CRACKING THE CODE: THE ENIGMA OF THE SELF-INCRIMINATION CLAUSE AND COMPULSORY DECRYPTION OF ENCRYPTED MEDIA

Jason Wareham*

CITE AS: 1 GEO. L. TECH. REV. 247 (2017)

https://perma.cc/KX56-QZVE

INTRODUCTION

Encryption, though once the narrow province of countries, commanders, and spies, has become widely commonplace. Akin to Prometheus bringing Zeus's fire to common man, modern computing has made even the most advanced encryption seamlessly and transparently available to the masses. People of the modern world routinely utilize

* U.S. Marine Corps Judge Advocate; Georgetown Law, LL.M. 2016; Creighton Law, J.D. 2007; University of Colorado at Denver; B.S.B.A 2004. The views and opinions expressed in this article are those of the author and do not reflect the official policy or position of the U.S. Marine Corps, Department of Defense, or the U.S. Government.

encryption standards strong enough to protect Top Secret government data;[1] encryption so strong the length of time necessary to break it with supercomputers is measured in trillions or even quadrillions of years.[2] Encryption is everywhere, on our phones, computers, and websites. For the most part, this encryption is unbreakable without the proper decryption key—a password of some kind, such as a text string, file, or biometric print, that makes the encrypted data accessible to the user.[3]

The ubiquitous nature of encryption today means that it is also increasingly utilized by criminals for unlawful purposes. Criminal investigations can be impaired by garden-variety encryption protecting otherwise legitimate or discoverable evidence, such as text, email, or instant messages supporting a conspiracy, photographs of the crime scene or evidence, or contraband files, such as child pornography.[4]

A quest for the decryption key unlocking this suspected evidence can lead the government down a path ending at the Fifth Amendment's Self-Incrimination Clause. This Clause, meant to protect individuals from compelled participation in their own convictions, now impacts whether someone may remain silent in the face of a government order to hand over their encryption password. So far, while there has been some scholarly work and opinions on the topic, there has been little academic or judicial guidance on the application of the Fifth Amendment's Self-Incrimination Clause to this digital issue.[5] Of those opinions, discussed below, there is little analysis that assists the everyday criminal litigator in understanding and applying constitutional principles to digital encryption cases. As of yet, there has been no case on point from the Supreme Court of the United States.

---

[1] COMM. ON NAT'L SEC. SYS., NATIONAL INFORMATION ASSURANCE POLICY ON THE USE OF PUBLIC STANDARDS FOR THE SECURE SHARING OF INFORMATION AMONG NATIONAL SECURITY SYSTEMS, https://www.cnss.gov/CNSS/openDoc.cfm?4uxTThystPbeZRHLdrANhw== (last visited Oct. 2016) [https://perma.cc/M8FP-UPRF].

[2] *Check Our Numbers: The Math Behind Estimations to Break a 2048-Bit Certificate,* DIGICERT, https://www.digicert.com/TimeTravel/math.htm (last visited Oct. 2016) [https://perma.cc/2E7D-VZB2].

[3] *See e.g., iOS Security,* APPLE, http://www.apple.com/business/docs/iOS_Security_Guide.pdf (last visited Dec. 2016) [https://perma.cc/JPG2-6D6A] (describing Apple iPhone encryption and multiple unlocking methods including a pin code, alpha-numeric text string, and biometric fingerprint methods).

[4] *See* FED. BUREAU INVESTIGATION, GOING DARK, https://www.fbi.gov/services/operational-technology/going-dark (last visited Oct. 2016) [https://perma.cc/Q2LV-UQAJ].

[5] *See* Dan Terzian, *The Micro-Hornbook on the Fifth Amendment and Encryption*, 104 GEO. L.J. 268 (2016).

In the few cases covering the topic, the government and courts alike have struggled for a simple analytical framework that consistently applies existing self-incrimination jurisprudence to digital encryption. Law enforcement fears of "going dark" and losing access to vital evidence have facilitated the erosion of individual constitutional rights through the twisted application of doctrines that never contemplated application to encrypted evidence.[6] Old doctrines should not be strained past all meaningful recognition to meet these emerging challenges. Rather, law enforcement must improve existing investigation techniques to properly gather evidence without compelling the password of the accused.

This Note will begin by describing the basics of encryption, digital encryption as it exists today, and encryption's myriad uses. It will then analyze those various implementations and methods to demonstrate how an individual subject to government investigation may rely on the Fifth Amendment to legally abstain from providing the encryption key. It will analyze the few cases that cover the interplay of the Fifth Amendment and digital encryption, specifically addressing the flawed application of the foregone conclusion and act of production doctrines that have been the primary argument justifying compelled access. Finally, this Note will propose basic investigatory techniques and methods the government could use to both investigate and acquire the evidence sought while respecting the boundaries and protections of the Fifth Amendment.

ENCRYPTION

Encryption is the act of obscuring a message in such a way that only the original author and an intended recipient can understand it.[7] In its simplest form, encryption requires a cipher (a set of rules or steps to apply the key to the original text) and a key (predetermined data applied to generate specific outputs from the cipher, to encrypt or decrypt a message).[8]

Historical Use of Encryption

The use of encrypted communications is found as early as the days of Julius Caesar. Thomas Jefferson also used wheel ciphers to communicate

[6] *Id*.
[7] *See* Margaret Rouse, et. al., *Encryption*, SEARCHSECURITY (Apr. 2016), http://searchsecurity.techtarget.com/definition/encryption [https://perma.cc/T385-KWBE].
[8] *Id*.

secret messages as the Secretary of State to American allies in France.[9] The Allies' ability to break Nazi encryption significantly impacted the outcome of World War II. Early encryption consisted largely of substitution ciphers, in which an individual substituted meaningless letters or numbers for the message he or she intended to hide. Encryption schemes could be quite simple as in the case of Julius Caesar's simple replacement cipher,[10] or encryption could need a large mechanical instrument such as the Nazi's Enigma machine.[11] But while encryption is not a new tool or concept, modern computing has dramatically increased the strength of encryption and facilitated the ease and versatility of its use.

