FIU Law Review

Volume 10 | Number 2 Article 21

Spring 2015

An Act of Decryption Doctrine: Clarifying the Act of Production Doctrine's Application to Compelled Decryption

Joseph Jarone
Florida International University College of Law

Online ISSN: 2643-7759

An Act of Decryption Doctrine: Clarifying the Act of Production Doctrine's Application to Compelled Decryption

Joseph Jarone[*]

I. INTRODUCTION

New technology creates new legal challenges. With the coming of the information age, encryption has become ubiquitous.[1] Almost anyone can easily acquire encryption software and use it to prevent unwanted third parties from reading one's private information.[2] Encryption can be incredibly powerful and nearly impossible to break.[3] This technology presents special problems for law enforcement because criminals use it to hide their misdeeds.[4] Due to encryption's strength, sometimes the only way to gain access to the encrypted evidence is with the assistance of the accused.[5] Compelling the accused to decrypt and assist in his or her own

[*] J.D. Candidate, 2015, Florida International University College of Law. I would like to thank those members of the *FIU Law Review* whose diligent efforts made this Comment ready for publication. I would also like to thank Clara Gomez and Amber Kornreich for their invaluable assistance. Finally, I am grateful for Professor Megan Fairlie for her guidance.

[1] *See* Dan Terzian, *The Fifth Amendment, Encryption, and the Forgotten State Interest*, 61 UCLA L. REV. DISC. 298, 302-03 (2014). Prior to 2007, there were no cases addressing encryption. *Id.* Now there is a "small universe." *Id.*; s*ee, e.g.*, *In re* Boucher, No. 2:06-mj-91, 2007 WL 4246473 (D. Vt. Nov. 29, 2007), *rev'd*, 2009 WL 424718 (D. Vt. Feb. 19, 2009); *In re* Boucher, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009); United States v. Fricosu, 841 F. Supp. 2d 1232 (D. Colo. 2012); *In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335 (11th Cir. 2012) [hereinafter *Doe III*]; *In re* Decryption of a Seized Storage Sys., 2:13-mj-00449-WEC, 2013 BL 116993 (E.D. Wis. Apr. 19, 2013), *overruled by* 2:13-mj-00449-WEC, 2013 BL 153162 (E.D. Wis. May 21, 2013) [hereinafter *Feldman I*]; *In re* Decryption of a Seized Storage Sys., 2:13-mj-00449-WEC, 2013 BL 153162 (E.D. Wis. May 21, 2013) [hereinafter *Feldman II*]; United States v. Kirschner, 823 F. Supp. 2d 665 (E.D. Mich. 2010).

[2] Encryption software is available commercially for a fairly low price. SYMANTIC, http://www.symantec.com/drive-encryption (last visited Feb. 13, 2014); BITLOCKER DRIVE ENCRYPTION, http://windows.microsoft.com/en-GB/windows7/products/features/bitlocker (lasted visited Feb. 13, 2014); McAfee Endpoint Encryption, MCAFEE, http://www.mcafee.com/us/products/complete-data-protection.aspx (last visited Feb. 13, 2014). Some software is even freely available on the Internet. *See, e.g.*, TRUECRYPT, http://www.truecrypt.org/ (last visited Feb. 13, 2014); GNU PRIVACY GUARD, http://www.gnupg.org/ (last visited Feb. 13, 2014); AXCRYPT, http://www.axantum.com/axcrypt/ (last visited Feb. 13, 2014).

[3] *See* sources cited, *infra* note 32.

[4] *See* cases cited *supra* note 1; *see also Statements by Louis J. Freeh, Director of the Federal Bureau of Investigation Before the Senate Committee*, ELECTRONIC PRIVACY INFORMATION CENTER (last visited Mar. 28, 2014), http://epic.org/crypto/legislation/freeh_797.html (discussing national security concerns with encryption).

[5] *See, e.g.*, *Boucher*, 2007 WL 4246473, at * 2; *Doe III*, 670 F.3d at 1340; *Fricosu*, 841 F. Supp.

prosecution runs headlong into the Fifth Amendment Right Against Compelled Self-Incrimination.

This Comment addresses the Fifth Amendment implications of compelled decryption. In addressing the issue of whether the government can compel someone to decrypt, courts have applied the "act of production doctrine." This somewhat arcane doctrine was originally created to address whether the physical production of physical documents receives a Fifth Amendment privilege.[6]

This Comment will discuss encryption technology in section II.A, the act of production doctrine in section II.B, and the current case law in section II.C. In section III, this Comment will argue that the lower courts, in applying this "act of production" doctrine, have done so incorrectly. In particular, courts have failed to recognize the difference between the physical production of documents and compelled decryption. The resulting analysis is unduly confusing and provides more Fifth Amendment protection than what the Constitution requires. This Comment will propose an alternative application in section IV. Finally, in section V, this Comment will discuss the insurmountable problem of the accused's refusal to decrypt.

II. BACKGROUND

A. Encryption Background

Encryption has its historical roots in antiquity and was famously used in World War II with the enigma machine.[7] Prior to the Information Age, encryption was closely regulated.[8] Following the popularization of the Internet, the government's attempts at regulation ultimately failed.[9]

2d at 1234. *But see* Motion to Dismiss Application, at 1-2, United States v. Decryption of a Seized Data Storage Sys. (2:13-mj-00449), *available at* http://www.bloomberglaw.com/document/X1Q6MM164J82 (dismissing a case after the government was able to decrypt the device).

[6] *See* Fisher v. United States, 425 U.S. 391, 434 (1976) (Marshall, J., concurring) (lamenting abandonment of the pragmatic *Boyd v. United States*, 116 U.S. 616 (1886), standard and its replacement with an "unduly technical focus on the act of production itself"); Samuel A. Alito, Jr., *Documents and the Privilege Against Self-Incrimination*, 48 U. PITT. L. REV. 27, 77-78 (1986) (saying the act of production doctrine "has led the fifth amendment into a realm of almost metaphysical abstraction"); Robert P. Mosteller, *Cowboy Prosecutors and Subpoenas for Incriminating Evidence: The Consequences and the Correction of Excess*, 58 WASH. & LEE L. REV. 487, 489 (2001) (calling the act of production doctrine "esoteric"); *see, e.g.*, *Fisher*, 425 U.S. 391; United States v. Doe, 465 U.S. 605 (1984) [hereinafter *Doe I*]; Doe v. United States, 487 U.S. 201 (1988) [hereinafter *Doe II*]; United States v. Hubbell, 530 U.S. 27 (2000).

[7] CHRISTOF PAAR & JAN PELZL, UNDERSTANDING CRYPTOGRAPHY 2 (1998), *available at* http://link.springer.com/book/10.1007%2F978-3-642-04101-3.

[8] James Andrew, *2014 as the Year of Encryption: A (Very) Brief History of Encryption Policy*, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (Jan. 10, 2014), http://csis.org/publication/2014-year-encryption-very-brief-history-encryption-policy.

[9] *See id.*; Aaron Perkins, Comment, *Encryption Use: Law and Anarchy on the Digital Frontier*,

Currently, some regulation of encryption exists, but for the most part, people's access to encryption is unhindered.[10] Through the use of easily accessible software one can encrypt both digital messages and the contents of an electronic storage device.[11]

The principles governing encrypting messages are nothing new.[12] A simple "substitution cipher"[13] such as the Caesar Cipher can encrypt the contents of a message. Take for example the following quote from Justice Jackson:

> If there is any fixed star in our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion or force citizens to confess by word or act their faith therein.[14]

Put through a simple substitution cipher, the quote becomes:

> Mj xlivi mw erc jmbih wxev mr syv gsrwxmxyxmsrep gsrwxippexmsr, mx mw xlex rs sjjmgmep, lmkl sv tixxc, ger tviwgvmfi alex wlepp fi svxlshsb mr tspmxmgw, rexmsrepmwq, vipmkmsr, sv sxliv qexxivw sj stmrmsr sv jsvgi gmxmdirw xs gsrjiww fc asvh sv egx xlimv jemxl xlivimr.[15]

The first quote is called the "plaintext"; the coded message is called the "cipher text."[16] The plaintext was "encrypted" using an algorithm where each character was moved to the right four characters (e.g., A became E; I became M).[17] Decryption requires moving each character of the cipher text back four characters to put it in its original position.[18]

The cipher shown above is one of the simplest forms of encryption.[19] One can most likely break it if given a few minutes and a piece of paper. However, asymmetrical public key encryption,[20] such as "Pretty Good

41 HOUS. L. REV. 1625, 1629-40 (2005); Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 434-41 (2013).

[10] *See* sources cited *supra* note 9.

[11] *See* sources cited *supra* note 2.

[12] *See* PAAR, *supra* note 7, at 2.

[13] *See id.* at 6 ("Historically [the substitution] type of cipher has been used many times, and it is a good illustration of basic cryptography.").

[14] *W. Va. State Bd. of Educ. V. Barnette*, 319 U.S. 624, 642 (1943).

