then why is it not generally possible for the government to compel decryption by promising not to use any such auxiliary testimony? It is important to remember that, even if taken at its word, the government must eventually establish the authenticity of the evidence independently. Indeed, the burden of proof on the government in such a case is greater, as it must additionally demonstrate that its knowledge does not derive in any way from the compelled act already undertaken.

116. *Boucher II,* 2009 WL 424718, at *4; *Feldman*, 2013 U.S. Dist. LEXIS 202353, at *2, 4; *Fricosu*, 841 F. Supp. 2d at 1238.

117. Commonwealth v. Gelfgatt, 11 N.E.3d 605, 608 (Mass. 2014).

118. *Id.* at 609.

119. *Id.*

120. *Id.*

121. *Id.* at 610.

122. *Id.* at 615.

Believing that evidence of Gelfgatt's criminal activities was located on the computers but could not be retrieved unless the correct password was entered and the data decrypted, the Commonwealth moved to compel Gelfgatt to enter his password into the encrypted computers.[123] The Commonwealth attested that it would not "view or record the password or key in any way."[124] The motion to compel decryption was initially denied, but was transferred to the Supreme Judicial Court of Massachusetts.[125]

The *Gelfgatt* court held that Gelfgatt could be compelled to enter his password so long as the "compelled decryption would not communicate facts of a testimonial nature to the Commonwealth beyond what [Gelfgatt] already had admitted to investigators."[126] This is a clear restatement of the *Fisher* foregone conclusion doctrine.

To decide whether any such facts would be communicated, the court identified a number of testimonial facts implicit in the act of entering a password: "ownership and control of the computers and their contents, knowledge of the fact of encryption, and knowledge of the encryption key."[127] However, because Gelfgatt had already acknowledged that he could decrypt the computers, the court held that these facts were a foregone conclusion, and reversed the earlier denial of the motion to compel.[128]

The *Gelfgatt* court followed the precedent set in *Fisher*: it identified those facts that the act of entering the password would convey, concluded that those facts were a foregone conclusion, and thereby concluded that the government could compel the act of entering the password.

D. Enter-the-Password Versus Produce-the-Decrypted-Contents

Though it may seem a straightforward application of *Fisher*, the *Gelfgatt* decision suggests a doctrinal distinction between produce-the-decrypted-contents cases and enter-the-password cases like *Doe II*. *Doe II* is essentially a classic act-of-production analysis. The object of the subpoena is the decrypted files on the computer, and the testimonial facts communicated by Doe's compliance included "knowledge of the existence and location of potentially incriminating files; of his possession,

123. *Id.* at 608, 610.

124. *Id.* at 611, n.10.

125. The Supreme Judicial Court of Massachusetts considered the legality of the motion with respect to both the Fifth Amendment and the Massachusetts Declaration of Rights. *Id.* at 608. This discussion focuses on the application of the Fifth Amendment in *Gelfgatt* and does not further discuss the Massachusetts Declaration of Rights.

126. *Id.* at 608.

127. *Id.* at 615.

128. *Id.* at 615–17.

control, and access to the encrypted portions of the drives; and of his capability to decrypt the files."[129] That is, Doe's knowledge of the existence of the files and Doe's ability to retrieve them in decrypted form: existence and possession.

In *Gelfgatt*, there is no attempt on the part of the court to cast the act of entering a password as an act of production of some thing, physical or digital.[130] There is no thing the fact of whose existence or possession could be communicated. Instead, the court performed the implicit testimony and foregone conclusion analysis with respect to the act to be compelled, namely, entering a password.[131] Compelling a defendant to enter a password is compelling an act, but that act is no act of production.

Understanding this distinction is helpful to reconciling the judgments in these and other compelled decryption cases. Conflating these types of acts can lead to confusion, as for example in *Boucher I*.[132] In that case, the District Court of Vermont began its analysis in a manner similar to *Gelfgatt*: "Entering a password into the computer implicitly communicates facts . . . that he knows the password and has control over the files . . . . The procedure is equivalent to asking Boucher, 'Do you know the password to the laptop?'"[133] But then, rather than analyzing the testimonial communications identified, the judge molded the analysis to resemble an act-of-production analysis. Because it was unclear what thing was being produced, the court considered two possibilities: that the subpoena either "compel[led] the production of the password itself or compel[led] the production of the files on [the hard drive]."[134] The court held that if the subpoena was for the password itself, the act-of-production framework did not apply.[135] Additionally, the court concluded, even if the subpoena was for the decrypted documents of the hard drive, there was no foregone conclusion because the government had only viewed a small subset of the encrypted files of the drive.[136]

It is instructive to contrast *Boucher I* with *Gelfgatt*. The court in *Boucher I* adhered too strictly to the format of *Fisher* in an analysis that ineffectively attempted to fit the facts of the case to an act-of-production

129. United States v. Doe (*Doe II*), 670 F.3d 1335, 1346 (11th Cir. 2012).

130. *Gelfgatt*, 11 N.E.3d at 622.

131. *Id.* at 622.

132. *In re* Grand Jury Subpoena to Sebastien Boucher (*Boucher I*), No. 2:06-mj-91, 2007 WL 4246473, at *3 (D. Vt. Nov. 29, 2007).

133. *Id.*

134. *Id.* at *6.

135. *Id.* ("The password is not a physical thing. If Boucher knows the password, it only exists in his mind.").

136. *Id.*

pattern, and which was ultimately overturned.[137] The judge may have erred by effectively treating *Boucher I* as a produce-the-decrypted-contents case (which involves compelling an act of production), instead of the enter-the-password case it was (which involves compelling an act, but not an act of producing an object).[138] In contrast, the *Gelfgatt* court recognized the doctrinal questions of an enter-the-password case. In doing so, it better followed the essence of the *Fisher* ruling by directly analyzing the testimony implicit in whatever act is compelled.

E. Use-a-Fingerprint Cases

Most of the cases that this Article discusses involve the use of encryption where decryption is effected by using a secret password. The final category of cases concerns situations where a defendant may instead decrypt using a fingerprint, or other biometrics (e.g., face ID on the iPhone X[139]). Such cases are increasingly common as the use of fingerprint-based security on smartphones becomes more prevalent.[140] Because a fingerprint is a physical feature of the body, and not some secret knowledge like a password, the doctrine for compelled decryption in these cases is very different. Generally, courts have found that compelling the use of a fingerprint to decrypt or unlock a device does not violate the Fifth Amendment.[141]

In *Commonwealth v. Baust*,[142] defendant David Charles Baust had been indicted for allegedly strangling a woman in his bedroom.[143] The

---

137. On appeal, the District Court of Vermont rejected the conclusion that the government needed to have viewed the remaining contents of the encrypted hard drive. *In re* Grand Jury Subpoena to Sebastien Boucher (*Boucher II*), No. 2:06-mj-91, 2009 WL 424718, at *3 (D. Vt. Feb. 19, 2009). "Second Circuit precedent, however, does not require that the government be aware of the incriminatory *contents* of the files; it requires the government to demonstrate with reasonable particularity that it knows of the existence and location of subpoenaed documents." *Id.* (quotations omitted) (citing *In re* Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d 87, 93 (2d Cir. 1993)).

Note that *Boucher II* was a produce-the-decrypted-contents case, not an enter-the-password case. It should not be construed to mean that government knowledge of the existence of encrypted files alone suffices to compel a defendant to enter a password in an encrypted computer.

138. *Cf.* G.A.Q.L. v. State, No. 4D18-1811, 2018 WL 5291918, at *1–*3 (Fla. Dist. Ct. App. Oct. 24, 2018) (applying *Fisher* similarly).

139. *See generally About Face ID Advanced Technology*, APPLE (Nov. 6, 2018), https://support.apple.com/en-us/HT208108 [https://perma.cc/FY5T-7C42].

140. Fionna Agomuoh, *Password-Free Smartphones Are No Longer the Stuff of Science Fiction — They're Everywhere*, BUS. INSIDER (Dec. 27, 2017), https://www.businessinsider.com/smartphone-biometrics-are-no-longer-the-stuff-of-science-fiction-2017-12 [https://perma.cc/N2YD-BK2G].

141. Terzian, *supra* note 68, at 169 ("Unquestionably, the government can force people to produce biometric passwords like fingerprints.").

142. Commonwealth v. Baust, 89 Va. Cir. 267 (Cir. Ct. 2014).

143. *Id.* at 267.

victim alleged that video recording equipment set up in the bedroom recorded the assault and that the recording would have been transmitted to Baust's cell phone.[144] Though the police seized the phone, access to its contents required a valid password or fingerprint.[145] The Commonwealth of Virginia then moved "to compel the production of the passcode or fingerprint associated with Baust's cell phone."[146]

The state circuit court examined whether production of the password or fingerprint should be considered testimonial. On the former question, the court adopted the reasoning of *Kirschner* and *Boucher I*: the password itself was testimony and the foregone conclusion analysis did not apply.[147] The motion to compel the password was accordingly denied.[148] On the other hand, the court granted the motion to compel the fingerprint because "like a key . . . [it did] not require [Baust] to 'communicate any knowledge' at all."[149] The fingerprint was like other "physical characteristics that are non-testimonial" and its use to decrypt the phone would have been "non-testimonial."[150] As the court held that the fingerprint had no testimonial content, it did not attempt a foregone conclusion analysis.[151]

Most courts seem to agree with *Baust* that fingerprint decryption can be compelled without running afoul of the Fifth Amendment.[152] There is, however, at least one federal judge who arrived at the opposite conclusion:

> [T]he connection of the fingerprint to the electronic source that may hold contraband (in this case, suspected child pornography) does explicitly or implicitly relate a factual assertion or disclose information . . . . With a touch of a finger, a suspect is testifying that he or she has accessed the phone before, at a minimum, to

144. *Id.*

145. *See id.* at 267–68.

146. *Id.* at 267.

147. *Id.* at 271 (quipping that "if the password was a foregone conclusion, the Commonwealth would not need to compel [Baust] to produce it because they would already know it.").

148. *Id.*

149. *Id.*

150. *Id.*

151. *See id.* Though it was unnecessary for ruling on the government's motion, the court additionally considered whether the government could compel Baust to produce the unencrypted video recording that they sought, concluding based on the facts that the Commonwealth suspected, but did not know, that the recording actually existed, failing to satisfy a foregone conclusion test. *Id.* This reasoning is consistent with *United States v. Doe (Doe II)*, 670 F.3d 1335 (11th Cir. 2012), and the other decrypted-contents cases in Section IV.B.

152. *See, e.g.*, Minnesota v. Diamond, 890 N.W.2d 143 (Minn. Ct. App. 2017); State v. Stahl, 206 So. 3d 124 (Fla. Dist. Ct. App. 2016); *In re* Search of iPhone seized from 3254 Altura Avenue in Glendale, Cal., No. 2:16-mj-00398-DUTY, slip op. at 4 (C.D. Cal. Mar. 15, 2016).

> set up the fingerprint password capabilities, and that he or she currently has some level of control over or relatively significant connection to the phone and its contents.[153]

The assertion that a fingerprint scan on a device can reveal private, possibly incriminating information is certainly valid. However, the conclusion that the mere touch of a finger is a testimonial act diverges starkly from most other fingerprint cases. The purely physical act of pressing one's finger onto a sensor neither reveals the contents of the mind nor relies on the truthfulness of the finger's owner. For example, if the government were mistaken and the defendant had never accessed the phone before, she could still perform the physical act of placing her fingerprint on the sensor, which would fail to unlock the phone. Doing so would not attest that the defendant had accessed the phone before.

F. Overlapping Categories

The four archetypes comprising the taxonomy of compelled decryption cases are useful both for making sense of past cases and for reasoning about future cases. However, not all cases fit neatly into the taxonomy.[154] Usually, the facts of a case will be compatible with several or all of the categories, and the category of a case is determined by the government's approach. Which category best fits a case is often a product of wording choices made when drafting a subpoena, warrant, motion, or order, and some cases may fit multiple patterns. It is unclear to what extent such wording choices are made deliberately to place a case in one category or another.

For example, in *Feldman*, the government applied for an order which adopted a clear produce-the-decrypted-contents approach, seeking to compel Feldman to "assist in the execution of a federal search warrant by providing federal law enforcement agents a decrypted version of the contents of his encrypted data storage system."[155] Ultimately, however, the court issued an order whose first part was more appropriate for an enter-the-password case:

> It is further ordered that *on or before June 4, 2013*, Feldman shall do *one* of the following: (1) . . . without

153. *In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073 (N.D. Ill. 2017) (internal quotations and citations omitted).

154. Some of the technologies discussed in Part V also have the tendency of further blurring the lines between categories.