In the 1970s, the use of computer technology allowed encryption to take a huge leap forward in complexity and strength. Modern computers enabled the use of complex encryption algorithms as the cipher to secure digital files.[12] These cipher algorithms are complex computational math functions used to scramble the data in a predetermined way shaped by the encryption key to transform the encrypted data.[13] These keys can be regular passwords, key files or biometric data, such as a fingerprint.[14] Computer

---

[9] *See* Ralph Simpson, *Cipher Machines Through History*, CIPHER MACHS. (Apr. 2016), http://ciphermachines.com/ [https://perma.cc/PPT4-UN23]; Anna Berkes, *Wheel Cipher*, JEFFERSON MONTICELLO, (Oct. 2016), https://www.monticello.org/site/research-and-collections/wheel-cipher [https://perma.cc/MEV5-AC4H].

[10] *Caesar Cipher,* PRACTICAL CRYPTOGRAPHY, http://practicalcryptography.com/ciphers/caesar-cipher/ (last visited Apr. 2016) [https://perma.cc/3SWR-LB3Z]; *see also*, *Caesar Cipher,* LEARN CRYPTOGRAPHY, https://learncryptography.com/classical-encryption/caesar-cipher (last visited Apr. 2016) [https://perma.cc/4WAN-G29G] ("The Caesar cipher, also known as a shift cipher, is one of the simplest forms of encryption. It is a substitution cipher where each letter in the original message (called the plaintext) is replaced with a letter corresponding to a certain number of letters up or down in the alphabet.").

[11] *The Enigma Cipher Machine,* CODES & CIPHERS, http://www.codesandciphers.org.uk/enigma/ (last visited Apr. 2016) [https://perma.cc/E3ZG-DTLU].

[12] *See Encryption Algorithms,* JETICO WEB HELP, https://www.jetico.com/web_help/bc8/html/02_basic_concepts/05_encryption_algorithms.htm (last visited Apr. 2016) [https://perma.cc/DKL9-ZNQ4].

[13] Norman D. Jorstad, *Cryptographic Algorithm Metrics*, INST. FOR DEF. ANALYSES SCI. & TECH. DIV. (1997), http://csrc.nist.gov/nissc/1997/proceedings/128.pdf [https://perma.cc/2T5B-Z2WJ].

[14] *See, e.g.*, *Keyfiles*, VERACRYPT DOCUMENTATION, https://veracrypt.codeplex.com/wikipage?title=Keyfiles%20in%20VeraCrypt (last visited Apr. 21, 2016) [https://perma.cc/5D8D-ZVNV] (describing a key file as a randomly generated text file or any other file type that can remain unaltered that acts as a key to unlock encryption); Colin Soutar, et. al, *Biometric Encryption*, ISCA GUIDE TO CRYPTOGRAPHY 4

ciphers and keys have become so complex that a brute force attack without knowledge of the key would take trillions of years against today's secure and commonly employed ciphers.[15]

As modern encryption schemes are becoming increasingly complex and secure, they are also becoming increasingly ubiquitous; encryption is no longer the exclusive province of sovereigns or their military forces. In today's online ecosystem, individuals seamlessly utilize the securest forms of modern encryption in their everyday lives without knowing it. In the brief span that a person wakes up in the morning to an iPhone alarm, and unlocks her phone before checking her email using a home wireless internet (WiFi) connection, that person has already used three different implementations of encryption with three different key types. Depending on the type of encryption key used, there may be various levels of legal protection for each different encryption key, should a prosecutor attempt to access those same devices without the user's consent and assistance.

Common Types of Digital Encryption

The most common types of encryption utilized in the digital space are password-based pre-shared key and public/private key exchange. The first and most commonly understood form of encryption key is the use of a single private password or file to decrypt, which is shared with all intended recipients. A user creates a text password or file ("key file") that is kept private, and then enters it each time she wishes to access the encrypted material. Shared Key or Pre-Shared Keys ("PSK") is a symmetric key encryption scheme,[16] through which individuals create a common encryption key that is used to decrypt messages, files, or transmissions through the use of the same key as everyone else.[17] This type of key is most commonly used in accessing protected WiFi connections or by emailing an encrypted document

(1999), http://www.cse.lehigh.edu/prr/Biometrics/Archive/Papers/BiometricEncryption.pdf [https://perma.cc/Q8CF-CPW6] (biometric encryption keys are the conversion of biometric scans (fingerprint, retina, face) data into a string of numbers and letters that acts as the key).

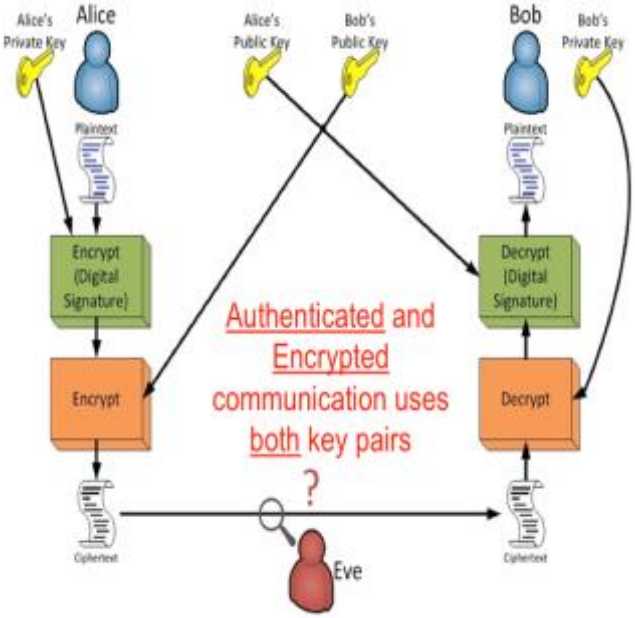
[15] Mohit Arora, *How Secure Is AES Against Brute Force Attacks?*, EE TIMES (May 7, 2016), http://www.eetimes.com/document.asp?doc_id=1279619 [https://perma.cc/F4UR-VZD7].