[15] *See* PAAR, *supra*, note 7, at 18-19; *Surveillance Self-Defense*, ELECTRONIC FRONTIER FOUNDATION, https://ssd.eff.org/tech/encryption (last visited Feb. 13, 2014).

[16] *See* RAMAKRISHNA THURIMELLA & LEEMON C. BAIRD III, *Network Security,* in APPLIED CRYPTOGRAPHY FOR CYBER SECURITY AND DEFENSE : INFORMATION ENCRYPTION AND CYPHERING 2 (2011); PAAR, *supra* note 7, at 3-5.

[17] *See* THURMIMELLA, *supra* at note 16, 2; PAAR, *supra* note 7, at 6-7.

[18] *See* sources cited *supra* note 17.

[19] *See* PAAR, *supra*, note 7, at 6.

[20] *See generally* Richard T. Petras, *Privacy for the Twenty-First Century: Cryptography*, 94 THE

Privacy" (PGP), a software program developed in 1991 by Philip Zimmerman, provides a far more secure system of encryption.[21] Encryption software like PGP is both free online and simple to use.[22]

The information stored on a computer or electronic storage device can also be encrypted. Encrypted scrambles the contents of an electronic storage device, making it unreadable. There are a variety of encryption methods including full-disk encryption (FDE), file and folder encryption, virtual volume encryption, and hard disk password.[23] FDE makes the entire device inaccessible and unreadable if the user does not know the correct password.[24] Once the password has been entered, the device becomes readable.[25] File or folder encryption makes individual files or folders inaccessible (e.g., encrypting "my documents").[26] Virtual volume encryption provides protection for information stored inside of a container (e.g., one's C drive or a portable hard drive) and requires a password or key to access the container.[27] Finally, a hard disk password is much like FDE except that where FDE uses software that interacts with one's operating system, with hard disk encryption, the user's computer hardware prompts the user for a key with no involvement from the operating system.[28]

While methods of cracking encryption exist,[29] one of the problems facing law enforcement is that without the passphrase to an encrypted device, decryption becomes difficult or even impossible.[30] Although

MATHEMATICS TEACHER 689, 691-92 (2001). Asymmetrical key encryption requires both a public and a private key. *PAAR, supra* note 7, at 6. A message encoded with a public key can only be decoded with the private key. *Id.* As a result, the public key can be made public without risk that a third party could use it to decode encrypted messages. *Id.* at 7-8. This allows one to be conveniently contacted with encrypted messages with little risk of those messages being read by another. *Id.* at 7-8.

[21] *See generally* OPENPGP, http://www.openpgp.org/ (last visited Mar. 28, 2014).

[22] *Id.*

[23] *See generally Surveillance Self-Defense*, ELECTRONIC FRONTIER FOUNDATION, https://ssd.eff.org/tech/disk-encryption (last visted Feb. 13, 2014); Eoghan Casey et al., *The Growing Impact on Full Disk Encryption on Digital Forensics*, DIGITAL INVESTIGATION 8, 130 (2011); KAREN SCARFONE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, NIST SPECIAL PUBLICATION 800-111, GUIDE TO STORAGE ENCRYPTION TECHNOLOGY FOR END USER DEVICES 3-1 - 3-4 (2007).

[24] *See* sources cited *supra* note 23.

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *See generally* J. Alex Halderman et al., *Lest We Remember, Cold Boot Attack on Encryption Keys*, Proc. 2008 USENIX Security Symposium (2008), *available at* http://citpsite.s3-website-us-east-1.amazonaws.com/oldsite-htdocs/pub/coldboot.pdf (cold-boot attack); MATT CURTIN, BRUTE FORCE: CRACKING THE DATA ENCRYPTION STANDARD 23-34 (2005) (brute-force attack); Casey et al., *supra* note 23, at 132-34 (live acquisition technique).

[30] Casey et al., *supra* note 23, at 130; Terzian, *supra* note 1, at 303-04; *see, e.g.*, *In re* Boucher, No. 2:06-mj-91, 2007 WL 4246473, at *2 (Nov. 29, 2007); *Doe III*, 670 F.3d 1335, 1340 (11th Cir. 2012).

encryption can keep one's private information private, it can also bar law enforcement's attempts to investigate crimes involving computers.[31]

B. The Modern Interpretation of the Fifth Amendment Self-Incrimination Clause

The Self-Incrimination Clause of the Fifth Amendment states, "No person . . . shall be compelled in any criminal case to be a witness against himself."[32] The Fifth Amendment does not grant one an unfettered "right to remain silent."[33] Instead, before the privilege attaches, an act must satisfy three elements. The act must be: (1) compelled, (2) incriminating, and (3) testimonial.[34]

A seemingly obvious, but important, point is that these elements are conjunctive.[35] The government can, therefore, compel the accused to incriminate himself or herself—so long as the compelled act is not testimonial.[36] Similarly, one can incriminate oneself with a testimonial communication, but if the government does not compel it, it is not privileged.[37] The government may also compel a testimonial act so long as one does not incriminate oneself when making it.[38]

[31] *See* sources cited *supra* note 2, 5.

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

[33] *See Doe II*, 487 U.S. 201, 214 n.12 (1988); *see, e.g.*, United States v. Dionisio, 410 U.S. 1, 13-14 (1973) (holding that compelling one to speak for the purposes of a voice exemplar was not privileged).

[34] Hiibel v. Sixth Jud. Dist. Ct. of Nev., 542 U.S. 177, 189 (2004).

[35] *Id.*

[36] *See* Fisher v. United States, 425 U.S. 391, 408 (1976); *see, e.g.*, Schmerber v. California, 384 U.S. 757 (1966) (permitting the government to compel a defendant to provide an incriminating blood sample because it was non-testimonial); *see also* Holt v. United States, 218 U.S. 245, 252 (1910) ("But the prohibition of compelling a man in a criminal court to be witness against himself is a prohibition of the use of physical or moral compulsion to extort communications from him, not an exclusion of his body as evidence when it may be material. The objection in principle would forbid a jury to look at a prisoner and compare his features with a photograph in proof. Moreover, we need not consider how far a court would go in compelling a man to exhibit himself. For when he is exhibited, whether voluntarily or by order, and even if the order goes too far, the evidence, if material, is competent.").

[37] *See Fisher*, 425 U.S. at 409-10; *Doe I*, 465 U.S. 605, 611-12 (1984); *see also* Edwards v. Arizona, 451 U.S. 477, 482 (1981) (noting that one may waive one's *Miranda* rights, but the waiver must be, among other things, voluntary); Colorado v. Connelly, 479 U.S. 157 (1986) (holding that the defendant's confession was voluntary when he approached the police during a psychotic episode and confessed to a murder).

[38] *See generally* Fed. R. Civ. P. 45 (subpoenas in federal civil proceedings); Fed. R. Crim. P. 17 (subpoenas in federal criminal proceedings).

1. Element 1: Compelled

To satisfy the compulsion element, the government must in some way coerce action.[39] When an act is done voluntarily, this element is not present.[40] For example, with a personal paper or document, the voluntary act of writing the document would not be compelled, but a government subpoena to produce the document would be.[41] Thus, if someone writes in his or her diary "I killed so-and-so" and the government seizes the diary, then the diary receives no Fifth Amendment protection because its creation was voluntary.[42] However, if the government were to coerce the same person to sign a confession saying much the same thing—or even affirm the fact that he or she wrote the diary—then the compulsion element would be present.[43]

2. Element 2: Incriminating

The incrimination element requires that an act either incriminate or lead to the sicvoery of incriminating evidence.[44] One does not necessarily need to have committed a wrongdoing; even the innocent may fear self-incrimination.[45] But the danger of self-incrimination must not be merely "imagined and unsubstantial."[46] Furthermore, to satisfy this element, the

[39] Minnesota v. Murphy, 465 U.S. 420, 427 (1984); *see also* Miranda v. Arizona, 384 U.S. 436 (1966) (holding that to avoid the danger of compelled self-incrimination, the accused must be warned of his or her Fifth and Sixth Amendment rights).

[40] *Doe I*, 465 U.S. at 610-11; *see also* South Dakota v. Neville 459 U.S. 553 (1983) (holding one is not compelled to refuse an alcohol test although the results of the test tended to incriminate).

[41] *Fisher*, 425 U.S. at 409-12. In this case, the Supreme Court addressed the question of whether the defendant's tax records were privileged. *Fisher*, 425 U.S. at 410. In *Fisher*, the taxpayer's accountant produced the records and the taxpayer's lawyer was in current possession of the records. *Id.* The Court found that the *creation* tax records were not compelled because the government did not compel the records' creation. *Id.*

[42] *Cf. Doe I*, 465 U.S. at 610 ("Where the preparation of business records is voluntary, no compulsion is present.") (footnote omitted).

[43] *Id.* at 611; *see also* Ziang Sung Wan v. United States, 266 U.S. 1, 14-15 (1924) ("[T]he requisite of voluntariness is not satisfied by establishing merely that the confession was not induced by a promise or a threat. A confession is voluntary in law if, and only if, it was, in fact, voluntarily made. A confession may have been given voluntarily, although it was made to police officers, while in custody, and in answer to an examination conducted by them. But a confession obtained by compulsion must be excluded whatever may have been the character of the compulsion, and whether the compulsion was applied in a judicial proceeding or otherwise.") (footnotes omitted).