155. *In re* The Decryption of a Seized Data Storage Sys. (*Feldman*), No. 13-M-449, 2013 U.S. Dist. LEXIS 202353, at *1 (E.D. Wis. Apr. 19, 2013).

> being observed . . . enter the appropriate password or passwords into forensic copies of the above-identified storage devices so as to decrypt those devices . . . *or* (2) take any actions agreed upon . . . for the purpose of, and with the result of, making available for their examination a decrypted copy of the data that exists in each of the above-identified storage devices.[156]

Notwithstanding the final order, this Article treats *Feldman* as a produce-the-decrypted-contents case because the court's analysis more closely aligns with that category.

The investigation against Sebastien Boucher presents another example.[157] The initial grand jury subpoena demanded Boucher's passwords, but the government later "suggested that Boucher could enter the password into the computer without the government, the grand jury, or the [c]ourt observing or recording the password in any way."[158] Upon appeal, the government again changed its request, only "requir[ing] Boucher to provide an unencrypted version of the drive to the grand jury."[159] The government modified its approach twice in order to achieve the desired outcome of compelling decryption.

A final example of a different nature comes from the reveal-the-password category. The government subpoena in *Pearson* compelled the production of "all passwords, keys, and/or log-ins used to encrypt any and all files."[160] In support, the government argued that Pearson "more than likely reduced the password to writing" and therefore that "[p]roduction of this voluntarily created writing would not . . . constitute compulsion."[161] By writing down the password, Pearson would have transformed a reveal-the-password case into one of pure physical production.[162] This calls into question the relevance of *Kirschner*. However,

---

156. Order Granting *Ex Parte* Request for Reconsideration of the United States' Application under the All Writs Act*, Feldman*, 2013 U.S. Dist. LEXIS 202353 (No. 13-M-449) (emphasis in original).

157. *In re* Grand Jury Subpoena to Sebastien Boucher (*Boucher I*), No. 2:06-mj-91, 2007 WL 4246473 (D. Vt. Nov. 29, 2007); *In re* Grand Jury Subpoena to Sebastien Boucher (*Boucher II*), No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

158. *Boucher I*, 2007 WL 4246473, at *2.

159. *Boucher II*, 2009 WL 424718, at *1.

160. United States v. Pearson, No. 1:04-CR-340, 2006 U.S. Dist. LEXIS 32982, at *3 (N.D.N.Y. May 24, 2006) (quoting the subpoena).

161. *Id.* at *53.

162. It is intriguing to consider a sort of converse situation in the context of a physical safe opened with a key. Key cutting machines can be operated to produce a key based just on a "blueprint" (i.e., the type of key blank and the shape, size, and location of each of the cuts in the key). Suppose that the defendant in question had destroyed the original key to the vault, and had memorized the blueprint so that whenever she wants to open the vault, she can cut a new key using her key cutting machine, based on the memorized blueprint. Then, even if all the circumstances of this situation are well known to the government, it would seem that it could

neither the subpoena nor the court's examination was limited to those passwords that may have been written down.[163] Rather, they concern all passwords, without an accompanying justification that all were indeed written down or otherwise eligible for compulsion.[164]

V. TECHNOLOGICAL HYPOTHETICALS

Part IV examined the application of *Fisher*'s act-of-production doctrine in a variety of past compelled decryption cases. This Part turns from the factual variations of past cases and examines instead a number of technological variations that could — in principle or in practice — present themselves in the future. Each Section in this Part explains some existing or realistic technology and then discusses its interaction with the compelled decryption doctrine. Some of these technologies are currently available to any person with some technical savvy and could in principle arise in a compelled decryption case today. Others are not readily available today, but their implementation would pose no significant technological hurdles.[165] Each technology highlights and challenges a different facet of the doctrine, making explicit the sometimes fragile technological assumptions made in existing analyses.

An anticipatory approach to technological changes, including preemptive consideration of the implications of plausible technological variations on case analyses, can serve as an essential tool in developing robust doctrine that will remain unequivocal and relevant over time. It also raises questions about the broader doctrinal landscape beyond the scope of specific cases — such as the extent to which the outcome of cases does or should depend on small, and sometimes seemingly minor, changes in technology.

Real cases are complex and multifaceted, and of course, technical considerations contribute only so much to a case's eventual outcome. Nevertheless, to more clearly analyze the sometimes subtle interaction

---

not compel her to disclose the key blueprint in court as that would reveal the contents of her mind and therefore be testimonial. Whether she could be compelled to use her key cutting machine to create a new key, and present that key in court, is another question that might arise in such a case.

Possessing a physical as opposed to a memorized copy of the key could be neatly analogized to keeping a password written down as opposed to memorized. Then, creating a new key and presenting it to the court would be analogous to writing down the password and presenting it to the court. This is perhaps a clearer example in which to see that to compel the defendant to create and hand over the key would likely be prohibited.

163. *Pearson*, 2006 U.S. Dist. LEXIS 32982, at *51–*52.

164. *Id.*

165. That is, a programmer experienced in writing software involving cryptography would be able to get started right away on implementing these technologies. The rapid pace of technological change, combined with the public's growing awareness of cryptography, means that these technologies could conceivably become available in the immediate future.

between legal doctrine and technical realities, Part V focuses its attention on the potential impact of purely technological variations. Each proposed technology has the potential to provide greater security for individuals against both governments and private actors. The potential users include not only child pornographers and terrorists, but also whistleblowers, activists, political dissidents, and others. Together, this collection of users constitutes a market of not insignificant size, whose demand is likely to be met one way or another.

The examples given are selected with an eye to variety: for example, some (e.g., the keyloggers of Section V.F) highlight potential difficulties with the enter-the-password approach to compelling decryption, whereas others (e.g., the kill switches of Section V.C) highlight potential difficulties with essentially all the other approaches to compelling decryption. When the example technologies from multiple Sections are used in combination, yet more intricate doctrinal issues may arise. Overall, the example technologies described herein would tend to make compelling decryption more difficult; however, the possibility of existing or future technologies whose widespread adoption would make compelling decryption easier rather than harder should not be discounted (fingerprint-based encryption is one such example).

A. Random Data May Just Be Random Data

In many compelled decryption cases, the court examines the question of whether the government has knowledge of the existence of any electronic files or other information within a seemingly encrypted drive.[166] Indeed, courts have typically required the government to demonstrate such knowledge in produce-the-decrypted-contents cases.[167]

In some cases, the task of establishing knowledge of the existence of information hidden beneath encryption presents little difficulty. In *Boucher II*, for example, a government agent had examined the laptop before it was decrypted,[168] and in both *Gelfgatt* and *Fricosu* the defendants had

166. Part V examines the courts' approaches to date to answering the question of existence of encrypted data. Part VII gives a more involved treatment of the general meaning of existence in the context of decrypted data, independently of the manner in which the courts have treated the subject.

167. *See, e.g.*, United States v. Doe (*Doe II*), 670 F.3d 1335, 1347 (11th Cir. 2012) ("[T]he Government has not shown that it had any prior knowledge of either the existence or the whereabouts of the [files]." (second alteration in original) (quoting United States v. Hubbell, 530 U.S. 27, 45 (2000))).

168. *In re* Grand Jury Subpoena to Sebastien Boucher (*Boucher II*), No. 2:06-mj-91, 2009 WL 424718, at *2 (D. Vt. Feb. 19, 2009).

intimated that there was information on the encrypted computers that would be safe from law enforcement.[169]

In stark contrast, the government in *Doe II* presented no specific evidence that there were any encrypted files on the hard drive in question.[170] Instead, the government argued that it "[knew] of the 'existence' and 'whereabouts' of the decrypted records it [had] subpoenaed because the government already physically possesse[d] those records."[171] To support its belief that the hard drives are indeed encrypted, the government "introduced an exhibit with nonsensical characters and numbers, which it argued revealed the encrypted form of data that it [sought]."[172] The government argued that because these nonsensical characters were consistent with the use of encryption, it was a foregone conclusion that the hard drive was indeed encrypted.[173] Then because the hard drive was encrypted, the existence of the corresponding "decrypted records" was also a foregone conclusion.[174]

The Eleventh Circuit rightfully found the government's argument unconvincing.[175] Rejecting the second half of the argument, the court pointed to the testimony of the government's forensic examiner who, when asked "whether the random characters definitively indicated that encrypted data [was] present or instead could have indicated blank space , . . . conceded, 'Well, you would see random characters, but you wouldn't know necessarily whether it was blank,'" and moreover, when asked whether the "random data [could have been] just random data," responded that "anything is possible."[176] The Eleventh Circuit concluded, "because the TrueCrypt 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."[177] As the court reasoned, just as a locked vault may contain nothing, there may be no meaningful data hidden within an encrypted drive.[178] An empty drive and a drive filled with data would become indistinguishable to any party ignorant of the password.

The first half of the government's argument — that a hard drive filled with nonsensical characters is encrypted — is also problematic. Encrypting a drive, empty or not, requires a password and involves per-

169. Commonwealth v. Gelfgatt, 11 N.E.3d 605, 615 (Mass. 2014); United States v. Fricosu, 841 F. Supp. 2d 1232, 1236 (D. Colo. 2012).
170. *Doe II,* 670 F.3d at 1347.
171. *Id.* at 1346–47 (emphasis omitted).
172. *Id.* at 1340.
173. *Id.* at 1346–47.
174. *Id.*
175. *Id.* at 1347–49.
175. *Id.* at 1347.
177. *Id.*
178. *Id.*

forming mathematical operations to obtain a sequence of random-looking characters and numbers. Naturally, random-looking characters and numbers can be generated directly, simply by choosing random characters and numbers, forgoing the use of encryption altogether. Random data generated this way truly "is just random data."[179] Moreover, filling a drive with random data is not difficult or unusual: many disk formatting[180] programs offer a user-friendly option to overwrite a disk with random data,[181] and this is a common method to erase the data on a drive in an irrecoverable fashion.[182] A drive filled with truly random data corresponds to the physical analogy described in Part II of a solid block of wood carved to look like a chest, which could not possibly contain anything at all.

The forensic examiner's inability to determine whether the drives had meaningful data stored on their encrypted portions, or the encrypted portions were simply blank, or they were just filled with random data rather than encrypted at all, was the result of a deliberate design goal of the program TrueCrypt which Doe used to encrypt the drives.[183] Other encryption software, such as VeraCrypt, employs similar design principles.[184]

B. Authenticity and Deniable Encryption

Establishing the authenticity of evidence is crucial to a criminal investigation, and is paramount in the doctrine of act-of-production testi-

---

179. *Id.*

180. Disk formatting is the process of setting up a digital data storage device, such as a hard disk drive, for initial use. The storage device need not necessarily be empty before formatting, and is transformed to an empty initial state by the process of formatting.

181. For example, the secure erase feature of Mac OS X's Disk Utility program involves overwriting with random data. Tom Nelson, *How To Securely Wipe the Data Stored on a Drive in macOS High Sierra*, ROCKET YARD (May 29, 2018), https://blog.macsales.com/44781-how-to-securely-wipe-the-data-stored-on-a-drive-in-macos-high-sierra [https://perma.cc/7JVA-YSCV]. Other programs such as Eraser offer a direct option to overwrite with random data. *Eraser*, SOURCEFORGE, https://sourceforge.net/projects/eraser [https://perma.cc/8EHD-V3K4].

182. For example, the Department of Defense's data sanitization standards employ this method. NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL: DOD 5220.22-M, U.S. DEP'T OF DEF. (Feb. 28, 2006), http://www.dss.mil/documents/odaa/nispom2006-5220.pdf [https://perma.cc/P5DZ-H8P9].

183. *Doe II,* 670 F.3d at 1340 n.11 ("[F]ree space on any TrueCrypt volume is always filled with random data when the volume is created and no part of the (dismounted) hidden volume can be distinguished from random data." (alteration in original) (quoting *Hidden Volume*, TRUECRYPT, http://www.truecrypt.org/docs/?s=hidden-volume (last visited Jan. 31, 2012, according to the source; no longer available at time of writing)).

184. *See, e.g.*, *Security Requirements and Precautions Pertaining to Hidden Volumes*, VERACRYPT, https://www.veracrypt.fr/en/Security%20Requirements%20for%20Hidden%20Volumes.html [https://perma.cc/8LYC-ZCRS].

mony.[185] In most of the compelled decryption cases examined in Part IV, courts either held that the government was able to independently authenticate the evidence or never directly addressed the question.[186]

Stahl and *Gelfgatt*, however, suggest an intriguing alternative: that the issue of authentication is all but irrelevant in the context of compelled decryption.[187] In *Stahl*, the court made this point explicitly, holding that passwords are "self-authenticating."[188]

Gelfgatt implicitly adopts the same reasoning, stating that decryption "does not present an authentication issue" because Gelfgatt was "merely entering a password into encryption software."[189] The court relied on the idea that a password is unambiguously authentic if its entry into decryption software appears to result in successful decryption.