[16] *Description of Symmetric and Asymmetric Encryption*, MICROSOFT, https://support.microsoft.com/en-us/kb/246071 (last visited Apr. 21, 2016) (describing a symmetric key encryption scheme as one where the same key (password, etc.) is used to both encrypt and decrypt).

[17] Alfred J. Menezes et. al., *Identification and Entry Authentication and Key Establishment Protocols*, *in* HANDBOOK OF APPLIED CRYPTOGRAPHY (2001), http://cacr.uwaterloo.ca/hac/ [https://perma.cc/QS5L-5RUR].

and then securely providing the recipient with the password. These types of keys are also utilized in a data-at-rest individual file level or whole disk encryption schemes, such as with a Microsoft Word file, a computer drive, or an iPhone that blocks access to the file or device as a whole without the correct key.

Figure 1. Asymetric Encryption[18]



Public key encryption ("PKE") is an asymmetric encryption key scheme, in which the individuals each possess a key pair, one public key published on a public directory server called a certificate authority, and the other a private key that is kept secret on the receiving systems, often protected further by a separate password.[19] The public and private keys are mathematically linked, and the public key can only be accessed through the use of the private key.[20] The key's linkage is a one-way process; the public key encrypts, the private key decrypts, and that process cannot be reversed to

[18] Image Courtesy of the U.S. Naval Academy, http://www.usna.edu/CyberCenter/si110/lec/cryptAsymmEnc/img/both.png

[19] Charles C. Mann, *A Primer on Public-Key Encryption*, ATLANTIC (Sept. 2002), http://www.theatlantic.com/magazine/archive/2002/09/a-primer-on-public-key-encryption/302574/ [https://perma.cc/UE8N-MUF6].

[20] *Id*.

decrypt.[21] The public key can be sent directly to anyone via email or published on a key directory server on the internet.

The public key encryption design serves as the basis for almost all encrypted connections online. In the form of an implementation called Secure Sockets Layer ("SSL"), websites are able to encrypt connections on a per client basis such that any connection between the server and the client is unreadable to another observer on the same network.[22] When a user opens a browser and connects using the prefix "https:" the website server provides the public certificate to the browser in that instant, along with the code to verify it.[23] The browser then begins to encrypt its traffic using that certificate to the website which then reads it using its private key.[24] This is how almost all secure websites function.

PKE is also employed to encrypt emails. A user obtains a key pair tied to her email address and loads it into the email client program.[25] The email client will then attach the public key with each message sent. Once the recipient has the public key, she can respond to emails securely with the email program automatically decrypting messages upon receipt.[26]

As a tool, encryption is independent of the nature, content, or importance of messages and files it protects – it shields legitimate and illegitimate activities equally well. This raises constitutional questions about the limits on the government's power to compel the production of encryption keys, which, in some cases, may not exist outside of the knowledge of the accused. In order to fully understand the constitutional implications raised by encryption, a basic understanding of the relevant law on self-incrimination generally must be understood.

---

[21] *Digital Certificates*, COMODO, https://www.comodo.com/resources/small-business/digital-certificates2.php (last visited Apr. 21, 2016) [https://perma.cc/5J5V-4FD8].

[22] UNDERSTANDING DIGITAL CERTIFICATES & SECURE SOCKETS LAYER, ENTRUST.COM, https://www.entrust.com/wp-content/uploads/2013/05/WP_UnderstandingSSL_FINAL_May07.pdf (2007) [https://perma.cc/2ZKX-X7ZS] [hereinafter *SSL*].

[23] *Id.* at 5.

[24] *Id.*

[25] *An Introduction to Public Key Cryptography and PGP,* ELEC. FRONTIER FOUND., https://ssd.eff.org/en/module/introduction-public-key-cryptography-and-pgp (last visited Apr. 21, 2016) [https://perma.cc/8TBC-PEDY].

[26] *Id*.

THE FIFTH AMENDMENT AND SELF-INCRIMINATION

The Self-Incrimination Clause

The Fifth Amendment states that no person "shall be compelled in any criminal case to be a witness against himself."[27] In the 1886 case *Boyd v. United States*,[28] the Supreme Court held that this Clause barred compelling a defendant to produce incriminating private documents, including documents held by a partnership in that case.[29] The Court in *Boyd* viewed this Clause as barring private evidence, in addition to testimony.[30]

This broad view is supported by one of the leading scholars on the topic.[31] Professor Leonard Levy, a constitutional historian and winner of the Pulitzer Prize for his book, *Origins of the Fifth Amendment*, traces the long-standing European practices from which the American right against self-incrimination arose.[32] He concludes that the right was not just a privilege against self-incriminating testimony, but rather protection for a defendant against making any unwilling contribution to his conviction.[33] Given the language in *Boyd*, this seemed to be the Supreme Court's original interpretation of the protection as well.[34]

The Supreme Court, however, retreated from a complete bar of compelling production of incriminating documents in *Boyd* with a later holding, *Fisher v. United States.*[35] The *Fisher* case involved the subpoenaed production of tax documents held by a defendant's lawyer. The Court in *Fisher* held that the Fifth Amendment only protects an individual from their own testimonial communications.[36] Specifically, the Fifth Amendment only protects persons where evidence sought from them individually was (1), compelled; (2), testimonial; and (3), incriminating.[37] As applied in that case,