[44] Kastigar v. United States, 406 U.S. 441, 444-45 (1972); United States v. Hubbell, 530 U.S. 27, 38 (2000); Hoffman v. United States, 341 U.S. 479, 486 (1951) ("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.").

[45] Ohio v. Reiner, 532 U.S. 17, 21 (2001).

[46] Mason v. United States, 244 U.S. 362, 365-66 (1917) ("[W]e are of opinion that the danger to be apprehended must be real and appreciable, with reference to the ordinary operation of law in the

witness must incriminate himself or herself. That is, if one's testimony just incriminates someone else, the incrimination element is not satisfied.[47]

3. Element 3: Testimonial

The Supreme Court has drawn a distinction between action that is testimonial versus action that is non-testimonial.[48] Testimonial acts require one to make use of "the contents of his own mind."[49] Testimonial acts are often verbal communications used for their contents, such as statements made during custodial interrogation,[50] before a grand jury,[51] or during a trial.[52] Verbal communication will almost always be testimonial.[53]

Physical or real evidence is not privileged.[54] For example, in *Schmerber v. California*, the Supreme Court held that the privilege against compelled self-incrimination did not apply when the government obtained a

ordinary course of things—not a danger of an imaginary and unsubstantial character, having reference to some extraordinary and barely possible contingency, so improbable that no reasonable man would suffer it to influence his conduct. We think that a merely remote and naked possibility, out of the ordinary course of law and such as no reasonable man would be affected by, should not be suffered to obstruct the administration of justice."); Marchetti v. United States, 390 U.S. 39, 88 (1968); *see also Hoffman*, 341 U.S. at 486 ("The witness is not exonerated from answering merely because he declares that in so doing he would incriminate himself—his say-so does not of itself establish the hazard of incrimination.").

[47] Couch v. United States, 409 U.S. 322, 328 (1973) ("[T]he Fifth Amendment privilege is a personal privilege: it adheres basically to the person, not to information that may incriminate him. As Mr. Justice Holmes put it: 'A party is privileged from producing the evidence, but not from its production.' The Constitution explicitly prohibits compelling an accused to bear witness 'against himself': it necessarily does not proscribe incriminating statements elicited from another.") (citations omitted); United States v. Nobles, 422 U.S. 225, 225 (1975) ("[T]he Fifth Amendment privilege against compulsory self-incrimination, being personal to the defendant, does not extend to the testimony or statements of third parties called as witnesses at trial.").

[48] Schmerber v. California, 384 U.S. 757, 763-64 (1966); Fisher v. United States, 425 U.S. 391, 408 (1976); United States v. Hubbell, 530 U.S. 27, 34 (2000).

[49] *Doe II*, 487 U.S. 201, 211 (1988) (quoting Curcio v. United States, 354 U.S. 118, 128 (1957); *See, e.g.*, *Hubbell*, 530 U.S. at 43 (using contents of the mind to put together documents in response to subpoena is testimonial); *Curcio*, 354 U.S. at 128 (testifying orally to the whereabouts of records required the witness to use the contents of his own mind); *see also* Pennsylvania v. Muniz, 496 U.S. 582, 597 (1990) (footnotes omitted) ("Whenever a suspect is asked for a response requiring him to communicate an express or implied assertion of fact or belief, the suspect confronts the 'trilemma' of truth, falsity, or silence, and hence the response (whether based on truth or falsity) contains a testimonial component.").

[50] *See, e.g.*, Miranda v. Arizona, 384 U.S. 436 (1966).

[51] *See, e.g.*, Curcio v. United States, 354 U.S. 118 (1957).

[52] *See* Counselman v. Hitchcock, 142 U.S. 547 (1892).

[53] *Doe II*, 487 U.S. 201, 213 (1988) ("There are very few instances in which a verbal statement, either oral or written, will not convey information or assert facts. The vast majority of verbal statements thus will be testimonial and, to that extent at least, will fall within the privilege.") (footnotes omitted).

[54] *See* Schmerber v. California, 384 U.S. 757, 763 (1966) (citing Holt v. United States, 218 U.S. 245, 252-53 (1910)); Pennsylvania v. Muniz, 496 U.S. 582, 588-89 (1990); *see also* United States v. Wade, 388 U.S. 218, 222 (1967) (standing in a police lineup non-testimonial).

blood sample from the defendant.[55] Even one's verbal and written acts may be non-testimonial so long as they are used for their physical characteristics and not their substantive content.[56] For example, voice exemplars[57] and handwriting exemplars[58] are non-testimonial because they are used for their physical properties and not what is said.[59]

The difference between a testimonial act and a non-testimonial act is the difference between requiring a defendant to answer an interrogatory and requiring a defendant to provide a handwriting exemplar.[60] Both can incriminate him or her, but with the former, the defendant is required to make use of the "contents of his own mind."[61]

Physical actions may, however, make implicit testimonial communications.[62] The following sections address the question of whether being physically compelled to produce documents is testimonial.

i. The Act of Production Doctrine

The Court has established the "act of production" doctrine in response to the issue of whether the production of a physical object (such as a personal or business paper) is a testimonial act. The lower courts have been applying this "act of production" doctrine to compelled decryption cases, so understanding it is of particular importance.[63] First, I will describe it generally and then discuss the small number of Supreme Court cases applying the doctrine.

The Court has distinguished between the *content* of a paper and the *act* of producing the paper.[64] While the *content* of a paper is certainly testimonial, its creation is voluntary (i.e., it lacks the compulsion element and is therefore not privileged).[65] The *act* of producing a paper is

[55] *Schmerber*, 384 U.S. at 765.

[56] *See Muniz*, 496 U.S. at 597 (physical qualities of speech not testimonial).

[57] United States v. Dionisio, 410 U.S. 1, 5-6 (1973); *see also* United States v. Wade, 388 U.S. 218, 222 (1967) (holding that requiring the accused to speak for identification purposes was non-testimonial).

[58] United States v. Gilbert, 388 U.S. 263, 266-67 (1967).

[59] *See Muniz*, 496 U.S. at 590-92.

[60] *Compare* United States v. Hubbell, 530 U.S. 27, 41 (2000) (stating that requiring a defendant to produce several thousand records was "tantamount to answering a series of interrogatories" and was therefore testimonial), *with Gilbert*, 388 U.S. at 266-67 (stating that a handwriting exemplar, taken for its physical characteristics, was non-testimonial).

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

[62] *See* section II.C.i *infra*.

[63] *See* section III.C *infra*.

[64] *See Hubbell*, 530 U.S. at 36.

[65] *See* United States v. Fisher, 425 U.S. 391, 408-09 (1976); *Doe I*, 465 U.S. 605, 618 (1984) (O'Conner, J., concurring) ("[T]he Fifth Amendment provides absolutely no protection for the contents of private papers of any kind"); *accord Hubbell*, 530 U.S. at 36. *Fisher*, 425 U.S. at 410; Baltimore City

compelled, but whether it is testimonial is a more difficult question.[66]

No bright line rule exists to determine whether the production of a paper is a testimonial act.[67] Instead it depends on the "facts and circumstances" of each case.[68] Whether the production of a paper is testimonial depends on whether that production makes implicit, testimonial communications.[69] Normally, when one produces a paper, one tacitly admits to the government that the paper exists and that one has control over it.[70] These tacit admissions may make the physical production of the paper testimonial.[71]

I say "may" because the government has the opportunity to "rebut" the claim that the production is testimonial.[72] The government may "produce evidence that possession, existence, and authentication [is] a 'foregone conclusion.'"[73] In other words, the accused may claim that he or she is making a testimonial communication, but if the government already knows what the production would implicitly communicate, then the production loses its testimonial quality and becomes a non-testimonial act.[74]

It is worth acknowledging that the exact meaning of "foregone conclusion" has proven an interpretative challenge because the Court has

Dep't of Soc. Servs. v. Bouknight, 493 U.S. 549, 555 (1990) ("[A] person may not claim the Amendment's protections based upon the incrimination that may result from the contents or nature of the thing demanded."). The rule that private papers are not privileged was established first in *United States v. Fisher*, 425 U.S. 391, 411 (1976). In that case, the Court brought the prior precedent of *Boyd v. United States*, 116 U.S. 616 (1886), into question. *See Fisher*, 425 U.S. 408-09. *Boyd* had held that the contents of private papers were privileged because using one's private books and papers was not "substantially different from compelling him to be a witness against himself." *Boyd*, 116 U.S. at 633-35. The Court distinguished *Boyd* by pointing out that the papers were the product of the accountant's efforts and not the accused. The Court, in *Fisher*, left open the question of whether its act of production doctrine would apply to individually produced papers. 425 U.S. at 414; *see also id.* at 421 (Brennan, J., concurring) (urging the Court not to extend *Fisher* to private papers).