The idea that a password is self-authenticating may seem plainly true. A key either opens a locked safe or it does not; so too, a password either decrypts a drive or it does not. However, both a safe and an encrypted drive might have two keys and two compartments: the first key opens the main compartment while a second key opens a hidden compartment whose existence is secret. In the case of a physical safe, a hidden compartment could be discovered with enough expertise and persistence. In the case of an encrypted drive, detecting the existence of a hidden virtual compartment with an appropriate configuration of settings is as infeasible as decrypting an encrypted drive without knowledge of the password. This is true even if the password for the "main compartment" is known.

With a special type of encryption called "deniable encryption,"[190] a user may create a "hidden volume,"[191] which may be thought of as a vir-

---

185. *See, e.g.*, *In re* Grand Jury Subpoena, Dated Apr. 18, 2003, 383 F.3d 905, 912 (9th Cir. 2004) ("The authenticity prong of the foregone conclusion doctrine requires the government to establish that it can independently verify that the compelled documents 'are in fact what they purport to be.'" (quoting United States v. Stone, 976 F.2d 909, 911 (4th Cir. 1992))).

186. As remarked by the District Court for the Northern District of California: "[T]he authenticity element is routinely cited but only applied loosely if at all." *In re* Search of a Residence in Aptos, California 95003*,* No.17-mj-70656-JSC-1, 2018 WL 1400401, at *10 (N.D. Cal. Mar. 20, 2018.).

187. *Cf.* Brief for the Commonwealth at *29, Commonwealth v. Jones, No. SJC-12564 (Mass. filed Aug. 27, 2018), 2018 WL 4859923 ("There is no real dispute here that the Commonwealth satisfied two of the three elements of the foregone conclusion analysis, namely that the PIN exists and is authentic." (citing Commonwealth v. Gelfgatt, 11 N.E.3d 605, 615–16 (Mass. 2014); State v. Stahl, 206 So. 3d 124, 136–37 (Fla. Dist. Ct. App. 2016))).

188. *Stahl*, 206 So. 3d at 136 ("If the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic."); *see also* Commonwealth v. Davis, 176 A.3d 869, 875 (Pa. Super. Ct. 2017) (quoting and agreeing with *Stahl*, 206 So. 3d 124).

189. Commonwealth v. Gelfgatt, 11 N.E.3d 605, 616 n.14 (Mass. 2014).

190. "Deniable encryption" is used within different parts of the cryptography and computer security community to mean several different things. The differences in definition can be subtle in nature, especially to a nontechnical reader. The definition presented here is chosen for its relevance to the present subject matter, and is not to be considered canonical in the technical literature.

tual compartment whose very existence is impossible to determine without the correct password.[192] Such schemes typically employ a second password, which this Article calls a "duress password," that will partially decrypt a drive (typically revealing something innocuous) while the contents and existence of the hidden volume remain secret.[193] This is possible for the very reasons raised in Section V.A: namely, it can be impossible to tell whether a hard drive or some portion thereof contains meaningful encrypted information or is just random data. Not only are the true contents of the encrypted data hidden by a duress password, but also, the very existence of the alternate (true) password remains secret.

Deniable encryption is no mere hypothetical: versions of it have been commercially available since at least 2000.[194] For example, the encryption software VeraCrypt claims to provide deniability powerful enough to hide the existence of whole virtual drives full of information, file systems, and even operating systems.[195] Deniable encryption is even alluded to in *Doe II*[196] and *Gelfgatt*.[197]

Nor has the idea that deniable encryption complicates compelled decryption doctrine been absent from scholarly discussion.[198] Timothy Wiseman argues that to compel the production of files hidden by denia-

---

It is also pertinent to briefly mention a different cryptographic technique, called steganography, which raises issues similar to those raised by deniable encryption. Steganography encompasses a very broad range of techniques for storing secret data undetectably within other, innocuous data or objects. Fabien A. P. Petitcolas, Ross J. Anderson & Markus G. Kuhn, *Information Hiding — A Survey*, 87 IEEE PROC. 1062, 1062 (1999). This Article does not discuss steganography in more detail, but mentions it here for completeness, as it seems to raise many of the same questions as deniable encryption. For a technical survey of "information hiding" techniques including steganography, see generally *id.* Legal issues raised by steganography and compelled decryption are considered briefly in Timothy A. Wiseman, *Encryption, Forced Decryption, and the Constitution*, 11 I/S: J.L. & POL'Y FOR INFO. SOC'Y 525 (2015).

191. A hard drive is a physical object while a volume is a virtual, software-defined organizational subdivision of the hard drive's storage space. In terms of an analogy: whereas the hard drive is like a library (the physical building), a volume is like the nonfiction section.

192. *See, e.g.*, *Hidden Volume,* VERACRYPT, https://www.veracrypt.fr/en/Hidden%20Volume.html [https://perma.cc/FU2B-CJLA].

193. *See, e.g.*, *id.*

194. *See, e.g.*, Suelette Dreyfus, *The Idiot Savants' Guide to Rubberhose*, MARUTUKKU (Oct. 29, 2012), https://archive.is/20121029045140/http://marutukku.org/current/src/doc/maruguide/t1.html [https://perma.cc/SHF2-7R7E] (taken from ARCHIVE.TODAY).

195. *See generally Hidden Volume*, *supra* note 189; *Hidden Operating System*, VERACRYPT, https://www.veracrypt.fr/en/Hidden%20Operating%20System.html [https://perma.cc/22EF-6UFT].

196. United States v. Doe (*Doe II*), 670 F.3d 1335, 1340 (11th Cir. 2012) ("[TrueCrypt] can create partitions within a hard drive so that even if one part of the hard drive is accessed, other parts of the hard drive remain secured.")

197. Commonwealth v. Gelfgatt, 11 N.E.3d. 605, 616 n.10 (Mass. 2014) (ordering Gelfgatt "[n]ot to enter a false or 'fake' password or key, thereby causing the encryption program to generate 'fake, prepared information' as advertised by the manufacturer of the encryption program.").

198. *See, e.g.*, Wiseman, *supra* note 190.

ble encryption, the government would need to establish knowledge of the "existence of the hidden [files]" along with "the location of the requested files with reasonable particularity."[199] Wiseman's approach, broadly speaking, is to apply the existence and location analyses that he uses for standard (non-deniable) encryption, to the additional encryption present when using deniable encryption.[200] In contrast, the discussion that follows focuses on authenticity, with the view that deniable encryption introduces a fundamentally new authenticity concern.

Deniable encryption challenges the notion that passwords are self-authenticating. Consider a prototypical compelled decryption case in which a defendant is forced to reveal her password to the government (as in *Stahl*) or to enter the password directly into the encrypted device (as in *Gelfgatt*). If there is only a single password that makes the device accessible, then perhaps there is indeed no authenticity issue. But even the possibility that the encryption employed is deniable makes authenticity — of both the password used to decrypt a drive and the information thereby produced — a central consideration to the foregone conclusion analysis.[201] The government might respond to the challenge of deniability in a number of ways. This Article suggests and explores some possible approaches; however, none of these seem wholly satisfactory.

First, the government may attempt to do as it did in *Gelfgatt* and directly forbid a defendant from using a duress password.[202] This approach does not solve the authenticity issue; rather, it ignores it. If the government has no way to authenticate the password used or the information thereby revealed, the government would be depending on the defendant to use a real password. The government would be relying on the "truthtelling"[203] of the defendant, leaving the Fifth Amendment challenge unresolved.

Second, it might attempt to demonstrate knowledge that the defendant is not using deniable encryption. While VeraCrypt offers deniability features, many encryption programs do not.[204] Furthermore, creating an undetectable hidden volume using VeraCrypt requires significant care and technical sophistication.[205] The government may be able to argue that it is a foregone conclusion that the defendant is not using deniable encryption (and therefore that the password should be considered self-

199. *Id.* at 573.

200. *See id.*

201. *See id.*

202. *See* Commonwealth v. Gelfgatt, 11 N.E.3d 605, 611 (Mass. 2014).

203. *Cf.* Fisher v. United States, 425 U.S. 391, 411 (1976) ("Surely the Government is in no way relying on the 'truthtelling' of the taxpayer to prove the existence of or his access to the documents.").

204. *See Comparison of Disk Encryption Software*, Wikipedia, https://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software#Features [https://perma.cc/EZ4C-VFVK].

205. *See supra* note 195 and accompanying text.

authenticating) if it could demonstrate that a defendant was using software that does not support deniable encryption or that the defendant lacked the knowledge or skills to successfully use such features. The power of this approach would likely diminish over time as deniability becomes more common and simpler to use.

Third, the government might attempt to demonstrate knowledge that the defendant is indeed using deniable encryption, and that it knows of the existence of hidden data that was not decrypted by the proffered password. This might be possible even if the government lacks any specific knowledge of the contents of an encrypted drive. For example, if the defendant lacks sufficient technical sophistication, the attempted use of deniable encryption could leave behind a trail of evidence detectable by digital forensic experts.[206] Against a technically savvy defendant, however, this approach would likely fail.

Alternatively, in some cases, the government might also know of certain files on the computer that were not produced by the given password. For example, in *Boucher II* a government agent had already seen child pornography on the computer in question.[207] If the password entered by Boucher failed to produce the illicit materials, the government could potentially argue that Boucher had used a duress password.

Courts generally agree that government knowledge of the precise content of encrypted data is unnecessary for compelled decryption.[208] However, the possibility of a technically savvy defendant using deniable encryption could force the government to have precisely such knowledge in order to establish authenticity and compel decryption. If the government cannot be certain whether deniable encryption is being used, this may be true even for defendants who are not actually using deniable encryption. Moreover, such knowledge of the contents of an encrypted computer may be harder to establish than it might seem, as discussed in the next Section.

C. Data Persistence and Kill Switches

In *Boucher II*, the court concluded that compelling Boucher to produce the decrypted contents of his computer would "add[] little or nothing to the sum total of the Government's information about the existence and location of files that may contain incriminating information," because it already "[knew] of the existence and location" of the drive and

206. *See id.*

207. *In re* Grand Jury Subpoena to Sebastien Boucher (*Boucher II*), No. 2:06-mj-91, 2009 WL 424718, at *2, (D. Vt. Feb. 19, 2009).

208. *E.g.*, United States v. Doe (*Doe II*), 670 F.3d 1335, 1349 n.28 (11th Cir. 2012).

files.[209] This conclusion was based upon Boucher's interaction with a border control agent:

> The agent located and examined several videos or images that appeared to meet the definition of child pornography. The agent arrested Boucher, seized the laptop and shut it down.[210]

The court's logic is apparent: the illicit files were on the laptop when the agent shut it down. Shutting down a computer preserves its contents in some form — therefore, the files remained on the laptop in some form.[211]

However, a syllogism is only as sound as its premises, and the premise that data persists upon shut down is fragile. Suppose that there are two identical computers each using a hypothetical encryption software Kill Krypt. Kill Krypt has an optional *kill switch* setting which is armed on one computer and disarmed on the other.[212] On the computer with the disarmed kill switch, pressing the power button causes Kill Krypt to encrypt the hard drive using the user's password and then to turn off the computer. The computer with the armed kill switch, on the other hand, can be shut down in two ways: either by pressing the power button or by using a special sequence of keystrokes. If the special sequence is used, Kill Krypt encrypts and shuts off the computer as normal. If instead the power button is used when the kill switch is armed, Kill Krypt overwrites all data on the hard drive with random, meaningless data before shutting down.

The hard drive of a computer shut down using the power button will only contain encrypted data — rather than random data — if that computer was *not* using Kill Krypt with an armed kill switch. Thus, for the existence of some encrypted information to be a foregone conclusion, it must also be a foregone conclusion that there was no armed kill switch. Without the password, it is infeasible to determine whether an armed kill switch was triggered by inspecting the resulting hard drive, because a

---

209. *Boucher II*, 2009 WL 424718 at *3 (internal quotation marks omitted).

210. *Id.* at *2.

211. The facts of *Boucher II* already illustrate the falsehood that "shutting down a computer preserves its contents" (without the caveat "in some form"). When the agent was perusing the drive, the computer's contents included *unencrypted* child pornography. *Boucher II,* 2009 WL 424718 at *2. After being shut down, the computer no longer contained unencrypted child pornography (though it plausibly contained *encrypted* child pornography). *Id. Boucher II* thus gives a real-world example of the contents of a computer undergoing a complex transformation when shut down. Overwriting the hard drive with meaningless data is a much simpler task.