---

[27] U.S. CONST. amend. V.
[28] 116 U.S. 616 (1886).
[29] 116 U.S. at 634-35 ("We are further of opinion that a compulsory production of the private books and papers of the owner of goods sought to be forfeited in such a suit is compelling him to be a witness against himself, within the meaning of the Fifth Amendment to the Constitution.").
[30] *Id.* at 634-35.
[31] LEONARD W. LEVY, ORIGINS OF THE FIFTH AMENDMENT: THE RIGHT AGAINST SELF-INCRIMINATION 432 (1968).
[32] *Id*.
[33] *Id*.
[34] *Boyd*, 116 U.S. at 634-35.
[35] 425 U.S. 391 (1976).
[36] 425 U.S at 409-10.
[37] *Id.* at 409-10.

the act of the defense's lawyer turning over voluntarily-created tax documents prepared by an accountant was an act of surrender, as opposed to testimony, such that the Clause did not apply.[38] While that was the discrete holding of *Fisher,* the Court, also created two phrases that have developed into doctrines of Fifth Amendment jurisprudence still relevant today: the act of production doctrine, and the foregone conclusion privilege.[39] While briefly mentioned in *Fisher* for the first time, both concepts bear increasingly on the issues surrounding compelled surrender of encryption keys.

The Act of Production Doctrine

The act of production doctrine, also called the act of production privilege, originated in a brief phrase in *Fisher*, but was articulated fully as a legal doctrine in *United States v. Hubbell*.[40] *Hubbell* reaffirmed that the privilege against self-incrimination is not a privilege barring the production of all incriminating evidence by an accused, but rather is limited to those acts that are considered testimonial.[41] *Hubbell*, in which the defendant asserted his Fifth Amendment right when called before a grand jury to confirm the existence of eleven categories of documents and subsequently produce them, also reaffirmed that the privilege covers more than statements admitted in the trial itself, but also compelled statements that may lead to other incriminating evidence even if the statement itself is not testimonial.[42] "The privilege afforded not only extends to answers that would in themselves support a conviction under a federal criminal statute but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant for a federal crime."[43]

Through this lens, the *Hubbell* Court determined that the testimonial communication, in that case, was not found in the contents of the documents, because the documents previously existed and were voluntarily created, and

[38] *Id*.
[39] *Id.* at 410 ("The act of producing evidence in response to a subpoena nevertheless has communicative aspects of its own, wholly aside from the contents of the papers produced. Compliance with the subpoena tacitly concedes the existence 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."); *Id.* at 411 ("…when the Government knows of the location and contents of a document there is no reliance on the truth-telling of the accused and no constitutional rights are touched.").
[40] 530 U.S. 27 (2000).
[41] 530 U.S. at 34-35.
[42] *Id*.
[43] *Id.* at 39 (quoting Hoffman v. United States, 341 U.S. 479, 486 (1951)).

were therefore not testimonial themselves. The act of producing the documents and thus enabling the documents to become a link in the chain of evidence, however, was itself a testimonial act.[44] This concept has become formalized as the act of production privilege, which bars the use and derivative use of information not already known by the government that is implicitly communicated simply by the accused's act of producing it.[45] This includes the existence of the evidence, the accused's knowledge of its existence, custody of the evidence by the accused, and the authenticity of the evidence.[46] The *Hubbell* Court specifically rejected the argument that producing documents under a broad categorical subpoena lacking reasonable particularity was merely a physical act, as opposed to a testimonial assertion the Clause would otherwise protect.[47]

The exception to this general rule is when a prosecutor has independent knowledge to support each of those communicative acts, independent of the accused.[48] While the granularity of knowledge required is subject to debate, the *Hubbell* Court rejected the government's foregone conclusion argument because the government lacked knowledge of the existence or whereabouts of the documents sought.

The Foregone Conclusion Doctrine

> The existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers. Under these circumstances by enforcement of the summons no constitutional rights are touched. The question is not of testimony but of surrender.[49]

With that brief statement, the *Fisher* Court created the concept that the government could defeat the protections of the Fifth Amendment based on its countervailing, independent knowledge of the evidence. The problem is that there are few cases that define the elements or limits of the foregone conclusion doctrine. The doctrine's lack of clarity is inherently problematic

---

[44] *Id*.
[45] *Id.* at 28.
[46] *Id.* at 28-29.
[47] *Id.* at 40.
[48] *Id*.
[49] Fisher, 425 U.S. at 411.

but creates even great problems as it has become a frequently used tactic to defeat Fifth Amendment claims in encryption cases.

There are only four cases, including *Fisher* and *Hubbell,* in which the Supreme Court has mentioned the foregone conclusion doctrine, and none of the cases provide significantly helpful analysis).[50] As discussed above, the foregone conclusion doctrine is an apparent counter to the act of production privilege. It acts as an equitable or logical rebuttal to the assertion that the accused is disclosing new, incriminating evidence, as a defendant cannot "disclose" to the government information the government already knows. But as the doctrine developed from dicta, there are no clear standards or limits espoused by the Supreme Court to provide further guidance for lower courts. Must a prosecutor show by a preponderance of the evidence that the material sought exists, or is there something more required? Must the prosecutor limit herself to documents of which she has actual knowledge, or can that prosecutor assume that the documents are available because it is reasonable under the circumstances to assume that they exist and that the accused possesses them? These questions have no clear answers, but profoundly affect the scope and strength of the Fifth Amendment protection against self-incrimination.

THE INTERSECTION OF ENCRYPTION AND THE SELF-INCRIMINATION CLAUSE

The Encryption Scheme Controls the Scope of Protection

Applying a legal framework to technology tends to produce a number of new questions. In the case of applying the self-incrimination clause to encryption, one of the key questions is how the strength of the protection is affected by the strength of the type of encryption used, whether private passwords, PSKs, or a public/private key exchange). Arguably, in a scheme where the key itself is a physical characteristic (i.e. thumbprint scans, retina scans, etc.) the physical characteristic data that forms the key implicates the Fourth Amendment rather than the Fifth, raising questions of privacy, seizure, and production.[51] This is also true if the scheme employs the use of a key file without an associated password (i.e. physical access cards or thumb drives). In that scheme, the key exists in an external form, such that employing it requires

[50] *See id.*; United States v. Hubbell, 530 U.S. 27 (2000); Braswell v. United States, 487 U.S. 99 (1988); United States v. Doe, 465 U.S. 605 (1984).