[66] *Fisher*, 425 U.S. at 410 (stating that in a compelled production case, the "more difficult" issue is whether production is testimonial).

[67] *Id. Compare id.* (finding the production of records to be non-testimonial after a factual inquiry), *with Doe I*, 465 U.S. 605 (1984) (finding the production of records to be testimonial after a factual inquiry) *and* United States v. Hubbell, 530 U.S. 27 (2000) (finding the production of records to be testimonial after a factual inquiry).

[68] *Fisher*, 425 U.S. at 410.

[69] *Id.*

[70] *See Doe I*, 465 U.S. at 613 n.11 (not showing disagreement with the position that subpoenas to compel production "with few exceptions" have communicative aspects).

[71] *See, e.g.*, *Doe I*, 465 U.S. 605; *Hubbell*, 530 U.S. 27.

[72] *Doe I*, 465 U.S. at 614 n.13.

[73] *Id.* (quoting *Fisher*, 425 U.S. at 411) ("[The defendant] argued that by producing the records, he would tacitly admit their existence and his possession. . . . These allegations were sufficient to establish a valid claim of the privilege against self-incrimination. This is not to say that the Government was foreclosed from rebutting respondent's claim by producing evidence that possession, existence, and authentication were a 'foregone conclusion.'").

[74] *See id.*; *Fisher*, 425 U.S. at 411; *Doe III*, 670 F.3d 1335, 1345-46 (11th Cir. 2012).

failed to define it clearly.[75] Commentators and courts have struggled to conceptualize the doctrine.[76] In addition to the conceptual difficulties, the Supreme Court has not answered the question of how much evidence the government must have before something becomes a "foregone conclusion."[77]

a. *Fisher v. United States*

The act of production doctrine was borne in *United States v. Fisher*. In this case, the defendant, a taxpayer, was facing both civil and criminal liability under federal income tax laws.[78] The taxpayer's tax documents had

[75] Mosteller, *supra* note 6, at 508-09 ("[T]he Supreme Court has never given real definition to [the foregone conclusion] doctrine."); Alito, *supra* note 6, at 49 ("The Court also left substantial doubt about what it meant by 'a foregone conclusion.'"); Lance Cole, *The Fifth Amendment and Compelled Production of Personal Documents After United States v. Hubbell - New Protection for Private Papers?*, 29 AM. J. CRIM. L. 123, 167 (2002) ("[O]n the most difficult and uncertain point—the question of when the foregone conclusion doctrine applies to an act of production of documents—the Court once again declined to provide a definitive answer.").

[76] I will not be addressing this difficult question. For a sampling of the variety of the views on this subject see generally Robert P. Mosteller, *Simplifying Subpoena Law: Taking the Fifth Amendment Seriously*, 73 VA. L. REV. 1, 32 (1987) ("[W]hen an implicit as opposed to an explicit communication is involved, it is necessary to consider whether the government is really asking a 'question' through the subpoena. Granted, the defendant's response to a documentary subpoena always reveals that the item does or does not exist; the government cannot eliminate the implicit question about the document's existence no matter how it phrases the subpoena's demand. But if the government already knows the answer to that question and is truly uninterested in the implicit answer provided by production, the witness' gratuitous communication of it should not violate the Fifth Amendment. In short, the *Fisher* decision suggests that constitutional rights are not violated by implicit communications that are inherent in a response to a documentary subpoena where those communications are unwanted because, though technically admissible, they are not substantially relevant to the prosecution's case given its other evidence.") (footnotes omitted); *Doe III*, 670 F.3d 1335, 1343 n.19 (11th Cir. 2012) (stating that the foregone conclusion doctrine bears a family resemblance to the independent source doctrine from use and derivative-use immunity cases); Michael S. Pardo, *Testimony*, 82 TUL. L. REV. 119, 188 (2007) ("The government's prior knowledge, however, may be relevant to show that it had an independent source for the information and, thus, did not make derivative use of the act of production and will not make use of it at trial."); Ronald J. Allen & M. Kristin Mace, *The Self-Incrimination Clause Explained and Its Future Predicted*, 94 J. CRIM. L. & CRIMINOLOGY 243, 277-89 (2004) (arguing that the foregone conclusion doctrine relates to the cognitive process of the witness and not the knowledge of the government).

[77] *See* sources cited *supra* note 76. Several lower courts have adopted the "reasonable particularity" standard to determine when something is a "foregone conclusion." Under this standard, the government must know with reasonable particularity the location and existence of the documents it subpoenas. *See* United States v. Ponds, 454 F.3d 313, 324 (D.C. Cir. 2006). In *Hubbell*, the lower appellate court, the D.C. Circuit, had adopted the reasonable particularity standard, but the Supreme Court declined to pass judgment on its validity. *See* United States v. Hubbell, 530 U.S. 27, 33, 44 (2000). Regardless, courts in the Second, Ninth, Eleventh, and D.C. Circuits still apply the reasonable particularity standard post-*Hubbell*. *See, e.g.*, *In re* Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d 87, 93 (2d Cir. 1993); *Ponds*, 454 F.3d at 324; *Doe III*, 670 F.3d 1335, 1344 (11th Cir. 2012); *In re* Grand Jury Subpoena, Dated Apr. 18, 2003, 383 F.3d 905, 910 (9th Cir. 2004).

[78] Fisher v. United States, 425 U.S. 393-94 (1976).

been prepared by his accountant, and the taxpayer gave them to his attorney.[79] The government subpoenaed those documents.[80] The taxpayer's attorney asserted the privilege against self-incrimination on his client's behalf.[81]

The Court considered the issue of whether a subpoena to produce the tax records was a testimonial act.[82] It noted that the compelled production of records does not require oral testimony or require the taxpayer to "restate, repeat, or affirm the truth the contents of the documents sought."[83] However, production of the tax records may have *implicit* testimonial qualities.[84] In some cases, production may implicitly communicate that the records exist and are controlled by the taxpayer.[85] Production may also authenticate the documents.[86]

But then the Court turned abruptly from what the defendant may implicitly communicate to what the government *knew* about what is implicitly communicated.[87] The Court found that the government could independently confirm and verify the existence of the taxpayer's records; the taxpayer's accountant had created the records, and the records were the kind that an accountant would normally create.[88] The production would not tell the government anything it did not already know and would not increase the "sum total" of the government's knowledge.[89] Therefore, the Court found that production of the records to be insufficiently testimonial to meet the Fifth Amendment's "testimonial" element.[90]

The *Fisher* analysis was, apparently, part of the Court's jurisprudence all along.[91] The *Fisher* Court said that the "act of production" analysis even applies to things like handwriting exemplars.[92] When one provides a

[79] *Id.*

[80] *Id.* at 394-95.

[81] *Id.* at 395-96. While irrelevant to this discussion, *Fisher* also held that, although the attorney was an "agent" of the taxpayer, under *Couch v. United States*, 409 U.S. 322 (1973), the attorney could not claim the Fifth Amendment privilege on the taxpayer's behalf. *Fisher*, 425 U.S. at 397-98; *see also* cases cited *supra* note 49.

[82] *Fisher*, 425 U.S. at 402-14.

[83] *Id.* at 409; *see also* Curcio v. United States, 354 U.S. 118 (1957) (holding that a grand jury could compel a custodian of records to produce a company's records but not to orally testify as to more records if that testimony could incriminate).

[84] *Id.* at 410-11.

[85] *Id.*

[86] *Id.* at 412-13, 413 n.12; s*ee generally* FED. R. EVID. 901 (Authentication and Identification).

[87] *Fisher*, 425 U.S. at 411-12.

[88] *Id.*

[89] *Id.*

[90] *Id.*

[91] *See id.* at 411-12.

[92] *Id.*; *see* United States v. Gilbert, 388 U.S. 263, 266-67 (1967) (holding that a handwriting

handwriting exemplar, one implicitly admits that one can write and admits that what he or she is providing is his or her handwriting.[93] But the government already knows that people can write; it is a "truism."[94] And the government already knows that the exemplar is someone's handwriting; it is "self-evident."[95] Thus, the things communicated were "foregone conclusions."[96] This would mean that this act of production analysis is at work in more than just cases where one is compelled to produce documents.

b. *United States v. Doe* (*Doe I*)

Eight years later, in *United States v. Doe*[97] (*Doe I*), the Court revisited the act of production doctrine.[98] In this case, the government sought to compel records from the defendant with a grand jury subpoena.[99] The defendant claimed that the content of the records was privileged, and the act of producing the records was privileged.[100] The lower courts sided with the defense on both claims.[101]

On the first point, the Court rejected the claim that the content of the records was privileged.[102] As discussed in section II.B.1, if a record is created voluntarily, it lacks the element of "compulsion."[103] The defendant argued that it should make a difference that the records in his own case were personally created, but in *Fisher*, the taxpayer's accountant had created the records.[104] The Court rejected this as a distinction without a difference and found that both records were created voluntarily.[105]

On the second point however, the Court sided with the defendant.[106] The Court relied on the findings of the lower courts that the production would involve a testimonial communication.[107] It also sided with the lower courts' finding that the government had no knowledge of whether the

exemplar is non-testimonial).