212. Unlike some of the other example technologies herein, "kill switch" is not a standard term in the technical literature. The terminology is the authors'.

drive with encrypted data is generally indistinguishable from a drive filled with random data.

To the best of the authors' knowledge, commercially available encryption software does not offer this sort of kill switch. However, there are no significant technological barriers to their development in the immediate future.[213] Moreover, though this discussion focuses on kill switches, a variety of hypothetical technologies could raise similar issues.[214]

Let us return to *Boucher II*, keeping in mind the Kill Krypt hypothetical. If Boucher had been using a disarmed computer, then the illicit files would have remained on the computer, albeit encrypted. If Boucher had been using an armed computer, then the government agent's act of shutting down the laptop would have destroyed the files. In the latter case, the government could no longer know of the existence and location of the files, because the files would have been destroyed. Even a cooperative Boucher would have been unable to decrypt the hard drive. There would have been nothing to decrypt; the password would have born no relation to the now random contents of the drive. In the hypothetical world where Kill Krypt exists, establishing existence of the files as a foregone conclusion implicitly requires the government to establish that it is a foregone conclusion that no armed kill switch was on the computer when it was shut down.

The possibility that the encryption scheme employed includes a kill switch complicates the foregone conclusion analysis. One possible solution for the government would be to demonstrate that the computer in question did not have a kill switch. However, in a possible future where this functionality is in wide use, the government may still be able to demonstrate that a defendant was using software that does not support a kill switch, that the defendant lacked the knowledge or skills to success-

---

213. Indeed, it would be much simpler than encrypting the hard drive. *See supra* note 211.

214. For example, it is fairly common for a computer or phone to support the option to automatically erase all data after a certain number of failed password attempts. *E.g.*, *iOS Security: iOS 12*, *supra* note 5, at 18; *Cross Reference: CryptKeeper.java*, ANDROIDXREF (2011), http://androidxref.com/9.0.0_r3/xref/packages/apps/Settings/src/com/android/settings/CryptKeeper.java, [https://perma.cc/B8LC-L29P] (providing Android source code that automatically erases the phone after failed password attempts on lines 97 and 210–16). Additionally, many computers and phones can have their contents remotely erased, i.e., a remote action can trigger the erasure of the contents, if the device is connected to the Internet. *E.g.*, *iOS Security: iOS 12*, *supra* note 5, at 81–82; *Find, Lock, or Erase a Lost Android Device*, GOOGLE (2018), https://support.google.com/accounts/answer/6160491 [https://perma.cc/VW4L-GVWK].

The Article discusses the hypothetical of kill switches, rather than the more familiar technology of remote erasure, because kill switches give rise to the interesting phenomenon that it is infeasible to distinguish between a drive resulting from encryption and a drive resulting from a triggered kill switch. This indistinguishability is core to the doctrinal challenge discussed here. While existing implementations of the other data-erasing technologies just described do not exhibit this property, it is conceivable that future implementations might.

fully use such features, or that an armed kill switch was not triggered (i.e., that the computer was shut down in a manner that did not destroy the data).

A different approach the government could take would be to compel the defendant to enter the password into the computer (like in *Gelfgatt*), rather than produce the decrypted contents. The court in *Gelfgatt* identified a number of testimonial statements implicit in the act of entering a password: "ownership and control of the computers and their contents, knowledge of the fact of encryption, and knowledge of the encryption key."[215] Notably absent was knowledge of the existence of encrypted data which was crucial to the analysis of the kill switch in a produce-the-password case like *Boucher II*.[216]

D. Testimonial Aspects of Biometric-Based Encryption

Encryption based on biometrics,[217] especially fingerprint-based systems on Apple iPhones, is becoming increasingly commonplace. Existing precedent suggests strongly that the use of biometric information to decrypt can be compelled with relative ease.[218] The purely physical act of pressing one's finger onto a sensor neither communicates information, nor reveals the contents of the mind, nor relies on the truthfulness of the finger's owner.[219]

That biometric-based decryption communicates little or no implicit testimony is not inherent, however. Biometric-based decryption can be modified in ways to enhance the protections afforded by the Fifth Amendment by adding some non-biometric, testimonial aspects. Some examples of such modifications are described below. The proposals generally have the effect of blurring the distinction between biometric-based and password-based systems, potentially reintroducing the additional doctrinal complexities of the latter.

---

215. Commonwealth v. Gelfgatt, 11 N.E.3d 605, 615 (Mass. 2014).

216. It may be tempting to suggest that there is an additional testimonial statement communicated to the government in this hypothetical, namely, the knowledge of whether a kill switch was armed. Without the password, the government is unable to determine whether the kill switch was armed or disarmed. Once the defendant enters a password, it becomes clear. However, this information is not implicit in, or created as a by-product of, the physical act of entering a password. Similarly, the fact that the government learns the decrypted contents of a computer after a password is entered does not by itself constitute testimonial communication implicit in the act of entering a password.

217. The precise meaning intended here is encryption systems where decryption is effected by entering biometric information. For more discussion, see *supra* note 27.

218. *See supra* Section IV.E.

219. *See id.*

1. Choosing Between Multiple Possible Biometrics

Although which finger is used for fingerprint-based encryption is not typically emphasized today,[220] what if, when setting up the encryption, the device instructed the user to choose a *secret* finger — or sequence of fingers — to place on the fingerprint reader?[221] Then the knowledge of which finger or fingers to use would be the contents of the user's mind, even though the fingerprint itself would still be purely physical evidence.

The government could require a defendant to place each finger onto the sensor in turn. However, if the phone deletes all its contents after a few failed fingerprint attempts, the government might risk losing the evidence it seeks.[222] Alternatively, the government could instead order the defendant to use the *correct* finger to decrypt, closely resembling an enter-the-password case.

2. Location-Based Decryption

Smartphones have built-in GPS functionality that allows them to determine their own geographical location. A straightforward enhancement to fingerprint- or password- based encryption would be to add the requirement that (perhaps only for particularly sensitive files), decryption may only take place when the smartphone is located in a secret, user-specified location.[223] Compelling decryption in such a case could easily

220. *See, e.g.*, *Use Touch ID on iPhone or iPad*, APPLE (Oct. 1, 2018), https://support.apple.com/en-us/HT201371 [https://perma.cc/Z64W-VA8X]. Apple's instructions for setting up Touch ID. An instruction says, "Touch the home button with your finger" and none of the instructions specify which finger. *Id.* A picture accompanying the instructions shows a person with their thumb on the fingerprint reader; given the design of the iPhone, the thumb is a convenient finger to use when holding the phone with one hand. *See id.*

221. The idea of uncertainty surrounding which finger is used to authenticate to a smartphone has previously been raised in this context. *See, e.g.*, Orin Kerr, *Can Warrants for Digital Evidence Also Require Fingerprints to Unlock Phones?*, WASH. POST (Oct. 19, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/19/can-warrants-for-digital-evidence-also-require-fingerprints-to-unlock-phones/ [https://perma.cc/6MQW-QV57].

222. Another situation in which such a feature would pose similar risks to the government is if it tried to compel many different people to place their fingers on a sensor. *Cf. In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1067 (N.D. Ill. 2017) (denying warrant to compel any individual present during the search to place her finger on the Touch ID of any iPhone implicated in the search).

223. Making the login procedure dependent on the user's location is a feature that is already widespread, e.g., on Android smartphones: Android's "Trusted Locations" feature allows users to turn off the screen lock when in trusted locations like home. *See* David Nield, *How To Set Up Trusted Locations in Android Lollipop*, GIZMODO (Dec. 1, 2014), https://gizmodo.com/how-to-set-up-a-trusted-location-in-android-lollipop-1664072507 [https://perma.cc/4GB3-H3G2]. The present suggestion is almost the opposite: instead of *relaxing* security in a location-dependent way, location-based decryption would *strengthen* it by only allowing a login to work when in certain specific locations.

cause the auxiliary testimonial communication of the secret location. If the user did not require frequent access to the encrypted files and chose a remote location for added security, then there could also be associated logistical challenges to compelling decryption.

3. Situation-Dependent Decryption

The ability to decrypt a device such as a smartphone could easily be tied to other specific properties of the surrounding environment. For example, the decryption might work only if the fingerprint were placed on the reader while the phone's clock's second hand is between seventeen and nineteen. Alternatively, the decryption might be designed to work only if the phone is held or moved in a certain way.[224] Yet another possible scheme would be to have the phone screen scroll through a sequence of pictures and to enable decryption only if the fingerprint is placed on the sensor while a specific type of picture (say, of cats) is showing. Similar modifications could apply to password-based decryption as well.

These sorts of systems could pose yet more complex challenges if coupled with the other technologies discussed in Part V. For example, the phone might erase all its data or decrypt to "decoy" content, if the fingerprint is entered while the second hand is between five and seven, or while the screen is showing a picture of a chameleon.

4. Voice Recognition for Commands

Voice command recognition is becoming an increasingly common feature of many devices, and a device's ability to recognize and respond to (only) its owner's voice, or log in using the user's voice, is present in some commonplace devices.[225] A natural way to make voice-based encryption more testimonial would be to require the user to say a specific secret phrase in order for decryption to work.

As a very different example, consider a smart (perhaps self-driving) car that keeps encrypted logs of the locations that it has been, that can only be decrypted or used when the owner gives a voice command. Could the government compel the car owner to say to the car, "Go to the

224. Smartphones have rotation and tilt sensors that can determine the orientation of the phone relative to the Earth.

225. For example, Android smartphones have the "Voice Match" feature, which allows the phone to respond to an "OK, Google" voice command from its owner even when the phone is locked. *Set Your Device to Automatically Unlock*, GOOGLE, https://support.google.com/nexus/answer/6093922?hl=en [https://perma.cc/9GH5-SL8R]. Amazon's Alexa devices have a similar feature called "Voice Purchasing" which allows easy ordering of purchases by voices recognized as trusted. *Manage Voice Purchasing Settings*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201952610 [https://perma.cc/7KC3-ZSYU].

place I went last Saturday afternoon," or "When was the last time I left the state?" This hypothetical resembles *Doe I*, in which a defendant was compelled to sign a form authorizing the release of certain records to law enforcement without acknowledging that those records existed.[226] As in *Doe I*, uttering the above phrases would not by itself constitute testimony, in contrast to the secret phrase example and the other examples in this Section.

E. Possession of Encrypted Data Without the Ability To Decrypt

A person's possession of an encrypted file need not imply that that they have the ability to decrypt the file. For example, they may simply be acting as a custodian for the real owner of the file, who is able to decrypt it. It is common today for computer users to store their files not only on their computers directly, but also on cloud servers that belong to companies such as Google and Dropbox, which offer services within which users pay to store data, possibly encrypted, on the company's machines.[227] This data can be accessed by logging in from any machine with an internet connection, rather than on just a single home computer. In terms of the familiar physical analogy of safes, this is analogous to a company that rents out safes in a building, but allows the renters to set their own combination and store what they wish. The company's possession of the safe implies neither that it has the ability to unlock the safe, nor that it has knowledge of what is inside.

Today, it is less common for a private person to be acting as a data custodian,[228] but it is eminently possible and arguably likely to become much more common. In recent years, new encrypted file storage services have cropped up,[229] which allow anyone with spare storage space (say, on their laptop computer) to join the system and get paid for securely storing other people's files in encrypted form. Customers are assured that their files will not be readable to anyone but themselves, thanks to the encryption used. As the sharing economy[230] continues to grow, people who have spare space to store digital data, or with access to cheap digital storage, may participate in such services and thereby intentionally pos-

---

226. Doe v. United States (*Doe I*), 487 U.S. 201, 201 (1988).

227. *See generally* GOOGLE DRIVE, https://www.google.com/drive/ [https://perma.cc/L8YN-3A2n]; DROPBOX, https://www.dropbox.com/ [https://perma.cc/5GUZ-97KM].

228. As noted in Part III, the Fifth Amendment privilege against self-incrimination extends only to natural persons.

229. *See, e.g.*, STORJ, https://storj.io [https://perma.cc/2U78-KFKM]; SIA, https://sia.tech [https://perma.cc/7CZ5-9GA8].

230. "Sharing economy" is a term used to describe economic activity arising from peer-to-peer sharing of access to goods and services. Examples of prominent businesses in the sharing economy include eBay, Uber, Lyft, and Airbnb. Some other examples not based on a profit model are craigslist and BitTorrent.

sess data that is not accessible to them in a meaningful (i.e., decrypted) form. If this were the case, the presence of encrypted data on a person's computer would not even imply that the corresponding decryption is accessible or belongs to the computer's owner.