[51] This is of course contingent on whether the act of production is itself incriminating, *infra* Part II-B.

no intrusion into the mind or knowledge of the accused. This may also be true for randomly generated passwords existing outside a person's mind (i.e. written down, or stored in a password manager database).[52] Without intrusion into the mind of the accused, it is hard to say that the Fifth Amendment could provide any protection.[53]

The most secure and protected encryption scheme within the gambit of the Fifth Amendment is a memorized password-based encryption key that has been kept completely private. Compared to the other forms, the use of this memorized password relies solely on the accused's knowledge and is the type of key that appears in the few cases analyzing this issue and the most likely to implicate Fifth Amendment protections.

Decryption as an Act of Production

The two doctrines, act of production and foregone conclusion, interact heavily in the area of compelled decryption. To help structure the analysis, it is best to apply the doctrines in the most common facts arising in these cases. In most cases, the encrypted laptop, cell phone, or drive has come into the hands of the government pursuant to a valid warrant, or a Fourth Amendment exception (thereby extinguishing any claims to a reasonable expectation of privacy, or invocations of the exclusionary rule). The forensic expert begins to access the device but is met with a password prompt either as he or she activates the encrypted device, or begins searching through the file system. The prosecutor then acquires a subpoena or similar direction to the accused to either provide the password, enter the password and allow access, or provide a decrypted version of the drive. The accused files a motion to quash the subpoena, asserting his Fifth Amendment privilege.

While it is possible that the contents of the drive themselves may be privileged, presume, for this stark illustration of the doctrine, that the items are actually contraband, in that the files "were voluntarily prepared or compiled and are not testimonial, [they] therefore do not enjoy Fifth Amendment protection."[54] Although the documents may not be testimonial themselves, *Fisher* and *Hubbell* should still provide Fifth Amendment protection, as the act of providing the password, entering the password, or

---

[52] Nathan K. McGregor, *The Weak Protection of Strong Encryption: Passwords, Privacy, & Fifth Amendment Privilege*, 12 VAND. J. ENT. & TECH. L. 581, 592 (2010).
[53] *Id*.
[54] In re Boucher, No. 2:06-MJ-91, 2009 WL 424718, at *2 (D. Vt. Feb. 19, 2009) (citing United States v. Doe, 465 U.S. 605, 611–12, (1984) ("Doe I")).

decrypting the drive admits the files "existed, were in the accused's possession or control, and were authentic."[55] This is because "[t]he Fifth Amendment applies to acts that imply assertions of fact. It is the attempt to force an accused to disclose the contents of his own mind that implicates the Self–Incrimination Clause. Additionally, compelled testimony that communicates information that may lead to incriminating evidence is privileged even if the information itself is not inculpatory."[56]

Returning to our fact pattern, the act of decrypting a hard drive is protected by the Fifth Amendment, as the act of decryption, not just the sharing of the password, is itself testimonial. Decrypting is testimonial logically because it provides access to files no other person can know of or otherwise access. The act of encryption is an admission proving both the existence of the accused's files and the accused's possessory relationship to these files. Since only the person who encrypted an item would have the key to decrypt it (presuming the knowledge-based password), it shows possession, dominion, or control. Finally, the accused's act of production would be a necessary link in the authentication for the files should the prosecutor seek to have the evidence admitted in court, as no one but the accused would be able to confirm that the files produced are indeed the accused's files. Under this kind of scenario, it seems that the act of production privilege should apply unless the prosecutor were to grant the accused immunity and derivative immunity for his production.[57]

Foregone Conclusion and the Government

The traditional counterargument to the existence and knowledge prongs of the act of production privilege is that the government already had sufficient knowledge of the existence and location of the files, such that the accused's production adds "little or nothing to the sum total of the Government's information by conceding that he in fact has the [files]."[58] In encryption cases, the prosecutor would argue that as there is sufficient knowledge of the contents of the computer or media, it is a foregone

[55] *Id.* at *2. (internal quotations omitted).
[56] *See id.* (quoting and citing Doe v. United States, 487 U.S. 201, 209 (1988) ("Doe II"); *see also* Curcio v. United States, 354 U.S. 118 (1957) ("The 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.").
[57] *See* Hubbell, 530 U.S. at 45 (holding that use and derivative use immunity for anything derived from the act of production sufficiently protects an accused).
[58] Boucher, 2009 WL 424718, at *3 (quoting Fisher, 425 U.S. at 411).

conclusion what is on the drive, and the accused is adding little by his act of production. This argument nevertheless contains two major flaws.

The first problem is the standard of proof and type of knowledge required of the files before their existence is deemed a foregone conclusion. There is not much in the origin or evolution of the foregone conclusion doctrine to aid courts in applying it, as the Court in *Fisher* provided little description or further guidance.[59] The *Hubbell* Court highlighted the opacity of the *Fisher* Court's logic when attempting to apply the doctrine, by refusing to delineate it.[60] The *Hubbell* Court then rejected the foregone conclusion assertion by the government because it lacked an independent source of authentication in that case. In *Fisher*, the government had the testimony of the actual accountants that created the documents sought, and had not demonstrated with reasonable particularity the prior knowledge of the existence or location of the documents.[61] The *Hubbell* Court rejected the government's assertion that it possessed sufficient knowledge since all businessmen would generally possess the documents at issue in that case.[62] This was the last time the Supreme Court commented on the foregone conclusion doctrine. The Court's lack of guidance has proven problematic for lower courts, as prosecutors have routinely asserted the foregone conclusion doctrine to compel decryption. Due to this lack of analytical clarity on the part of the Supreme Court, courts vary on what facts must be shown with reasonable particularity, with some requiring knowledge of the contents of the folders and files and others merely the likely existence and location of any files. Note that the argument here stems from the premise that as the prosecutor knows there are always unencrypted files shielded by the encryption, the files' existence is a foregone conclusion—a circular argument which, if validated by courts, would forever swallow any real protection the Fifth Amendment is intended to provide.