[93] *Gilbert*, 388 U.S. 263, 266-67.

[94] *Id.*

[95] *Id.*

[96] *Id.*

[97] 465 U.S. 605 (1984).

[98] *Id.*

[99] *Id.* at 606-07.

[100] *Id.* at 608.

[101] *Id.*

[102] *Id.* at 612.

[103] *See id.* 611-12.

[104] *Id.* at 608.

[105] *Id.* at 611-12.

[106] *Id.* at 617.

[107] *See id.* 613-14, 613 n.11.

compelled documents existed and were in the defendant's control.[108]

The Court, in dicta, helped to clarify the somewhat perplexing act of production doctrine from *Fisher*.[109] This dictum provides a framework for the act of production and foregone conclusion analyses.[110] First the one seeking to claim the privilege must show that the compelled production has implicit testimonial qualities.[111] Then, the burden shifts to the government to rebut the claim of privilege.[112] To "rebut" this privilege, the government must produce evidence that the testimonial qualities implicitly communicated are already a foregone conclusion and therefore non-testimonial.[113]

c. *Doe v. United Stat*es (*Doe II*)

Four years after *Doe I*, the Court decided another case, *Doe v. United States*[114] (*Doe II*), again addressing the act of production doctrine.[115] As part of a grand jury investigation, the government sought records in the possession of foreign banks.[116] The government could not access those records without the defendant's assistance.[117] It needed the defendant to execute a directive to release the foreign bank records and compelled him to do so with a grand jury subpoena.[118] The directive was carefully written as to not make reference to a specific account, to a specific bank, to the existence of an account, or to an account owned by the defendant.[119] Thus signing the directive did not require the defendant to admit anything.[120] The defendant refused to sign the directive on self-incrimination grounds.[121] The Court rejected the defendant's claim and found that it was not sufficiently

[108] *Id.* at 613-14.

[109] *See id.* at 613 n.11.

[110] *See id.*

[111] The Court, although it did not explicitly show agreement with the district court, did not express disagreement with the lower court's statement that "[w]ith few exceptions enforcement of the subpoenas would compel [respondent] to admit that the records exist, that they are in his possession, and that they are authentic." *Id.* at 613 n.11 (second alteration in original) (internal quotation marks omitted). This seems to show that this initial burden is easily met in most cases.

[112] *Id.*

[113] *Id.* The Court did not say what evidentiary standard the government would need to meet. *See id.*

[114] 487 U.S. 201 (1988).

[115] *Id.*

[116] *Id.* at 202-03.

[117] *Id.* at 203-04.

[118] *Id.*

[119] *Id.* at 204-05, 215.

[120] *Id.*

[121] *Id.* at 204.

testimonial.[122]

The Court reaffirmed *Fisher*, saying that "an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information."[123] The execution would not assert or disclose any information itself.[124] Instead, it would just open up "a potential source of evidence."[125] Thus, compelled execution of the directive would be more like a handwriting or voice exemplar because it lacked testimonial significance.[126]

Significantly, unlike either *Doe I* or *Fisher*, the Court did not require the government to know what the directive would produce.[127] The Court looked narrowly to whether signing the directive would require the defendant to "make a statement."[128] The directive made no statement as to whether evidence existed, and it did not "point the Government towards hidden accounts or otherwise provide information that will assist the prosecution in uncovering evidence."[129] Therefore, while incriminating, the directive was not testimonial.[130] Consequently, the defendant could not claim the privilege against self-incrimination.[131]

d. *United States v. Hubbell*

The last time the Court addressed the act of production doctrine was in *United States v. Hubbell*.[132] Here, the defendant had entered into a plea bargain where he would provide the government with information relating to an ongoing investigation.[133] The prosecutor served the defendant with a subpoena calling for the production of eleven categories of documents.[134] The defendant then invoked his Fifth Amendment Privilege.[135] In response, pursuant to 18 U.S.C. § 6002,[136] the prosecution provided the defendant

[122] *Id.* at 219.

[123] *Id.* at 210.

[124] *Id.*

[125] *Id.* at 215.

[126] *Id.*

[127] *See* 215-16.

[128] *Id.*

[129] *Id.* at 217.

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

[131] *Id.*

[132] See United States v. Hubbell, 530 U.S. 27 (2000).

[133] *Id.* at 30.

[134] *Id.* at 31.

[135] *Id.*

[136] 18 U.S.C. § 6002 (1994).

> Whenever a witness refuses, on the basis of his privilege against self-incrimination, to testify or provide other information in a proceeding before or ancillary to
>
> (1) a court or grand jury of the United States,
>
> (2) an agency of the United States, or

with immunity for the production of the papers.[137] The defendant then produced 13,120 documents.[138] These documents led to a prosecution, despite the grant of immunity.[139] The Supreme Court ultimately dismissed the indictment because 18 U.S.C. § 6002 immunized the defendant from future prosecutions.[140]

The government argued that it did not need to offer immunity in the first place because the production was insufficiently testimonial.[141] The Court rejected this however, saying that the production of the 13,120 documents "was tantamount to answering a series of interrogatories asking the witness to disclose the existence and location of particular documents fitting certain broad descriptions."[142]

The government then argued that the production of the documents was insufficiently testimonial because the defendant's control over the documents was a foregone conclusion.[143] The Court rejected this argument because prior to the defendant's production of the documents, the government did not have "any prior knowledge" that the documents existed. Because the facts of this case were so unfavorable to the government, the court failed to explain what it meant by "foregone conclusion," except that "whatever the scope of this 'foregone conclusion' rationale, the facts of this

> (3) either House of Congress, a joint committee of the two Houses, or a committee or a subcommittee of either House,
>
> and the person presiding over the proceeding communicates to the witness an order issued under this title, the witness may not refuse to comply with the order on the basis of his privilege against self-incrimination; but no testimony or other information compelled under the order (or any information directly or indirectly derived from such testimony or other information) may be used against the witness in any criminal case, except a prosecution for perjury, giving a false statement, or otherwise failing to comply with the order.

[137] *Hubbell*, 530 U.S. at 31.

[138] *Id.*

[139] *Id.*

[140] *Id.* at 46. In *Kastigar*, the Court interpreted this grant of immunity to be co-extensive with the privilege against self-incrimination such that the government cannot use either the testimony or the derivatives of the testimony in a future criminal action. Kastigar v. United States, 406 U.S 441, 453 (1972). The only permissible way that the government could successfully prosecute subsequent to granting immunity is if it is based on information independent of the immunized testimony. *Id.* at 460-61. 18 U.S.C. § 6002 does granted not total immunity to all subsequent prosecutions (i.e., "transactional immunity"). *Id.* at 462. Rather, once immunity has been granted, the burden shifts to the prosecution to show that proposed evidence comes from an independent source. *Id.* at 461-62. In *Hubbell*, the documents themselves were not going to be used against the defendant, they were the "first step in a chain of evidence" leading to the indictment. *Hubbell*, 530 U.S. at 42. Thus the government had made derivational use of the documents and could not show that it had attained the information necessary for these second prosecutions from an independent source. *Id.* at 45-46.

[141] *Id.* at 44.

[142] *Id.* at 41.

[143] *Id.* at 44.

case plainly fall outside of it."[144]

C. Encryption Case Law

Few courts have thus far had the opportunity to address whether the compelled decryption of an electronic device is testimonial.[145] The courts that have addressed the problem have made use of the act of production doctrine discussed in II.B.3. These "compelled production" cases are factually distinct from one another and so this Comment will briefly discuss the factual and procedural circumstances of the cases and how they have applied the act of production doctrine to compelled decryption.

1. *In re Boucher*

In re Boucher[146] was one of the first encryption cases. On December 17, 2006, the defendant passed through a routine border checkpoint and an Immigration and Customs Enforcement (ICE) agent searched his vehicle.[147] Within the vehicle, the ICE agent found a laptop computer.[148] He opened it to discover several thousand images, some of which were pornographic.[149] Among the prodigious amount of pornography, he found a file titled "2yo getting raped during diaper change." He was unable to open it.[150] However, he could see that the file had been opened in the past month.[151]

A second ICE agent was then called in, this one an expert in child pornography.[152] He read the defendant his *Miranda* rights, which were waived.[153] The defendant told the agent that he downloaded a lot of

[144] *Id.*; *see also Doe I*, 465 U.S. 605, 613-14 (1984) (holding that the defendant's possession and control of records was not a foregone conclusion but neglecting to further define the doctrine). Engaging in a bit of speculation as to what went in chambers on this point, Justice Stevens wrote both the dissent in *Doe II* and the majority opinion in *Hubbell*. Justice Stevens all but ignores *Doe II* (aside from his dissent), favoring *Doe I* and *Fisher*. Appearing to be no fan of the foregone conclusion doctrine, he dismisses the foregone conclusion saying "*this* 'foregone conclusion' rationale" with foregone conclusion in scare quotes. *See Hubbell*, 530 U.S. at 44. Whether this marks a sign that a future Court would abandon the foregone conclusion approach is worth considering. Also worth considering is the fact that Justices Scalia and Thomas would abandon the entire act of production analysis in favor of a rule saying that the accused should *never* need to assist the government in one's own prosecution. *See id.*, at 49-54. But these considerations are outside the scope of this Comment.