This is not the only way that the possessor of encrypted data might not have the ability to decrypt it. For example, the data might be owned by multiple stakeholders (such as a married couple, or business partners) who encrypt the data in a special way so that it can only be decrypted if *both* people agree.[231] While this sort of multi-stakeholder encryption is not in widespread use today, it is possible by a straightforward combination of existing software. For example, such a system could work by having both parties in possession of a distinct secret password, and having the decryption require both correct passwords. If one party destroys her password, then she unilaterally renders the data irrecoverable in a permanent way.

The use of technologies like these could render the task of establishing a person's ability to decrypt some encrypted data a more granular one: instead of arguing that a person can or cannot decrypt an entire storage device, different files might require separate arguments (assuming it can even be ascertained whether there are one or many files on the device). In past cases, a defendant's sole ownership and use of a computer or hard drive along with the ability to decrypt some portion thereof has been used to argue that it is a foregone conclusion that the defendant can decrypt all of the encrypted data.[232] When acting as a data custodian by storing some other party's encrypted data, or as just one stakeholder in a multi-stakeholder encryption, a defendant would be unable to follow any legal order to decrypt certain files.

F. Keystroke Logging Revealing the Contents of the Mind

Courts have generally found that entering a password (or producing decrypted contents) is testimonial only insofar as the act implicitly communicates something about the knowledge or beliefs of the person entering the password.[233] Accordingly, under appropriate circumstances, these courts have permitted the government to compel a defendant to effect decryption by entering a password into a device in the government's

---

231. This is possible using a relatively simple cryptographic technique called "secret sharing." For a more detailed technical exposition of secret sharing, *see, e.g.*, KATZ & LINDELL, *supra* note 20, at 501–03.

232. *See, e.g.*, *In re* The Decryption of a Seized Data Storage Sys. (*Feldman*), No. 13-M-449, 2013 U.S. Dist. LEXIS 202353, at *4 (E.D. Wis. Apr. 19, 2013); *see also supra* note 112.

233. *See supra* Section IV.C.

control, provided that the government agrees not to "view or record the password or key in any way."[234]

The distinction made between *entering* and *revealing* a password implicitly assumes that the only way by which the government might learn a password entered by a defendant is by "view[ing] or record[ing]" it.[235] But what if the password was recorded upon entry, not by the government, but by the very computer being decrypted?

Imagine a strange combination safe where the number pad used to enter the combination on the outside of the safe is connected to a small printer inside the safe. Each time one presses a button on the outside, the corresponding digit is printed on paper within. When the safe is opened using a memorized password, the contents of the mind (the combination) are made physically manifest. Under what circumstances, if any, could the government compel a defendant to open such a safe?

Observe that this differs importantly from the scenario in which the defendant simply writes the combination on paper and locks it within the safe. The difference is in whether the creation of the physical record is compelled. If the record of the combination was voluntarily written down, then its contents enjoy no Fifth Amendment protection.[236] In the case of the printer, the written record is created only as a result of entering the combination. By compelling a defendant to open the safe, the government compels the creation of this potentially testimonial record.

In the digital world, the printer in the safe is analogous to something called a "keylogger": a program that records the keys pressed on a keyboard.[237] This record is stored on the computer in a file called a "log file."

Keyloggers are commonplace. They have long been used to covertly record passwords typed on electronic keyboards: in malware, in federal investigations,[238] and in Soviet espionage during the Cold War.[239]

---

234. Commonwealth v. Gelfgatt, 11 N.E.3d 605, 622 n.10 (Mass. 2014).

235. *Id.*

236. *See, e.g.*, United States v. Hubbell, 530 U.S. 27, 36 (2000) (quoting Fisher v. United States, 425 U.S. 391, 396 (1976)) ("Because the papers had been voluntarily prepared prior to the issuance of the summonses, they could not be 'said to contain compelled testimonial evidence.'").

237. Keyloggers (also called keystroke loggers) may also be physical devices instead of software. *Comparison Keyloggers*, REFOG, https://www.refog.com/comparison-of-hardware-and-software-keyloggers.html [https://perma.cc/57X6-U65H].

238. *See, e.g.*, Declan McCullagh, *Feds Use Keylogger To Thwart PGP, Hushmail*, CNET (July 20, 2007, 10:41 AM), https://www.cnet.com/news/feds-use-keylogger-to-thwart-pgp-hushmail (last visited Dec. 19, 2018).

239. *See, e.g.*, Dan Goodin, *How Soviets Used IBM Selectric Keyloggers To Spy on US Diplomats*, ARS TECHNICA (Oct. 13, 2015, 2:15 PM), https://arstechnica.com/information-technology/2015/10/how-soviets-used-ibm-selectric-keyloggers-to-spy-on-us-diplomats [https://perma.cc/5BVK-DHFX].

Much like the printer, the keylogger blurs the distinction between entering and revealing the password.[240] When a keylogger is present, forcing the defendant to enter a password entails forcing the defendant to make a record of the contents of her mind, a record that could readily be viewed by the government. The interaction between keyloggers and compelled decryption doctrine is of some immediacy given that keyloggers are quite commonplace.

Consider a prototypical compelled decryption case in which the defendant acknowledges her knowledge of the password and ability to decrypt (e.g., *Gelfgatt*), but in which the computer in question has a keylogger installed. Under what circumstances, if any, can the government compel a defendant to enter the password into such a computer?

The contents of the log file are testimonial and potentially incriminating, and the creation of the log file would arguably be compelled. Thus, decryption should not be compelled if the government subsequently has access to the log file containing the password. For example, either entering a password or producing the complete decrypted contents of the computer would entail the government gaining access to the log file.

This suggests that redacting the log file from the decrypted contents of the computer may be necessary for compelled decryption. Two potential approaches for the government to compel decryption in the presence of a keylogger are, briefly, as follows. One possibility would be to order the defendant to enter the password — causing the decryption of the data — and then require the defendant or a special master to find and delete the log file. An alternative would be to order the production of specific decrypted documents that do not include the log file. The applicability of these two approaches would depend on the specific circumstances of a case. For example, the latter approach would only be viable where the government has enough specific knowledge of the documents sought.

Just like deniable encryption, both of these approaches could make establishing the authenticity of the furnished files more challenging than in past compelled decryption cases. The defendant would no longer

240. Perhaps keyloggers are unnecessary for the password to be revealed. Indeed, security researchers have demonstrated that cryptographic keys used to decrypt a computer can, under certain circumstances, be fully recovered given a few minutes of physical access to the computer itself. *See, e.g.*, J. Alex Halderman et al., *Lest We Remember: Cold Boot Attacks on Encryption Keys*, PROCEEDINGS OF THE 17TH USENIX SECURITY SYMPOSIUM, July 2008, at 45.

The relevance of this demonstration in the present context is mitigated by two facts. First, while such an attack may be feasible, it is substantially more involved than recovering a password from a log file. This raises an interesting doctrinal question: does the ease or difficulty of learning contents of the defendant's mind from a compelled act affect whether the act is considered testimonial? If so, where does the threshold lie?

Secondly and more significantly, the cryptographic key recovered in this attack is something distinct from the password entered by the user. *See supra* note 27.

simply be entering a password or producing the complete contents of a decrypted computer, but rather would be filtering the results according to the government's instructions.

The preceding discussion assumes that the creation of the log file is compelled. Another strategy to compel decryption might be to attack this assumption: perhaps the government could argue that the voluntary installation of a keylogger on the encrypted computer somehow forfeits any Fifth Amendment protection over the password.

G. Decryption and the Use of the Contents of the Mind

A typical conception of a password is a short sequence of characters that is relatively easy to recall. Some passwords are used so frequently that entering them may become a physical act more than a mental one.[241] And while the act of entering a password to decrypt may implicitly relate some facts or beliefs, the government may compel it if the testimonial communication implicit in the physical act is a foregone conclusion.

We return now to the nature of testimony, discussed briefly in Part III. Justice Stevens wrote in his dissent in *Doe I*: "can [a defendant] be compelled to *use his mind* to assist the prosecution in convicting him of a crime? I think not."[242] Likewise, the Eleventh Circuit wrote that "[t]he touchstone of whether an act of production is testimonial is whether the government compels the individual to *use 'the contents of his own mind'* to explicitly or implicitly communicate some statement of fact."[243] Finally, the Supreme Court in *Hubbell* wrote that "[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."[244]

These excerpts can be interpreted in two different ways. One reading is that whether, and the extent to which, a defendant is forced to use his mind is germane to the determination of whether an act of production is testimonial. Read this way, use of the contents of the mind is sufficient to elevate an act to the level of testimony. This Article calls this the "use-alone" interpretation. An alternative is that use of the contents of the

---

241. In fact, this idea has been discussed in research designing cryptography in which a "password" consists of muscle memory movements, and it is deliberately difficult or impossible for the user to recall the password without employing muscle memory. *See* Hristo Bojinov et al., *Neuroscience Meets Cryptography: Designing Crypto Primitives Secure Against Rubber Hose Attacks*, PROCEEDINGS OF THE 21ST USENIX SECURITY SYMPOSIUM, Aug. 2012, at 129.

242. Doe v. United States (*Doe I*), 487 U.S. 201, 219 (1988) (Stevens, J., dissenting) (emphasis added); *see also supra* note 45.

243. *In re* Grand Jury Subpoena Dated March 25, 2011 (*Doe II*), 670 F.3d 1335, 1345 (11th Cir. 2012) (emphasis added) (quoting Curcio v. United States, 354 U.S. 118, 128 (1957)).

244. United States v. Hubbell, 530 U.S. 27, 43 (2000) (emphasis added) (quoting Curcio v. United States, 354 U.S. 118, 128 (1957)).

mind is not sufficient; additionally, "some statement of fact" must be communicated or revealed.[245] This Article calls this the "revelation" interpretation.

The distinction is subtle and the courts have yet to consider a case in which a defendant must make significant use of the contents of his mind to comply with a court order, but in which no statement of fact is thereby revealed to the government.[246] While it is difficult to imagine such a scenario in the physical world,[247] passwords that require mental effort are not only conceivable, they have already seen use in banking and social networking websites, as described below.[248] This raises the interesting doctrinal question of whether possibly extensive use of the contents of the mind is sufficient, absent their revelation, for testimoniality.

Online banking systems in a number of countries often check a user's passwords in a somewhat unusual way: instead of asking the user to type in the entire password, they ask only for selected characters from the password. [249] For example, the bank might request the second, fifth, and sixth characters of the user's password — and which characters are requested changes at each log-in.

Another example comes from Facebook. One way that Facebook used to identify users who forgot their passwords was to provide a series

---

245. *Doe II*, 670 F.3d at 1345; *see also* text accompanying *supra* note 243.

246. The only case of which we are aware that distinguishes the two interpretations is *State v. Stahl*, 206 So. 3d 124, 133–35 (Fla. Dist. Ct. App. 2016). That court adopted the second reading, that use of the contents of the mind alone does not suffice. *Id.* at 134. However, that court went even further, concluding that a password — though contents of the mind — has no testimonial significance and communicates no statement of fact, and can therefore be compelled. *Id.* at 134–35; *see also supra* note 87 and accompanying text.

247. For a physical-world hypothetical, we may consider modifying the facts of *Doe I*, 487 U.S. at 202–03. In that case, the government compelled Doe to sign a document authorizing his bank to reveal some information to law enforcement. *Id.* at 203. Doe was only compelled to perform a physical act (i.e., sign a document making no factual assertions) which was not considered testimonial. *Id.* If instead of requiring only a simple signature, the bank required something more mentally taxing (e.g., solving a crossword or translating some text into Yiddish), a court may have to decide if extensive use of the contents of the mind by itself suffices for testimony.

248. Note that the language in Section V.G uses the term "passwords" more loosely than that in the rest of the Article. Technically speaking, the two examples presented below use passwords for limiting access to certain information to specific users, rather than securing information using encryption. This task (called authentication by the computer security community) is very different from encryption. Nonetheless, the examples can be illustrative; from a technical perspective, similar examples could arise in the context of encryption. The authors have chosen to avoid using the term "authentication" to prevent confusion with the notion of authenticity of evidence discussed throughout this Article.