Courts are split on whether or at what level of particularity to apply the foregone conclusion doctrine or to reject the circularity of that argument. The Court of Appeals for the Eleventh Circuit rejected the use of the foregone conclusion doctrine finding "[n]othing in the record before us reveals that the Government knows whether any files exist and are located on the hard drives; what's more, nothing in the record illustrates that the Government knows with reasonable particularity that [the accused] is even capable of accessing the

---

[59] Fisher, 425 U.S. at 411.

[60] "Whatever the scope of this 'foregone conclusion' rationale, the facts of this case plainly fall outside of it." Hubbell, 530 U.S. at 44.

[61] *Id*.

[62] *Id*.

encrypted portions of the drives."[63] The District Court for the Eastern District of Pennsylvania agreed with this standard of analysis in a Securities and Exchange Commission (SEC) case, rejecting the SEC's argument that the defendants' possession and control of the smartphones at issue compelled the application of the forgone conclusion doctrine, and thus the invalidation of the privilege.[64] The district court's rationale, that application of the foregone conclusion doctrine would require reasonable particularity of the actual location and existence on the specific device, was also applied by the Circuit Court of Virginia.[65] Finally, while addressing the foregone conclusion doctrine outside the context of encryption, the District Court for the Eastern District of Michigan emphatically defended the position that the government is required to show actual knowledge of documents prior to production when it stated that, "[i]n other words, the government must show that it had knowledge of the documents before they are produced. [The] government cannot make an end-run around the Fifth Amendment by fishing for a document that will answer a question for which it could not demand an answer in oral examination."[66]

In contrast, some courts have accepted the government's argument that the foregone conclusion doctrine can be satisfied at a high level of generality.[67] In *United States v Friscou*, the trial court found it sufficient to apply the foregone conclusion doctrine based solely on the information that the government knew that there were files within the computer and that it was owned by the accused.[68] The reasonable particularity standard was not mentioned in the ruling.[69] This application of the foregone conclusion doctrine was shared by the Supreme Judicial Court of Massachusetts, when the court held the files' existence were a foregone conclusion allowing decryption as the accused admitted that all his documents were on his computer; the documents were all encrypted; the accused stated that the police would be unable to obtain files from the computer (demonstrating knowledge of

[63] In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012).
[64] Sec. & Exch. Comm'n v. Huang, No. CV 15-269, 2015 WL 5611644, at *3 (E.D. Pa. Sept. 23, 2015) ("Here, the SEC proffers no evidence rising to a 'reasonable particularity' any of the documents it alleges reside in the passcode protected phones.").
[65] Commonwealth v. Baust, 89 Va. Cir. 267 (2014).
[66] United States v. Sabit, No. 14-MC-50155, 2014 WL 1317082, at *3 (E.D. Mich. Apr. 1, 2014).
[67] United States v. Fricosu, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012).
[68] *Id*. at 1237.
[69] *Id*.

accused's attempt to block retrieval); and that the accused knew the key.[70] Neither of these cases discussed the authentication aspects of the underlying act of production doctrine.

While a split is forming around the foregone conclusion doctrine between federal district courts, circuit courts, and even state courts, it seems the best example of the proper application of the doctrine exists in the first federal case on record addressing encryption and self-incrimination, *In re Grand Jury Subpoena to Sebastien Boucher* (*Boucher* I).[71] In *Boucher* I, the accused was stopped entering the United States at the Canadian Border.[72] The border agent found a laptop in the accused's car and began to inspect it.[73] The agent observed files that he believed may have been child pornography.[74] The accused was read his *Miranda* rights and waived his right to remain silent.[75] The agent asked the accused to show him where he had downloaded child pornography.[76] The accused showed him the contents of his "Z:\" drive and confessed that he would accidently download child pornography from newsgroups at times.[77] The agent located several photos and video of child pornography and arrested the accused, seized the laptop, and shut it down.[78]

The laptop was then taken for further forensic analysis, but when the agents re-booted the laptop they were met with a password.[79] The government issued the accused a subpoena for the defendant to produce his password.[80] The accused filed a motion to quash the subpoena on Fifth Amendment grounds.[81] The federal magistrate judge ruled that producing the password was testimonial and the act of decrypting the documents overall was also testimonial under the Act of Production doctrine.[82] The magistrate judge then rejected the foregone conclusion argument on the basis that the government was seeking the entire contents of the Z:\ drive, but had only seen a small portion.[83] The magistrate judge reasoned that the discovery of the substantial

---

[70] Commonwealth v. Gelfgatt, 468 Mass. 512, 524, 11 N.E.3d 605, 615 (2014).
[71] No. 2:06-mj-91, 2007 WL 4246473 (D. Vt. Nov. 29, 2007).
[72] *Id*. at *1.
[73] *Id*.
[74] *Id*.
[75] *Id*.
[76] *Id*.
[77] *Boucher I, No.* 2:06-mj-91, 2007 WL 4246473, at *1-2.
[78] *Id*. at *2.
[79] *Id*.
[80] *Id*.
[81] *Id*.
[82] *Id*. at *3-4.
[83] *Boucher I,* No. 2:06-mj-91, 2007 WL 4246473, at *5-6.

remainder of the Z: drive would add much to the government's case, thus mooting the foregone conclusion argument.[84] The magistrate judge quashed the subpoena.[85]

The government appealed that decision to the Chief Judge of the District Court.[86] The District Court reversed the magistrate judge, holding that the foregone conclusion doctrine did indeed apply.[87] The reason the foregone conclusion doctrine applied in this case was that the accused had already waived his right to remain silent and shown the agents the Z:\ drive files.[88] The court reasoned that knowledge of the existence (and contents) of the Z:\ drive, the location of the files, and the admission that the laptop belonged to the accused, and the confession regarding accused's files were sufficient to meet the foregone conclusion doctrine (though the court did not address the impact of the files the government had not examined previously).[89] These prior disclosures by the accused met the knowledge, dominion, and authenticity requirements, as all this testimony could now be provided by the border agent who had examined the accused's files.[90]