[145] *See* cases sited *supra* note 1.

[146] No. 2:06-mj-91, 2007 WL 4246473 (D. Vt. Nov. 29, 2007).

[147] *Id.* at *1. *See generally* United States v. Ramsey, 431 U.S. 606, 616 (1977) (establishing the border search exception to probable cause).

[148] *Boucher*, 2007 WL 4246473, at *1.

[149] *Id.*

[150] *Id.*

[151] *Id.*

[152] *Id.*

[153] *Id. See generally* cases cited *supra* note 31.

pornography, and occasionally, would mistakenly download child pornography, but he would delete it upon discovery.[154] The agent then asked the defendant to show him the pornography.[155] The defendant complied and entered in a password into his "drive Z"—the agent did not see what the password was.[156] The agent looked through the computer and a found a video titled "preteen bondage," which appeared to depict an underage girl.[157] After finding even more child pornography, the defendant was then arrested and the computer was powered down.[158]

When the computer was powered back on, law enforcement found it encrypted using PGP encryption software.[159] The software made the disk unreadable despite a Secret Service forensics expert's best efforts.[160] It could take years to decrypt.[161]

The government then subpoenaed the defendant to hand over all documents that reflected the password to the laptop.[162] The court did not address the demand for papers because the government refined its request at a hearing and demanded that the defendant enter the password himself.[163] The government promised not to use the defendant's act of entering in the password against him.[164]

The magistrate first determined that the act of entering in the password would be testimonial.[165] The act of entering in the password would communicate both the contents of the defendant's mind and that he had access to the device.[166] It did not matter to the court that the government had promised not to look at the password because the defendant would still implicitly communicate that he knew the password regardless of whether the government learned the actual password.[167]

The magistrate concluded that the government did not meet its burden

[154] *Boucher*, 2007 WL 4246473, at *1.

[155] *Id.*

[156] *Id.*

[157] *Id.* at *2.

[158] *Id.*

[159] *Id.* For more information on the software used in this case, *see generally Encryption Family*, SYMANTEC, http://www.symantec.com/encryption (last visited Mar. 3, 2014).

[160] *Boucher*, 2007 WL 4246473, at *2.

[161] *Id.*

[162] *Id.*

[163] *Id.* The flaws in this request are obvious under *Hubbell*, 530 U.S. 26 (2000). The government had no idea if any papers existed; therefore production of the papers would implicitly communicate the existence of such papers—a testimonial act.

[164] *Id.*

[165] *Id.* at *3-4.

[166] *Id.*

[167] *Id.*

under the foregone conclusion doctrine.[168] The court interpreted the government's requests as either for the password itself or for the production of the files from drive Z.[169] A request for the password itself would be a request for something purely communicative and so the act of production doctrine would not apply.[170] The request for the files from drive Z would fail because the government only knew of some of the device's files and did not know the entire contents of the device.[171] Therefore, decryption would increase the "sum total" of the government's knowledge.

In *In re Boucher*[172] (*Boucher II*), the government appealed the magistrate's order to the district court judge.[173] This time, the government had refined its request to just be for the unencrypted version of "drive z."[174] The district court found that the government's knowledge of the drive's existence, the defendant's control of the drive, and the drive's authenticity was a foregone conclusion.[175] Therefore, the decryption of the device could be compelled.[176] The district court disposed of the magistrate's argument, saying that the government did not need to know of the incriminating contents of the files.[177]

2. *United States v. Fricosu*

United States v. Fricosu,[178] a case from the District of Colorado, also resulted in the defendant being compelled to decrypt because of the foregone conclusion doctrine.[179] In this case, the prosecution sought files contained in an encrypted laptop computer, which resisted FBI attempts at decryption.[180] The prosecution petitioned the court for a writ compelling the

[168] *Id.* at *5-6.

[169] *Id.* at *6.

[170] *Id.*; *see also* United States v. Kirschner, 823 F. Supp. 2d 665, 668-69 (E.D. Mich. 2010) (holding that the government could not compel the defendant to communicate the password of an encrypted device because it was not a physical production).

[171] *Boucher*, 2007 WL 4246473 at *1.

[172] No: 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

[173] *Id.*

[174] *Id.* at *2.

[175] *Id.* at *4.

[176] *Id.*

[177] *Id.* at *3. On this point the *Boucher II* court relied on the controlling Second Circuit precedent of *In re Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992*, 1 F.3d 87 (2d Cir. 1993), which held that the government was not required to know the contents of an allegedly altered calendar when it could state with reasonable particularity the existence and location of the calendar. *In re Jury Subpoena*, 1 F.3d at 93. Thus, the Court stated that the government was not required to know the content of individual files so long as it could show that the files existed. *Boucher*, 2009 WL 424718, at *3.

[178] 841 F. Supp. 2d 1232 (D. Colo. 2012).

[179] *Id.* at 1237-38.

[180] *Id.* at 1234.

defendant to decrypt the computer and assist with the execution of the warrant.[181]

The district court considered two issues.[182] The first was whether the government knew of the existence and location of the computer's files.[183] The court relied in large part on the *Boucher II* court's analysis to find that the government did not need to be able to know specific content of the files; knowing the "existence and location" of the computer's files was sufficient.[184]

The second issue was whether the government could show that the defendant could access the computer.[185] On this point the court found: "[T]he government has met its burden to show by a preponderance of the evidence that the [device] belongs to [the defendant], or, in the alternative, that she was its sole or primary user, who, in any event, can access the encrypted contents of that laptop computer."[186] The court relied on the following facts: (1) the computer had been seized from the defendant's room; (2) the computer was named "RS.WORKGROUP.Romana" (Romana being the defendant's first name); and (3) the agents had recorded a conversation between the defendant and her husband where the defendant admitted to owning and being able to access the laptop.[187] Therefore, the court found that the compelled decryption of the laptop did not violate the Fifth Amendment.

[181] *Fricosu*, 841 F. Supp. 2d at 1235. *See generally* 28 U.S.C. § 1651 (1949).

> (a) The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.
>
> (b) An alternative writ or rule nisi may be issued by a justice or judge of a court which has jurisdiction.

[182] *See Fricosu*, 841 F. Supp. 2d at 1237.

[183] *Id.*

[184] *Id.*

[185] *Id.*

[186] *Id.* In my research, the *Fricosu* court is the only court to identify a preponderance of the evidence standard as the burden the government must meet before it may compel decryption. The *Fricosu* court does not cite any authority in stating that the government must meet this burden. No other court has addressed or accepted this standard of proof requirement. However, as the Eleventh Circuit has noted, the foregone conclusion doctrine bears a resemblance to the independent source doctrine from *Kastigar*. *See Doe III*, 670 F.3d 1335, 1343 n.19 (11th Cir. 2012); *see also supra* notes 135, 138. Several courts have applied a preponderance of the evidence standard to the question of whether the discovery of evidence following a grant of immunity stems from an independent source. *See, e.g.*, *In re* Grand Jury Proceedings, 9 F.3d 1389, 1390 (9th Cir. 1993); *cf.* Nix v. Williams, 467 U.S. 431 (1984) (applying a preponderance of the evidence standard to the independent source exception to the exclusionary rule). So perhaps that is where the evidentiary standard in *Fricosu* comes from.

[187] *See Fricosu*, 841 F. Supp. 2d at 1237.

3. *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011* (*Doe III*)

In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011[188] (*Doe III*) stands as the only circuit court case to consider the issue of compelled decryption, and the only case, in any jurisdiction, where the defendant was not compelled to decrypt. This Eleventh Circuit case has also provided the most detailed analysis of the act of production doctrine's application to encryption.[189]

In 2010, the FBI investigated a YouTube.com account suspected of sharing child pornography.[190] The user of the account accessed the account from three different internet protocol addresses (IP address). The FBI linked these addresses to three different hotels.[191] The only common individual staying in the hotels during the relevant times was the defendant.[192] The FBI executed a search warrant and seized two laptops and five external hard drives.[193] However, the hard drives had been encrypted using TruCrypt's Hidden Volume software.[194] One of the features of the Hidden Volume software is that it prevents one from determining whether an encrypted device is empty or full.[195] The device could be either full of information or completely empty (aside from the encryption) and no one could know the difference.[196]

The government sought to subpoena the decryption of a device that it suspected had child pornography on it.[197] The defendant refused and claimed his privilege against self-incrimination.[198] The prosecution then

[188] 670 F.3d 1335 (11th Cir. 2012).

[189] This case also misreads the act of production cases. *See* section III.

[190] *Doe III*, 670 F.3d at 1339.

[191] *Id.*

[192] *Id.*

[193] *Id.*

[194] *Id. See generally Hidden Volume*, TRUECRYPT, http*://www.truecrypt.org/docs/hidden-volume* (last visited Mar., 25, 2014) ("It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.") (footnotes omitted).