249. *See* David Aspinall & Mike Just, *"Give Me Letters 2, 3 and 6!": Partial Password Implementations & Attacks*, PROCEEDINGS OF THE 17TH INT'L CONFERENCE ON FIN. CRYPTOGRAPHY & DATA SEC., April 2013, at 131 (figure 2) (noting that at least sixteen banks in four countries, including the United Kingdom, use this log-in method).

of photographic challenges.[250] The user was presented with a series of photographs of her friends and had to identify the people in the photographs.[251] If the user was able to identify most of the subjects, the log-in attempt succeeded.[252]

In each example, successfully logging in requires the user to respond to a mental challenge. No matter how familiar a user is with her password or social network, these methods for logging in require some mental effort and cannot be considered a purely physical act. It is easy to imagine computer encryption software using similar password schemes.[253] To decrypt a file, the software could require significant use of the contents of the user's mind. Though there would be some associated technical challenges, it is in principle possible to create such software.

Supposing a case otherwise similar to *Gelfgatt*, then, let us consider the following natural question: could the government compel a defendant to decrypt a file or computer if the act of decryption is mentally taxing? Under the "revelation" interpretation, the government could compel decryption if all implicit testimonial communication is a foregone conclusion. Under the "use-alone" interpretation, however, the government could not compel decryption — regardless of what information it already knows. Even if neither the decrypted files nor the act of decryption would communicate anything testimonial, the act itself would require extensive use of the mind of the defendant. The defendant would, as Justice Stevens wrote, be "us[ing] his mind to assist the prosecution in convicting him of a crime."[254]

VI. REFLECTIONS

This Part reflects on the compelled decryption doctrine presented in Part IV and the collection of technological hypotheticals taken as a whole. Together, they suggest that while the doctrine sometimes turns on non-obvious technological details in surprising ways, with careful consideration of both technology and precedent it can be applied in a consistent manner. While a heartening finding, this should not discourage

250. Josh Constine, *Facebook Has Users Identify Friends in Photos To Verify Accounts, Prevent Unauthorized Access*, ADWEEK (July 26, 2010), http://www.adweek.com/digital/facebook-photos-verify [https://perma.cc/B6HQ-ESKU] (corroborated by personal experience of the authors).

251. *Id.*

252. *Id.*

253. The authors would love to hear from readers about any other types of log-in schemes that require "heavy" use of the contents of the mind.

254. Doe v. United States (*Doe I*), 487 U.S. 201, 219 (1988) (Stevens, J., dissenting) (emphasis added); *see also supra* note 45 and accompanying text.

reexamining our basic assumptions when reasoning about compelled decryption cases.

A. The Importance of Detailed Protocols

It is manifest, in both the cases and hypotheticals already discussed, that the doctrine of compelled decryption is sensitive not only to the facts presented by a particular case, but also to the action the government seeks to compel and even the details of exactly how the compelled action is to be carried out. This sensitivity is related to the fact that the government's desired outcome — obtaining the decrypted contents of a storage device already in its possession — is a non-testimonial byproduct of the action being compelled. Thus, the government may choose any of a number of different actions to request, which would produce the desired outcome as a byproduct.

When a physical item (e.g., a weapon or a paper document) is the object of the government's interest, the natural course of action is to compel the defendant to furnish it to the court. The testimonial aspects of the act of production can usually be discussed without specifying the precise way by which the defendant is to journey home, by which door she must enter the house, and the manner in which she must transport and furnish the requested item to the court. Varying these details cannot plausibly change the testimonial aspects of the action undertaken.

The opposite is true in compelled decryption cases. When the object of the government's interest is some or all of the decrypted files on an encrypted digital storage device that is in its possession, the precise manner by which the defendant is to furnish the files is significant. Indeed, this fact underlies much of the complexity of both the existing case law discussed in Part IV and the hypothetical cases in Part V. The most obvious illustration is the much weaker legal protections available for biometric-based than for password-based encryption.[255] Equally relevant is the distinction drawn in Part IV between enter-the-password cases and produce-the-decrypted-contents cases. This distinction is highlighted in the exploration of deniable encryption, kill switches, and the other technical hypotheticals of Part V.

It should be possible to compel decryption if and only if each of a sequence of steps that comprise the act of decryption can be compelled.[256] *Gelfgatt* refers to this sequence of steps as a "protocol."[257] If a single step cannot be compelled, then decryption should not be com-

255. *See supra* Section IV.E.

256. The relevant consideration is whether each step in the sequence would be compellable after the previous steps are performed, not whether the step can be compelled in isolation.

257. Commonwealth v. Gelfgatt, 11 N.E.3d 605, 622 n.10 (Mass. 2014)

pelled. Conversely, if each step in a sequence can be compelled, then the resulting decryption should be compellable. In drafting compelled decryption orders, law enforcement and courts should clearly specify the protocol for decryption. Failure to do so causes confusion, whereas precisely specifying the manner of decryption would likely tend to make rulings clearer and, hopefully, more consistent.[258]

Where there are a variety of ways to perform decryption, better specification of the manner of decryption may benefit both investigators and defendants. As an illustration, consider a hypothetical case in which either a fingerprint or a password will result in decryption, but in which the government does not know whether a defendant knows the password. Entering a password could communicate implicit testimony that using a fingerprint would not. Specifying that a fingerprint is to be used in a compelled decryption order limits the ability of a defendant to quash, benefiting the government. A compelled decryption order issued by a court which specifies that a fingerprint is to be used will limit the implicit testimony, benefiting the defendant.

B. On Applying Fisher to Compelled Decryption

Faced with sometimes inconsistent rulings in past cases and the complexities introduced by variations in technology, it is easy to be pessimistic about *Fisher*'s suitability for compelled decryption cases. Leaving aside the question of whether the doctrine is jurisprudentially desirable, can *Fisher* be applied consistently in compelled decryption cases? We think so.

Applying *Fisher* consistently will require a careful understanding of the facts and circumstances of a particular case, the technology in question, and the greater social and technological context. Drawing upon the collection of issues raised by the cases to date, as well as the hypotheticals described in Part V, this Section compiles a list of questions to serve as a starting point to a *Fisher* analysis of compelled decryption. The purpose of these questions is to facilitate critical examination of technological assumptions inherent in a case's analysis, by making the assumptions

258. Compare the cases against Sebastien Boucher and Leon Gelfgatt. In the former, the initial grand jury subpoena sought Boucher's password. *In re* Grand Jury Subpoena to Sebastien Boucher (*Boucher II*), No. 2:06-mj-91, 2009 WL 424718, at *1 (D. Vt. Feb. 19, 2009). After Boucher moved to quash, the government pivoted, seeking to compel Boucher to enter his password. *Id.* After the subpoena was quashed, the government pivoted again, seeking instead the decrypted contents of Boucher's laptop. *Id.* In contrast, the *Gelfgatt* court considered whether decryption could be compelled pursuant to the "Commonwealth's proposed protocol," a highly detailed description of exactly how decryption was to be performed. *Gelfgatt*, 11 N.E.3d at 622 n.10. *Gelfgatt* did not consider compelled decryption in the abstract, but with respect to a specified sequence of instructions to be followed. *Id.*

explicit and prompting the question of whether they are justifiable in the case's specific context.

1. *Is there meaningful encrypted data? How is this known, and with what certainty?* As discussed in Section V.A, it may not be possible to tell the difference between an encryption (whether it is of meaningful information or not) and truly random data. This fact was important in *Doe II*, but is also relevant to the hypotheticals of deniable encryption and kill switches in Sections V.B and V.C. Even if there is encrypted data, that data may be meaningless. The encryption could be of blank space or of meaningless numbers.

2. *What encryption method or software is being used, and with what settings? How is this known, and with what certainty?* As illustrated throughout Part V, the different capabilities provided by and the settings available on certain encryption software can be significant in a case's analysis. They could overturn seemingly basic assumptions about, for example, the persistence of digital data or the authenticity of decrypted data.

3. *Can the defendant decrypt all or some of the encrypted data? How is this known, and with what certainty?* It may seem fairly likely that a defendant would be able to decrypt an encryption that is in her possession, but in certain scenarios this might not be true. For instance, if the defendant is simply a custodian of the encrypted data, or if the defendant's ability to decrypt is influenced by circumstances outside her control (such as action taken by another person, the phone's location, or the time of day).

4. *What are the ways in which the defendant could, directly or indirectly, furnish the decrypted data to the court? For each way, specify the sequence of actions required and consider the following questions.*

    a. *Can the defendant perform the act? How is this known, and with what certainty?* As discussed in item 3 just above, it is important for an analysis to take into account any plausible reasons that the defendant might be unable to decrypt the data, or more specifically, unable to decrypt the data *by a particular method*.

b. *Would the act communicate any testimonial information? Would performing the act reveal (or make extensive use of) the contents of the defendant's mind? Why or why not?* The testimonial aspects of the compelled act are fundamental to the applicability of the Fifth Amendment to a specific case. Implicit or explicit communication of the contents of the mind is the touchstone of testimony.[259] Depending on the circumstances, examples might include: the defendant's knowledge of the fact of encryption, the password, or the persistence of the encrypted data; the defendant's capability to decrypt; the authenticity of the furnished data or password; or the very password itself. As discussed in Section V.G, one interpretation of dicta in *Hubbell* and other cases suggest that the Fifth Amendment may protect use or extensive use of the contents of the mind, even absent revelation.

c. *Is all such testimonial information already a foregone conclusion from the standpoint of the government? How is this known, and with what certainty?* If the answer to item 4(b) is "yes," then the desired action cannot be compelled unless it is possible to establish that the content of the testimonial communication resulting from the act is already a foregone conclusion.[260] As discussed earlier, the assumptions related to technology that may reasonably be invoked in determining a testimonial communication to be a foregone conclusion change rapidly over time.[261] When considering a case, it is therefore essential to reexamine each step of the foregone conclusion analysis anew in light of changes to the technological context.

259. *In re* Grand Jury Subpoena Dated March 25, 2011 (*Doe II*), 670 F.3d 1335, 1345 (11th Cir. 2012).

260. *See supra* Part III.

261. *See supra* Section IV.A.

C. Alternative Doctrinal Proposals and a Critique of Their Technological Robustness

This Article focuses primarily on a single version of compelled decryption doctrine, but the law is far from settled. Both courts and legal scholars frequently disagree on the correct way to interpret *Fisher* and to apply it to compelled decryption. This Section briefly discusses two alternative doctrines that have been proposed: a password-centered rule suggested by Orin Kerr[262] and a content-centered rule suggested by Laurent Sacharoff.[263] Kerr and Sacharoff each attempt to distill the foregone conclusion analysis for compelled decryption into a relatively simple test. While the rules they put forth are very different from each other, both arguments depend on premises about the testimony implicit in the act of decrypting, which are challenged by the technologies described in Part V. This suggests that both of their rules are excessively tailored to the current technological landscape, and thus are likely to be inadequate in the face of changing technology.

Kerr's analysis of the foregone conclusion doctrine is similar to this Article's except on the question of what testimony is implicit in an act of decryption.[264] According to Kerr, when a defendant decrypts a computer using a password, the defendant implicitly testifies only that she "knows the password."[265] Kerr bases this conclusion on the premise that "[i]f you know the password, you can enter it."[266] Therefore, he reasons, if the government "knows that you know the password," it can compel decryption.[267]

Yet Kerr's argument depends on an overly simplistic conception of a password that, while accurately describing the common usage of passwords today, does not take into account other procedures by which one might access one's encrypted data. For example, the possibility of location- or situation-based decryption[268] challenges the idea that "if you know the password, you can enter it." Deniable encryption[269] complicates the very notion of "the" password by introducing an alternate du-

---

262. Orin Kerr, *The Fifth Amendment Limits on Forced Decryption and Applying the "Foregone Conclusion" Doctrine*, WASH. POST (June 7, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/06/07/the-fifth-amendment-limits-on-forced-decryption-and-applying-the-foregone-conclusion-doctrine/?utm_term=.2370cd044550 [https://perma.cc/V8EA-J6T7]. Kerr's forthcoming article on the topic was unavailable at the time of writing.

263. Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 FORDHAM L. REV. (forthcoming 2018).

264. *Compare* Kerr, *supra* note 262, at Part IV *with supra* Part III.

265. Kerr, *supra* note 262, at Part II.

266. *Id.* at Part IV.

267. *Id.* at Part IV.

268. *See supra* Section V.D.

269. *See supra* Section V.B.

ress password. It is not clear how to make sense of Kerr's proposal when deniable encryption may be in use.