To echo the *Hubbell* Court, whatever the limits of the foregone conclusion doctrine, this case seems the best application of the doctrine to digital encryption so far. *Hubbell* recognizes the testimonial aspects of both producing a password and the act of decrypting files, and the *Boucher* case balances those aspects with the specific facts and disclosures from the accused. *Boucher*, applying *Hubbell* recognizes that, absent the accused's own specific disclosures, the Fifth Amendment would likely protect the accused from decryption. It uses the accused's own prior waiver of the right against him; rightly placing the control and responsibility for the shield of the Fifth Amendment in a defendant's hands.

A WAY FORWARD FOR ENCRYPTION CASES

As it stands, the jurisprudence governing compulsory decryption is poised to devolve into an indiscernible morass. Courts, lacking clear guidance on compulsory decryption under the Fourth and Fifth Amendment, and facing the accelerating technological complexities of encryption systems, tend to

---

[84] *Id*.
[85] *Id*. at *6
[86] In re Boucher, No. 2:06-MJ-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009) ("Boucher II").
[87] *Id*. at *4.
[88] *Id*. at *3.
[89] *Id*.
[90] *Id*.

adopt analogies justifying the result they want to reach, regardless of their accuracy or nuance, such as "key to a desk drawer" or "combination to a safe."[91] Additionally, some courts require little knowledge beyond mere ownership before they approve the use of the foregone conclusion doctrine. Other courts hold the prosecutor to similar knowledge requirements found in *Fisher*: independent knowledge from other sources or the accused directly that independently establishes the contents, knowledge, possession, and authenticity outside the act of production. No matter what standards or method courts use, the majority of cases seem driven by reasoning propelled by a certain desired result. If a court deems access to the material necessary, it will adopt the analogy or standard of knowledge that allows for access. As it stands, there is no discernable rule, standard, or analysis emerging for the use of the act of production or foregone conclusion doctrines as applied to encryption.

This is especially troublesome as ever-advancing technology will only make encryption increasingly prevalent. The Supreme Court must eventually resolve the question, but until that time, lower courts should work to better discern usable principles with the doctrines they already have, and err in favor of protecting the Constitutional rights. A right as core to American values as the one protecting against compulsory self-incrimination deserves solemn deference, regardless of the fact that modern encryption may sometimes block significant evidence collection. To that end, this article proposes an analysis that seems to best balance the individual right, and which properly assigns the burden to the government to improve its investigation techniques to properly employ the foregone conclusion doctrine in the future.

Compulsory Decryption is Testimonial

First, as a legal principle, practitioners, governments, and courts alike should accept that compelling an individual to either produce a password or to compulsorily decrypt their digital files in a private knowledge-based-key scheme is presumptively a testimonial act. This is a reasonable position that avoids the need to extend obscure doctrines to weaken the intent and purpose of the Self-Incrimination Clause. It is immaterial what analogy is used by the courts, be it a physical lock and key, combination to a safe, or the much more

[91] *See* Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L. J. 357 (2003) (writing how courts and practitioners must be wary in deciding issues in the cyber realm by analogy as the perspective of the analogy (real world vs. code level) often dictates the outcome of the legal issue).

technically accurate analogy of a translation of a coded ledger: The result is the same.[92] In cases involving a private key, there is never a way to avoid an accused being a "link in the chain" of his own incrimination.[93] The government must rely on his particular combination to access the material.[94] Recognizing that an encrypted file system with one private key has but one owner to the exclusion of the rest of the world, the unlocking and production will always broadcast to the world that the accused was the only person capable of controlling the incriminating evidence. Additionally, absent a tour through the evidence[95] or facts gained elsewhere in the investigation, the accused will continually be the only source of authentication for admission.

A small thought experiment involving the admission steps at court displays the incrimination problem. Imagine the court orders a defendant to produce an unencrypted file system, notwithstanding that this would be an impermissible compulsory creation of evidence not previously in existence. Once the prosecutor presents the evidence for admission to the judge, he would be forced to mention the accused in the chain of custody under Federal Rule of Evidence 901.[96] Imagine the judge allows the use of the accused's authentication in some form, then what can be done in front of the jury? In front of the jury, the prosecutor would have to omit the origin of the evidence—deceiving the factfinder—in its predicate foundation and argument. This would require the accused to either object on foundation or argue its lack of weight based on its suspicious origins. Does this defense argument then open the door for the prosecutor to again rely on the accused's production? Any trial practitioner can see how this thought exercise becomes unwieldy and unavoidably places the accused in the classic "cruel trilemma" of testifying, which every accused has a Constitutional right not to do.[97] The better practice judicially and constitutionally is to acknowledge compulsory decryption as presumptively testimonial.

---

[92] *See* McGregor, *supra* note 52, at 599 (detailing how decryption could be regarded as a continuous translation of coded text into discernable form thereby elevating the testimonial character of it since the translator is actually creating a new document or file; a direct testimonial infringement as opposed to a mere Act of Production issue).

[93] *See* Hoffman v. United States, 341 U.S. 479, 486 (1951).

[94] *See* Hubbell, 530 U.S. at 43 (acknowledging that a combination to a safe would carry greater Fifth Amendment protection).

[95] *See* In re Boucher, No. 2:06-mj-91, 2007 WL 4246473 (D. Vt. Nov. 29, 2007).

[96] FED. R. EVID. 901.

[97] Pennsylvania v. Muniz, 496 U.S. 582, 597 (1990) ("the 'trilemma' of truth, falsity, or silence, and hence the response (whether based on truth or falsity) contains a testimonial component.").