[195] *Id.* The TrueCrypt hidden volume basically allows the user to create a "Russian nesting doll" of encryption. *See id.* ("[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.") (footnotes omitted). The software encrypts a volume, resulting it that volume appearing to be random information. *Id.* Then a sub-part of the encrypted drive is encrypted again, but because the volumes appear to just be random data, despite the number of times it has been encrypted, it is difficult to impossible to determine whether the sub-drive is full or empty. *Id.*

[196] *Id.*; *see also Doe III*, 670 F.3d at 1340 (discussing TrueCrypt software).

[197] *Id.* at 1339.

[198] *Id.*

offered use immunity[199] for the act of decryption but not for the derivational evidence.[200] The defendant again refused, claiming that use immunity would be insufficient to protect him from incriminating himself.[201] The Eleventh Circuit agreed with the defendant and held that the defendant's act of decryption was testimonial and the grant of use immunity was insufficient to immunize the defendant's action.[202]

The Eleventh Circuit first provided a broad overview of the Supreme Court's act of production doctrine.[203] It identified that an act is non-testimonial if either the compulsion is merely with regard to a physical act and is non-communicative or the compulsion is communicative but this communication is a foregone conclusion.[204]

The court held first that decryption was a testimonial act.[205] Decryption would require the defendant to admit that he knew the files existed and knew the location of the files.[206] Decryption would also require him to admit to possessing the files, controlling the files, being able to access the files, and being able to decrypt the device.[207]

The court then turned to whether the implicit testimony was a foregone conclusion.[208] On this point, the court put heavy emphasis on the government's expert whom, during a hearing, was unable to say whether the encrypted device actually had anything on it.[209] The most he could say was that the device *could* have files on it, but TrueCrypt's Hidden Volume functionality prevented one from determining whether a device was full or empty.[210]

The court held that the foregone conclusion rationale was inapplicable because the government could not show that it knew any files even existed

[199] For a general description of immunity, see generally *supra* notes 135, 138 and accompanying text. Use immunity is distinct from use and derivational use immunity. *See Doe* III, 670 F.3d at 1338. Use immunity is not coextensive with the Fifth Amendment, *id.* at 1350, while derivational use immunity is coextensive with the Fifth Amendment Privilege, s*ee* Kastigar v. United States, 406 U.S. 441, 462 (1972).

[200] *Doe III*, 670 F.3d at 1338.

[201] *Id.*

[202] *Id.* at 1341.

[203] *Id.* at 1341-46.

[204] *Id.* at 1346.

[205] *Id.*; *see also id.* at 1341 n.13 ("If the decryption of the hard drives would not constitute testimony, one must ask, 'Why did the Government seek, and the district court grant, immunity for Doe's decryption?' The answer is obvious: Doe's decryption would be testimonial.").

[206] *Id.* at 1346.

[207] *Id.*

[208] *Id.*

[209] *Id.* at 1340, 1345.

[210] *Id.*; *see supra* note 195 and accompanying text.

(let alone where they were located).[211] The government argued that the files *could* exist, but the court dismissed the argument stating that "the Government physically possesses the media devices, but it does not know what, if anything, is held on the encrypted drives."[212] Nor could the government show that it knew within any degree of certainty that the defendant *could* decrypt.[213] Thus, the court reasoned, the case was like *Hubbell* and unlike *Fisher* because the government lacked knowledge of the encrypted files.[214]

The Eleventh Circuit distinguished, but did not show disagreement with, both *Boucher II* and *Fricosu*. In those cases, unlike this one, the prosecution at least had information that *something* was on the computer.[215] The Eleventh Circuit seemed to agree with the other courts that the government did not need to go so far as to show knowledge of the specific content of other devices.[216] But the government at least needed to know that *something* existed on the drive.[217] Specifically, the government would need to be able to show that a file did exist, either because it knew the account's name or because it knew "that (1) the file existed in some specific location, (2) the file is possessed by the target of the subpoena, and (3) the file is authentic."[218]

4. *In re Decryption of a Seized Storage System* (*Feldman*)

In *In re Decryption of a Seized Storage System*[219] (*Feldman*), the prosecution sought to compel the decryption of several external hard drives seized during a search of the defendant's home.[220] The government believed the devices seized contained child pornography, and the forensic examiners were able to determine that they had transferred over 1,000 files over the file sharing network E-mule.[221] Most of the file names implicated child pornography.[222]

The magistrate adopted the standards set by the other courts, and

[211] *Doe III,* 670 F.3d at 1347-49.

[212] *Id.*

[213] *Id.* at 1346 ("[N]othing in the record illustrates that the Government knows with reasonable particularity that Doe is even capable of accessing the encrypted portions of the drives.").

[214] *Id.* at 1347.

[215] *Id.* at 1348, 1349 n.27.

[216] *Id.* at 1348.

[217] *Id.*

[218] *Id.* at 1349 n.28.

[219] 2:13-mj-00449, 2013 BL 153162 (E.D. Wis. Apr., 19 2013), *available at* http://ia601700.us.archive.org/6/items/gov.uscourts.wied.63043/gov.uscourts.wied.63043.3.0.pdf.

[220] *Id.* at *1.

[221] *Id.*

[222] *Id.*

looked, first, to determine whether the government knew the device had content, and, second, whether the defendant could access the device.[223] On this first point, the court, distinguishing *Doe III*, found that it was a foregone conclusion that the device had contents and that the contents were child pornography.[224] On the second point however, the court concluded that the government could not show that the defendant was able to decrypt the device and thus held the government could not compel decryption.[225]

On reconsideration however, the government was able to present more evidence that the defendant was able to access the device.[226] This evidence was in a somewhat similar form as the evidence the court considered in *Fricosu* and included circumstantial evidence linking the defendant to the device, thus increasing the likelihood that the defendant could decrypt.[227]

The court then ordered decryption.[228] Litigation on this issue abruptly ceased however when the prosecution was able to fully decrypt the defendant's computer, finding over four hundred thousand pictures and videos of child pornography.[229]

III. Analysis

The current collection of compelled decryption cases have some general similarities. Almost every major court case has turned on the issue of whether the foregone conclusion doctrine applies.[230] In other words, in these cases, the accused met his or her initial burden of showing that decryption was a testimonial act, and the government has sought to show that the implicit communications were a foregone conclusion.[231]

[223] *Id.* at *4.

[224] *Id.*

[225] *Id.* at *5.

[226] *Feldman II*, 2013 BL 153162 (E.D. Wis. May 21, 2013), *available at* http://www.courthousenews.com/2013/05/31/decryptorder.pdf.

[227] *Id.* at *2 ("d. In addition to numerous files of child pornography, the decrypted part of Feldman's storage system contains detailed personal financial records and documents belonging to [the defendant]. e. The decrypted part of [the defendant's] storage system contains dozens of personal photographs of [the defendant]. . . . [T]he defendant] is a competent software developer who could have learned how to use encryption.") The court did not say it was applying a preponderance of the evidence standard to the question of whether the defendant could decrypt. *See id.* The court did not say what evidentiary standard it was applying at all. *See id.*

[228] *Id.*

[229] *See* Motion to Dismiss Application, at 1-2, United States v. Decryption of a Seized Data Storage System (2:13-mj-00449), *available at* http://www.bloomberglaw.com/document/X1Q6MM164J82.

[230] *See, e.g.*, *In re* Boucher, No. 2:06-mj-91, 2008 WL 424718, at *3 (D. Vt. 2009); United States v. Fricosu, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012); *Doe III*, 670 F.3d 1335, 1347-49 (11th Cir. 2012); *Feldman II*, 2:13-mj-00449, 2013 BL 153162, at *2 (E.D. Wis. May 21, 2013).

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

Not enough care and attention has been paid to *what* is testimonial about decryption—i.e., what decryption implicitly communicates. Courts have said that decryption communicates that data is located on an encrypted device exist and that the accused controls it.[232] This assumption misreads the act of production line of cases and fails to take into account the seemingly obvious fact that decryption and the physical production of documents are different actions. Different actions will implicitly communicate different things.

First, I will argue that decryption communicates that a witness can access a device. Second, I will argue that decryption does not communicate the existence of a device's contents or accused's control over of those contents. Therefore, to compel decryption, it must be a foregone conclusion that a witness is able to access a device. However, neither existence nor control needs to be a foregone conclusion.

A. Decryption Communicates that One Has Access to an Encrypted Device

Decrypting a device necessarily requires one enter a correct password.[233] Thus if the government seizes an encrypted device, compels the accused to decrypt the device, and the accused does so, it necessarily means that the accused knows the password and has access to the device.[234] This should be enough to establish that decryption is testimonial.