Sacharoff's proposed test, in contrast, requires that the government know something about the contents of the encryption (i.e., the plaintext).[270] Specifically, in order to compel the defendant to decrypt and furnish the contents of an encrypted file, "the government must show it knows that the [defendant] possesses the file and be able to describe it with reasonable particularity."[271] Sacharoff bases this conclusion on the premise that the testimony implicit in the act of "entering the password" includes that "the documents revealed by decryption exist, are possessed by the defendant, and are authentic."[272]

Sacharoff's interpretation of *Fisher* differs substantially from ours (and from Kerr's).[273] The conception of encryption in Sacharoff's argument does not capture realistic variant technologies such as those of Part V. For example, deniable encryption directly challenges the claim that entering a password communicates the authenticity of the resulting decrypted contents.[274] Moreover, the idea that entering a password communicates anything at all about "the documents revealed by decryption" requires that documents are indeed revealed by decryption; in the kill switch hypothetical,[275] entering the password "reveal[s]" a drive with no contents at all.[276]

Both Kerr and Sacharoff attempt to distill the doctrine into a simple set of rules: a natural and appealing endeavor — but one which carries a high risk of failing to adapt to technological change — in a context where the interaction between the law and technology has a complex dependence on contextual details. Expressing the doctrine in an overly simplified form may obfuscate rather than clarify the act-of-production doctrine: it obscures the subtleties of reasoning from which the doctrine was derived, and thus makes it difficult to adapt to variations in technology, whether mundane or speculative. A robust application of *Fisher* to compelled decryption cases will require explicitly taking into account the full complexity of the doctrine, the legal and technological contexts in which it has developed, and the doctrine's interaction with specific technologies, on a case-by-case basis.

---

270. Sacharoff, *supra* note 263, at 36.

271. *Id.*

272. *Id.* at 43–44.

273. Many of the differences are beyond the scope of this Section and therefore are not discussed.

274. *See supra* Section V.D.

275. *See supra* Section V.B.

276. Sacharoff, *supra* note 263, at 43–44.

VII. ON EXISTENCE

What does it mean for a thing to *exist*?

While this question may seem fruitlessly abstract at first glance, a look to the compelled decryption case law exemplified in the excerpts below, demonstrates the question's relevance to compelled decryption.[277]

Courts have diverged in their conception of the existence of passwords:

> "The password is not a physical thing. If Boucher knows the password, it only exists in his mind."[278]

> "The State established that the phone could not be searched without entry of a passcode. A passcode therefore must exist."[279]

On the existence of plaintext files:

> "In short, the Government physically possesses the media devices, but it does not know what, if anything, is held on the encrypted drives."[280]

> "[T]he files are already in the Government's possession [in encrypted form]. Their existence is a foregone conclusion."[281]

And on the existence of encrypted files:

> "Further, the Government has already concluded upon forensic examination that they are encrypted . . . Thus, the existence and use of encryption software on the

277. Similar language, typically in reference to the existence of plaintext files, is found in other cases. *See, e.g.*, United States v. Fricosu, 841 F. Supp. 2d 1232, 1236 (D. Colo. 2012); Matter of Decryption of a Seized Data Storage Sys. (*Feldman*), No. 13-m-449, 2013 WL 12327372, at *3 (E.D. Wis. Apr. 19, 2013); *In re* Grand Jury Subpoena to Sebastien Boucher (*Boucher I*), No. 2:06-mj-91, 2007 WL 4246473, at *6 (D. Vt. Nov. 29, 2007).

278. *Boucher I*, 2007 WL 4246473, at *6.

279. State v. Stahl, 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016).

280. *In re* Grand Jury Subpoena Dated March 25, 2011 (*Doe II*), 670 F.3d 1335, 1347 (11th Cir. 2012).

281. United States v. Pearson, No. 1:04-cr-340, 2006 U.S. Dist. LEXIS 32982, at *58 (N.D.N.Y. May 24, 2006).

> files recovered from Defendant is all but a forgone conclusion . . . ."[282]
>
> "[T]he Government has also shown that the drives are encrypted."[283]

These excerpts demonstrate the subtle confusion often surrounding the meaning of existence. *Boucher I* and *Stahl* presented two contrasting conceptions of the existence of a password. According to *Boucher I*, the password existed only in Boucher's mind.[284] If Boucher had forgotten the password, it would have ceased to exist. *Stahl*, in contrast, claimed to deduce the existence of a password from the mere presence of an encrypted phone;[285] if such a deduction is sound, the password's existence is independent of the defendant altogether. *Doe II* and *Pearson* present a similar disparity regarding the existence of plaintext files. According to *Doe II*, the encrypted device did not by itself imply the existence of any computer files or other meaningful content.[286] *Pearson* disagreed.[287]

As evidenced above, reasoning based on what does or does not exist appears frequently in compelled decryption decisions. However, despite the growing literature on compelled decryption and the Fifth Amendment, the authors have come across only one scholarly allusion to the meaning of existence in encryption, in an insightful single-paragraph remark.[288]

This Part focuses on possible meanings of existence in the context of encryption, and explores when ciphertexts, passwords, and plaintexts can be said to exist. This exploration is not based on a belief that existence should necessarily be important in deciding compelled decryption cases. Indeed, we believe it essential to recognize the reasoning underlying *Fisher*'s foregone conclusion analysis and reconsider the meaning of implicit testimony for each case under consideration, rather than to proceed immediately to a prototypical existence-possession-authenticity analysis (as, for example, in *Gelfgatt*). With such an approach, there may well be compelled decryption cases where a foregone conclusion analysis will not present questions of existence at all. That said, questions about the nature of existence of encrypted data, passwords, and the like

---

282. *Id.* at *58–*59.

283. *Doe II*, 670 F.3d at 1347.

284. In re Grand Jury Subpoena to Sebastien Boucher (*Boucher I*), No. 2:06-mj-91, 2007 WL 4246473, at *6 (D. Vt. Nov. 29, 2007).

285. *See* State v. Stahl, 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016).

286. *Doe II*, 670 F.3d at 1347.

287. *Pearson*, 2006 U.S. Dist. LEXIS 32982, at *58.

288. *See* Benjamin Folkinshteyn, *A Witness Against Himself: A Case for Stronger Legal Protection of Encryption*, 30 SANTA CLARA HIGH TECH. L.J. 375, 401 (2014).

are interesting in their own right, and the proportion of cases that place weight on such questions calls for an examination thereof in order to inform a critical understanding of compelled decryption case law.

A. Physical and Conceptual Existence

This Section describes two distinct types of existence, dubbed "physical" and "conceptual."[289] We do not expect that ours will be the final word on this issue, but rather only a first step in the right direction.[290]

There are (at least) two distinct senses in which Lewis Carroll's poem, "Jabberwocky," exists. Each copy of the poem, whether in printed form or digitally stored on a computer, exists in some *physical* way. But while each of the perhaps millions of physical manifestations of the poem is physically distinct, there are not millions of poems: there is only one poem called "Jabberwocky." The latter *unique* form of existence is a decidedly non-physical way in which the poem exists, hereafter referred to as "conceptual existence."

One may unambiguously refer to this same poem in a number of ways: "Lewis Carroll's 'Jabberwocky'" is the most direct, but "the poem which Alice partially recites to Humpty Dumpty in the book *Through the Looking-Glass*" or "the poem in which the English word 'galumphing' first appeared"[291] serves just as well to uniquely identify which poem is meant.[292]

Numbers also enjoy a conceptual existence; the number "77" exists much like "Jabberwocky" exists. And as with a poem, a number can be uniquely described without using its name: "the smallest number whose name (in English) is five syllables long" refers to a thing that has conceptual existence: namely, the number "77."[293] There are many ways to uniquely describe a number: "the number that is larger than '76' and smaller than '78'" would be another way to identify "77."

---

290. Both the taxonomy and terminology are the authors'.

290. It would be remiss not to mention here the centuries of study of the concept of existence by philosophers. While metaphysics encompasses furthering the general understanding of existence and related concepts, our purpose is incomparably narrower: to highlight a couple of distinct notions of existence that present interesting subtleties when applied to encryption. It is for this reason that the discussion herein is set in the context of a simple classification of our devising, which neither captures many nuances recognized by metaphysics, nor fits neatly into established notions.

291. *Galumph*, MERRIAM-WEBSTER.COM DICTIONARY, https://www.merriam-webster.com/dictionary/galumph [https://perma.cc/5EPY-HQWR].

292. LEWIS CARROLL, THROUGH THE LOOKING-GLASS, ch. 1, 6 (Project Gutenberg 1991) (1871), https://www.gutenberg.org/files/12/12-h/12-h.htm [https://perma.cc/6NN4-ZENG].

293. Here and throughout, "number" is used to mean "positive integer" like 1, 20, and 378, but not 1.5, 0, or -6.

Not everything that could conceivably conceptually exist does. Neither "Lewis Carroll's 'Wabberjocky'" nor "the poem which Snow White recites to Moses in *The Hobbit*" conceptually exists.[294] Likewise, neither "the largest number" nor "the number that is larger than five and smaller than three" conceptually exists.

Even if an object conceptually exists, it might be infeasible to actually discover it. Consider, for example, Malaysia Airlines Flight 370, which disappeared somewhere over the Indian Ocean in March, 2014. An almost four-year, multinational search for the aircraft covered about 46,000 square miles of ocean and found almost no significant remains of the aircraft.[295] While the flight recorder almost certainly exists both conceptually and physically, even the combined resources of multiple nations have been insufficient to locate it.[296]

In the realm of mathematics, examples of things which exist conceptually but are very difficult to discover are numerous. Moreover, it may be difficult to know whether a phrase describes something that exists conceptually or not. For example, "the smallest prime number between x and $x + 1000$" conceptually exists for certain values of x but not for others.[297] It may be effectively impossible to discern which is the case for many very large values of x.

---

294. *See* J. R. R. TOLKIEN, THE HOBBIT, OR, THERE AND BACK AGAIN (1937).

295. *See, e.g.*, Jonathan Perlman, *MH370 Search Becomes Most Expensive Aviation Hunt in History, yet Still No Clues*, TELEGRAPH (May 29, 2014, 5:56 PM), http://www.telegraph.co.uk/news/worldnews/asia/malaysia/10863605/MH-370-search-becomes-most-expensive-aviation-hunt-in-history-yet-still-no-clues.html (last visited Dec. 19, 2018); Juliet Perry et al., *MH370: Search Suspended but Future Hunt for Missing Plane Not Ruled Out*, CNN (Jan. 18, 2017, 12:10 AM), http://edition.cnn.com/2017/01/17/asia/mh370-search-suspended [https://perma.cc/L3G4-CV5D].

296. *Id.*

297. For example, for $x = 1{,}693{,}182{,}318{,}746{,}371$, there are no prime numbers between x and $x + 1000$.

B. Existence and the Fifth Amendment

Recall that *Fisher* established a two-pronged test to determine whether an act of producing some evidence may be compelled. First, would the act of production implicitly communicate information?[298] If not, the production may be compelled.[299] Second, is the information implicitly communicated a foregone conclusion?[300] If not, the act is deemed testimonial and may not be compelled; otherwise, production may be compelled.[301] Any production of some evidence communicates that the evidence exists, whether conceptually or physically.

Every act of production therefore requires that the existence of the evidence be a foregone conclusion. However, while it might be considered a foregone conclusion that a person suspected of a crime would have some memory of a day or event — that the memory (conceptually) exists — the government cannot compel the suspect to divulge that memory.[302] This is not a contradiction. First, a person's memory, were it to be divulged, would be testimony. Even if the memory had been previously committed to writing, the government could not compel the suspect's memory, only the written version. Second, existence is necessary, but not sufficient, for compulsion.

Neither the courts nor the academic literature on compelled decryption have clearly distinguished between physical and conceptual existence. As such, the status of conceptual existence in foregone conclusion doctrine is unclear. This lack of clarity contributes to the confusion in compelled decryption cases as illustrated in the beginning of this Part. The rest of this Part discusses the nature of the existence of each of the main objects of interest in an encryption case — namely, the ciphertext, the password, and the plaintext.

C. Existence and Encryption

When considering an encrypted hard drive, there are three objects of potential interest: the ciphertext, i.e., the data in encrypted form; the plaintext, i.e., the data that would result from decrypting the ciphertext; and the password, i.e., the secret information needed to perform decryption. Suppose a law enforcement agency has a seemingly encrypted hard drive in hand: What can be said about the existence of the ciphertext? The password? The plaintext? Let us consider them one by one.

---

298. Fisher v. United States, 425 U.S. 391, 410 (1976).
299. *Id.*
300. *Id.* at 411.
301. *Id.*
302. Schmerber v. California, 384 U.S. 757, 763–64 (1966) ("It is clear that the protection of the privilege reaches an accused's communications, whatever form they might take.").

The seeming ciphertext — that is, the data on the hard drive that appears to be in encrypted form — certainly exists physically. It has a physical manifestation on the storage medium, much as the written word has a physical manifestation on paper. However, as discussed in Part V and recognized by the Eleventh Circuit in *Doe II*, it may be unclear, given a seeming ciphertext, whether it is in fact a *valid* ciphertext that encrypts some plaintext, or it is simply some random-looking data that cannot be decrypted to a plaintext at all.[303] Thus, whether the seeming ciphertext that the government has in hand is really a valid ciphertext may be hard or impossible to determine.