The logic of the foregone conclusion doctrine is unbearably circular: if the prosecutor knows sufficient information that the accused's contribution adds so little to his or her case, the justification for its production is of equally marginal value. The government should not compel evidence that is cumulative to independent evidence already in its possession. In fact, the Rules of Evidence bar the admission of cumulative evidence.[98] Thus, if the decrypted files are not cumulative then they add something to the government's case. If they add something to the government's case, then the decrypted files are a link in the chain of evidence against the accused. If the decrypted files are a link and the decryption comes from the accused, then his self-incrimination right has been infringed because he was compelled to join that chain. This seems the most logical interpretation of the function behind the foregone conclusion doctrine.

Nevertheless, the doctrine exists and may be applicable in the narrowest circumstances, such as those similar to the standard of knowledge originally displayed in *Fisher*. In *Fisher*, the government had the complete testimony of the accountant who prepared the subpoenaed tax documents. The accountant likely could have testified to contents of the tax documents, had the documents themselves been unavailable. The documents themselves lacked any testimonial value and instead were more the best evidence of the tax issues than a link in the chain of evidence. This is the intended and proper application of the foregone conclusion doctrine, although authentication concerns remain. Applied to encrypted evidence, this would require the prosecutor to show by a preponderance of the evidence that he or she had sufficient knowledge to substitute for the files provided by testimony or copies of the evidence.[99] Any lesser standard swallows the self-incrimination right by allowing the government to avoid the right by mere prediction of the files' existence over actual knowledge; the knowledge piece then substantiated by the accused, against his will.

A Plausible Way Forward

It is arguable that this approach does not afford the prosecutor sufficient opportunity to acquire evidence it is otherwise entitled to under a

---

[98] *See* FED. R. EVID. 403.

[99] The preponderance of the evidence standard is required to prove Miranda waiver. *See* Colorado v. Connelly, 479 U.S. 157, 168 (1986).

Fourth Amendment analysis.[100] Some will argue that it would allow for a "law-free zone" of impunity by easy employment of computer encryption blocking lawful authority.[101] This is not the intent of the approach, nor would it be the result although the protection, at times, may result in the constitutionally appropriate suppression of evidence in the government's case. Moreover, the approach would prevent the otherwise inevitable dilution of the Constitutional protection against self-incrimination as the doctrine is inexpertly applied in encryption cases. The proposal outlined here appropriately shifts the burden of production and investigation to the government, and rather than acting as a complete bar, requires that the government employ greater investigative methods and techniques to gain the evidence rather than the shortcut of seeking production from the accused.

To illustrate my point, consider the possible investigative techniques that could be employed in cases like *Boucher*. A border agent discovers some evidence of child pornography possession. Instead of immediately arresting and seizing the laptop, the agent could obtain a warrant and install a suite of malware on the computer that could capture both keystrokes and report any website or file sharing downloads. The agent then quietly returns the laptop to the subject. The government then captures this evidence over a brief period of time and then executes an arrest. The evidence is now much more likely a foregone conclusion as the government has had "surveillance" on the accused via malware. This same technique applies to those computers identified as broadcasting or downloading illicit files on the internet. Once the government receives a report, be it personal or technical, of an individual dealing with contraband online, instead of immediately seizing the material, the government could once again gain a warrant and "hack" the computer while it is connected in an unencrypted state. This lawful surveillance could provide all the government needs to know without involving the accused's testimony at all.

These methods require additional assets and skills be used in computer crimes than the current method requires. Currently, it is unlikely that the typical border agent like the one in *Boucher* has the forensic skills to engage

---

[100] The government, having satisfied the Fourth Amendment's search and seizure requirements, would otherwise be entitled to "every man's evidence" absent the assertion of a valid privilege. *See* United States v. Monia, 317 U.S. 424, 442 (1943).

[101] James B. Comey, Director, Fed. Bureau of Investigation, Address at the Brookings Institution: Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? (Oct. 16, 2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course [https://perma.cc/5P6P-RWSJ] (describing encryption and Tor as creating a zone of lawlessness).

in the investigative techniques described above. Surely, the government would need to better train and employ personnel to implement these digital investigations before this level of digital surveillance becomes a viable option. That is as it should be, as the government should be held to the same investigative standards as it would be if the issue occurred offline.

In the physical world, if a defendant opts to remain silent in the face of an investigation, the government is left to build its case using traditional methods: physical surveillance, wiretapping, procuring a warrant to search for evidence upon probable cause. No lesser standard should be applied to digital evidence. If the prosecutor has probable cause to believe that encrypted evidence exists on a computer, it should not be able to argue that the knowledge of the existence of the evidence entitles them to production from the accused under *Hubbell*. Instead, the government should be required, as in other cases, to use other methods and tools to obtain this purported evidence without the involvement of the accused to assist them in translating the material into useable form.[102] This approach would ensure that the foregone conclusion doctrine, if it must be applied, is applied with the greatest deference to the underlying principles of the Self-Incrimination Clause—the government could then show by these other methods conclusive possession and knowledge of the evidence, truly "adding little or nothing to the government's case by the disclosure of the accused."

CONCLUSION

Accessing encrypted digital evidence requires ingenuity and technical knowledge above that which is normally employed in offline investigations. The cyber realm is an area in constant change and innovation, where stronger security and access methods will make it more and more of a challenge to catch smart criminals online. Despite these additional challenges, the Constitution's principles must be properly respected and adapted even to this new evidence. In so doing, the government, courts, and American people can be assured that upholding the precious rights of all citizens—even those accused of crimes—will be a foregone conclusion.

---

[102] The volume of methods and techniques possible of employment is enormous, but there is a rational corollary to every physical investigative technique and separate article dedicated to their employment. Summarily, the government could obtain a warrant to "wiretap" an accused's internet traffic in real-time and observe all data flowing through the internet service provider. The government could gain a warrant to "enter" and "search" the accused's computer while it is turned on and connected to the internet (which places it in a generally unencrypted state while it is being used).