In contrast with the ciphertext, the password and the plaintext have no physical manifestation on an encrypted hard drive. Of course, they may exist physically elsewhere. For example, the password might have been written down on a note or a copy of the plaintext may have been sent in an email. The government might attempt to compel production of physical copies directly. But absent such circumstances, if the password and plaintext exist at all, they exist only conceptually.

Given a *valid* ciphertext, the password and plaintext do exist conceptually. If the defendant is able to decrypt the ciphertext, then "the password employed by the defendant to decrypt the ciphertext" and "the plaintext resulting from aforesaid decryption" both describe objects that conceptually exist. *Boucher I* employed this conception of the password.[304] That the defendant indeed has the ability to decrypt the ciphertext would have to be otherwise established.

Boucher I additionally claimed that the password *only* existed in the mind of the defendant. [305] A strong interpretation of this statement is that there is no description of the password and the plaintext that does not appeal to the contents of the defendant's mind. In a typical setting, this is not true. For many encryption algorithms in common use, nearly all ciphertexts can be decrypted to only a single meaningful plaintext, using a single password.[306] Thus, "the password that, when used to decrypt the ciphertext, yields a meaningful plaintext" and "the plaintext resulting from aforesaid decryption" describe a unique password and plaintext. That is, the conceptual existence of the plaintext and password can be

303. *Cf. In re* Grand Jury Subpoena Dated March 25, 2011 (*Doe II*), 670 F.3d 1335, 1347 (11th Cir. 2012) ("The Government has not shown, however, that the drives *actually* contain any files . . . .").

304. *In re* Grand Jury Subpoena to Sebastien Boucher (*Boucher I*), No. 2:06-mj-91, 2007 WL 4246473, at *6 (D. Vt. Nov. 29, 2007) ("The password is not a physical thing. If Boucher knows the password, it only exists in his mind.").

305. *Id.*

306. Ran Canetti et al., *Deniable Encryption*, PROCEEDINGS OF THE 17TH ANNUAL INT'L CRYPTOLOGY CONFERENCE ON ADVANCES IN CRYPTOLOGY, Aug. 1997, at 91 ("Standard encryption schemes do not guarantee deniability. Indeed, typically there do not *exist* two different messages that may result in the same ciphertext (with *any* random input).").

formulated in a way that does not depend at all on the defendant. Later, Section VII.D discusses other types of encryption algorithms — those in which a ciphertext may be able to decrypt to many different plaintexts with many different passwords.

This observation could lend some credence to the *Stahl* court's reasoning of (conceptual) existence of the password: namely, that because the phone "could not be searched without . . . a passcode," one must exist.[307] *Pearson* makes the analogous statement of the plaintext: because "the files are already in the Government's possession" in encrypted form, "[t]heir existence is a foregone conclusion."[308] Though *Stahl* and *Pearson* were probably not considering these issues, taken in isolation, their statements can be understood as having some truth. While physical existence is clearly germane to the *Fisher* doctrine, it is a leap to adopt a conceptual-existence framework for a foregone conclusion analysis.

Moreover, the preceding discussion is predicated on the assumption of a valid ciphertext. A seemingly encrypted hard drive may instead be filled with random data that is not an encryption at all. Then, there would be no combination of password and meaningful plaintext that would result in this data as a ciphertext. Thus, no password and no plaintext exist at all — not even in the mind of the defendant. The difficulty of distinguishing a real ciphertext from random data explains the astute observation from *Doe II* that the government may not know "what, if anything," is contained within a seemingly encrypted drive even if "the Government physically possesses" it.[309]

D. Information-Theoretic Encryption

Let us turn finally to a less common type of encryption algorithm: those in which a ciphertext can be decrypted to many different plaintexts using many different passwords. There is a much stronger type of encryption than the standard encryption typically used, called "information-theoretic encryption,"[310] which has the property that every possible ci-

307. State v. Stahl, 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016).

308. United States v. Pearson, No. 1:04-cr-340, 2006 U.S. Dist. LEXIS 32982, at *58 (N.D.N.Y. May 24, 2006).

309. *In re* Grand Jury Subpoena Dated March 25, 2011 (*Doe II*), 670 F.3d 1335, 1347 (11th Cir. 2012).

310. Also called "perfectly secure encryption," information-theoretic encryption is not a recent innovation, but rather has been around since the founding days of modern cryptography. *See* C. E. Shannon, *Communication Theory of Secrecy Systems*, 28 BELL SYS. TECH. J. 656, 659 (1949). The most well-known information-theoretic secure encryption scheme is called "one-time pad" and was used by the Soviets in the 1960s to secure their most important communications. *See* David E. Hoffman, *NSA's Early Cold War Struggle To Crack Soviet Spy Codes*, WASH. POST (Sept. 9, 2016), https://www.washingtonpost.com/opinions/nsas-early-cold-war-struggles-to-crack-soviet-spy-codes/2016/09/08/9113cbd4-62f2-11e6-be4e-23fc4d4d12b4_story.html [https://perma.cc/2WT7-Y4QX]. Espionage is one of the scenarios

phertext can decrypt to every possible plaintext using some password.[311] For example, *any* seven-character ciphertext could decrypt to "TURTLES," "HELIPAD," "ILUVYOU," and to every other seven-character sequence; each possible plaintext would result from using a different password. Conversely, any seven-character password can be used to decrypt the ciphertext, resulting in a different plaintext. Absent the password, a ciphertext alone carries no information about the plaintext, since *any* plaintext is a possibility.[312]

Information-theoretic encryption is not widely used because it is very cumbersome for several reasons; one reason is that the passwords must be as large as the plaintext data being encrypted. Encrypting one megabyte of data requires a one-megabyte password. In contrast, in standard encryption schemes, a single short password can be used to encrypt as much information as desired. Still, information-theoretic encryption could practicably be used to encrypt a small amount of very sensitive information.[313]

For a ciphertext resulting from information-theoretic encryption, "the password employed by the defendant to decrypt the ciphertext" is still a meaningful description of the password. On the other hand, "the password that, when used to decrypt the ciphertext, yields a meaningful plaintext" loses all meaning. This is because every meaningful plaintext can result from decryption, each using a distinct password. In contrast with the case of standard encryption schemes, the password, as *Boucher I* found, "only exist[ed] in his mind."[314]

Counterintuitively, the same can be said about the plaintext: it only exists as a byproduct of the contents of the mind of the person who knows the password, even though this person might not literally know what the plaintext is. Because every plaintext can result from decryption, it is only the password in the mind of the decryptor that distinguishes the

---

in which memorizing very long and complicated passwords might be considered viable and worth the effort; highly trained spies could conceivably perform many such memorizations as a matter of routine, with the intention of encrypting future communications based thereupon.

311. More accurately, every possible ciphertext *of a given length* can decrypt to every possible plaintext *of a given length*. In fact, the length of the plaintext is the one piece of information about the plaintext which is revealed by the ciphertext. Interestingly, the revelation of plaintext length is an inherent, unavoidable property of encryption. *See* KATZ & LINDELL, *supra* note 20, at 56.

312. Formal mathematical expositions of information-theoretic encryption are given in many cryptography textbooks. *See, e.g.*, KATZ & LINDELL, *supra* note 20, at 26–37.

313. The astute reader might ask: if the password must be the same length as the plaintext data, then why not just memorize the plaintext instead? In some contexts, memorizing the plaintext is not a possibility. For instance, in the context of encrypting extremely sensitive communications (say, in the course of an intelligence operation), it may be necessary to agree in advance on some passwords in person, and only later use those passwords to exchange encrypted messages remotely.

314. *In re* Grand Jury Subpoena to Sebastien Boucher (*Boucher I*), No. 2:06-mj-91, 2007 WL 4246473, at *6 (D. Vt. Nov. 29, 2007).

correct plaintext. As an analogy, "ten more than the defendant's favorite number" can indicate any number, and is well-defined only as a byproduct of the knowledge of the defendant's favorite number; moreover, the phrase ceases to have meaning if the defendant does not have a favorite number.

Standard encryption and information-theoretic encryption may be considered as two ends of a spectrum. On the one end, each ciphertext uniquely defines a password and a plaintext; on the other, a ciphertext carries no information about the password and plaintext — they only exist in the mind of the user. Given a (seeming) ciphertext, it may be impossible to determine on which end of the spectrum it lies. It may even lie in the middle: deniable encryption schemes, described in Part V, may have multiple passwords, each yielding a different plaintext. With a deniable encryption scheme, there may be two possible plaintexts, or there may be several. What can be said about the existence of passwords and plaintexts correspondingly lies somewhere in the middle of the typical case and the information-theoretic case.

VIII. CONCLUSION

This Article has examined the compelled decryption doctrine to date and found that it sometimes turns on non-obvious technological details in surprising ways. Despite this fragility, it does seem possible to apply in a consistent manner by carefully considering the technologies involved.

That the doctrine is not fundamentally inconsistent does not by itself mean that it is satisfactory. However, consistency is a necessary condition, and not one that can be taken for granted. To date, courts have differed in the legal standards applied in compelled decryption cases and also in their understanding of the technologies involved.[315] Indeed, the possibility of consistent application is a crucial factor in evaluating the robustness of a doctrine that has proved so sensitive to technological details that its adaptability to future technological developments is far from obvious.

Taking as a baseline the potential for consistent application, let us now consider the technological sensitivity of today's doctrine, towards the broader aim of assessing its long-term desirability. Today's doctrine is highly sensitive to changes in available technology and in the common usage of existing technology, including small changes to default settings, or in the details of how a particular product is implemented in soft-

315. *See generally supra* Parts IV and VII.

ware[316]; this is one of the recurring themes of Parts V and VI. As a result, applying the doctrine in a consistent manner requires technical expertise applied to the details of exactly which technologies were used and in exactly what way, to inform the legal reasoning on a case-by-case basis.

In other words, the technological sensitivity of today's compelled decryption doctrine renders it brittle in the sense that it is prone to yielding differing outcomes in cases that differ primarily, or only, in the details of the software used, or even in the nature of technical expertise available when analyzing the case. Given all the details of a case involving encryption — except for the exact configuration of the encryption software — it might still be uncertain whether or not compelled decryption would be protected under the Fifth Amendment, because the protection could depend on that exact configuration. The doctrine seems to give rise to a range of situations where even a lawyer with extensive knowledge of the doctrine, let alone a reasonable defendant in general, would be unable to distinguish whether any particular action she is requested to perform would be testimonial or not, due to lack of technological expertise.

Such brittleness is likely to cause variability in the courts' decisions hinging on technological details often largely independent of the normative considerations that interested parties — whatever normative beliefs they may hold — consider ought to have bearing on the outcome of a case. This would be an undesirable state of affairs, whether from the perspective of a civil libertarian, law enforcement, or a defendant, and unsatisfactory from a range of jurisprudential perspectives too. Moreover, it bears mentioning that from a social justice perspective, such brittleness may exacerbate systematic bias against poorer, less educated, or technologically illiterate defendants (whether guilty or not).

Against the backdrop of *Fisher*, any broad shift based on normative considerations would have to result from a Supreme Court decision on the Fifth Amendment and compelled decryption. Such a decision may come slowly, extend precedent gradually, or depart altogether from

316. Making implicit assumptions that the technological landscape is relatively constant, especially over short periods of time, can be easy to do without noticing. For instance, Apple's personal computer full disk encryption capability (called "FileVault") was introduced in version 10.7 of their operating system; in version 10.10 it became an opt-out feature instead of an opt-in feature. *See Use FileVault*, *supra* note 5; Hern, *supra* note 5.

This change in the default setting affects what may be inferred from the presence of encryption. For example, before the change, one might argue that under the right circumstances, the presence of encryption on a computer implies that the user has knowledge of the fact of encryption; after the change to encryption by default, such an argument would lose all strength.

courts' and scholars' current understanding of the doctrine.[317] But the Fifth Amendment is only one of the myriad factors in the complex and increasingly frequent interactions between law enforcement and cryptography — both vital to modern society. While the topic of this Article is an essential component of this broader landscape, it is important to recognize that the Fifth Amendment is not, and need not be, the primary source of protection against excessive government access to encrypted data in general: an eventual unified doctrine will weave together protections afforded by different parts of the Constitution, including the Fourth Amendment. We are cautiously optimistic about progressing towards a sensible and unified doctrine surrounding law enforcement and cryptography.

317. *Cf.* Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018) ("When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents.").