Boucher I, *Doe III*, and *Feldman* explicitly acknowledged that decryption communicates one's ability to access a device.[235] This is a unique feature of encryption and inapplicable to more "traditional" act of production doctrine cases.[236] But this divergence is proper. Physically producing documents requires a different action than entering a password

[232] *See In re* Boucher, No: 2:08-mj-91, 2007 WL 4246473, *5 (D. Va. Nov. 29 2007); *Boucher*, 2009 WL 424718, at *3; *Doe III*, 670 F.3d at 1346. The court in *Fricosu* did not explicitly say that decryption had testimonial qualities but instead jumped to the foregone conclusion analysis. *Fricosu*, 841 F. Supp. 2d at 1237. During its foregone conclusion analysis, it noted that existence and control were both foregone conclusions so the court at least assumed that decryption presumptively communicated these qualities. *Id.*; *see also id.* at 1236 (discussing *Boucher* and the court's analysis there).

[233] *See generally* section II.A *supra*.

[234] For the purposes of clarity, the general noun used for the one the government is attempting to compel will either be the witness, the defendant, or the accused. This is not to indicate that anyone compelled to decrypt is *necessarily* filling one of those roles.

[235] *See In re* Boucher, No. 2:06-mj-91, 2007 WL 4246473, at *4 (D. Va. Nov. 19, 2007); *Doe III*, 670 F.3d at 1349; *Feldman II*, 2013 BL 153162, at *2 (E.D. Wis. May 21, 2013). *Fricosu* implicitly assumed it because it held that the defendant's ability access the devices was a foregone conclusion. *Fricosu*, 841 F. Supp. 2d at 1237. *Boucher II* did not conduct a foregone conclusion analysis or say whether decryption implicitly communicates an ability to access a device. *See Boucher*, 2009 WL 424718, at *3-4. But because a government agent had already watched the defendant enter the password in that case, the court most likely thought it a non-issue.

[236] *See* discussion *supra* part II.C.i-v.

into a computer—different actions will have different implicit communications.[237] For example, in *Hubbell* the government sought to compel the defendant to physically assemble thousands of documents.[238] In comparison, in *Doe II*, the government sought to compel the defendant to execute a directive that would provide the government *access* to potential evidence.[239] In *Hubbell*, the defendant communicated that the documents existed, were controlled by him, and were authentic.[240] In *Doe II*, all the defendant communicated was an ability to write.[241] While the end result remained the same, the government got access to incriminating documents, the defendants' actions differed significantly and thus made different implicit communications.

This is not to say that because the act of decryption has fundamental differences from the act of production that courts should not apply the *Fisher* line of cases. Instead, courts should embrace the differences between decryption and production and acknowledge these differences in their analysis.

B. Before the Government May Compel Decryption, the Defendant's Ability to Access the Device Must Be a Foregone Conclusion

Simply because a witness is able to meet his or her initial burden of showing that the act of decryption is testimonial does not mean the analysis is over.[242] The next step is to consider whether the government can produce sufficient evidence to show the defendant's ability to decrypt is a forgone conclusion.[243] If the defendant's ability to decrypt is a foregone conclusion, then the defendant would "add little or nothing to the sum total of the government's information by conceding" to the fact that the defendant can

[237] *Compare* Hubbell v. United States, 530 U.S. 27, 43 (2000) (quoting Curcio v. United States, 354 U.S. 118, 128 (1957)) ("It 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 request in the subpoena.") *with Doe II*, 487 U.S. 201, 217 (1988) ("[D]irecting the recipient of a communication to do something is not an assertion of fact or, at least in this context, a disclosure of information. In its testimonial significance, the execution of such a directive is analogous to the production of a handwriting sample or voice exemplar: it is a non-testimonial act.").

[238] *Hubbell*, 530 U.S. at 43.

[239] *Doe II*, 487 U.S. at 204-06.

[240] *Hubbell*, 530 U.S. at 45.

[241] *See Doe II*, 487 U.S. at 217 (describing the execution like a handwriting exemplar); *see also* Fisher v. United States, 425 U.S. 391, 411 (1976) (saying a handwriting exemplar communicates one's ability to write).

[242] *See* Fisher, 425 U.S. at 410-11; *Doe I*, 465 U.S. 605, 614 n.13 (1984); *Doe III*, 670 F.3d 1335, 1343 n.19 (11th Cir. 2012).

[243] *See Doe III*, 670 F.3d at 1343 n.19; *Feldman II*, 2:13-mj-00449, 2013 BL 153162, at *2 (E.D. Wis. May 21, 2013); *accord Doe I*, 465 U.S. at 614 n.13.

decrypt.[244]

Courts addressing this issue, in one way or another, have considered whether the defendant's ability to access an encrypted device is a foregone conclusion.[245] The clearest example of a defendant's ability to decrypt being a foregone conclusion is *Boucher* where a government agent watched the defendant decrypt his computer once before.[246] In comparison, in *Doe III*, the government put forward no evidence that the defendant was able to decrypt.[247] *Fricosu* and *Feldman* present an interesting middle ground where the courts' decisions were based on circumstantial evidence.[248]

Once the government shows that the accused's ability to decrypt is a foregone conclusion, then "no constitutional rights are touched."[249] However, courts have also said that the content and control of a device must also be a foregone conclusion. But, as I will argue, decryption does not communicate content and control and so requiring these things to be a foregone conclusion is erroneous.

C. Decryption Does Not Communicate the Existence of a Device's Contents

Along with requiring the government to know that the witness can decrypt, every court has required that the government be able to know that the device contains information.[250] However, decryption communicates

[244] *Id.*

[245] *See In re* Boucher, No. 2:06-mj-91, 2007 WL 4246473, at *5-6 (D. Va. Nov. 29 2007); *In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *3-5 (D. Va. Feb. 19 2007); United States v. Fricosu, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012); *Doe III*, 670 F.3d 1346-47; *Feldman II*, 2013 BL 153162, at *2.

[246] *Boucher*, 2009 WL 424718, at *3.

[247] *Doe III*, 670 F.3d at 1346.

[248] *Fricosu*, 841 F. Supp. 2d at 1236; *Feldman II*, 2013 BL 153162, at *2. The *Fricosu* court adopted an evidentiary standard where the government must show by a preponderance of the evidence that the defendant is able to decrypt. *Fricosu*, 841 F. Supp. 2d at 1236. The *Feldman* court did not follow this evidentiary standard expressly; it did not say what evidentiary standard it was applying. *Feldman II*, 2013 BL 153162, at *2. This Comment is consciously avoiding the question of how much knowledge the government must have before something becomes a foregone conclusion. However, I am concerned that a "preponderance of the evidence" standard could result in injustice. There is a possibility that one could be compelled to decrypt a device that one does not have access to. For instance, if there are multiple users to a device, one user could have an inability to access a particular area or volume of a device. *See Doe III*, 670 F.3d at 1340 n.9 ("[T]here was no evidence that [the defendant] was the only person who had access to his hard drives."). Holding that person in contempt for being unable to do the impossible would result in a serious injustice. Courts should consider adopting a "clear and convincing" evidence standard instead. *See* Aaron M. Clemens, comment, *No Computer Exception to the Constitution: The Fifth Amendment Protects Against Compelled Production of an Encrypted Document or Private Key*, 2004 UCLA J.L. & TECH. 2 (2004).

[249] *See* Fisher v. United States, 425 U.S. 391, 411 (1976); *Doe III*, 670 F.3d at 1346.

[250] *See* cases cited *supra* note 224. Despite *Doe III* being the only case where the court upheld the defendant's claim of privilege against self-incrimination, courts are not necessarily split on the issue. *See*

nothing about the device's contents. If there are no communications as to the contents of a device, the government should not need to know about it.

Decryption is different than physically producing documents. This is perhaps an obvious point—but an important one nonetheless—because different actions will implicitly communicate different things. Entering in a password to decrypt will implicitly communicate something different from physically going out and searching for documents and producing them in response to a subpoena.

This premise is rooted in the Supreme Court's cases.[251] In *Hubbell* and *Fisher*, the Court indicated that production of documents implicitly communicates that the documents existed and the accused controlled the documents.[252] Importantly though, it was the means by which the accused would produce the documents that communicated existence and control.[253] The Court in *Hubbell* put great weight on the fact that the accused would have had to "make extensive use 'of the contents of his own mind' in identifying the hundreds of documents responsive to the request in the subpoena."[254] The "assembly" of the documents resulted in the act being testimonial.[255] Conversely, in *Doe II*, the accused did not need to go out and assemble any documents—he just executed a directive—and so the accused did not implicitly communicate existence and control of the documents to the government.[256]

Decryption is more like executing a release for foreign bank records than the assembly of documents.[257] In both executing a release and decryption, the accused is not required to use the contents of his mind to

Feldman I, No. 2:13-mj-00449-WEC, 2013 BL 116993, *3 (E.D. Wis. Apr. 19, 2013). Whether an act is testimonial depends on the "facts and circumstances of particular cases." *Fisher*, 425 U.S. at 410. At least on this point, the legal rule has not differed significantly between courts, instead the "facts and circumstances" have differed. It is, for example, altogether possible that courts in the Eleventh Circuit would permit compelled decryption should a case be factually similar to *Boucher* or *Fricosu*. *See Doe III*, 670 F.3d at 1348-49 (distinguishing *Boucher* and *Fricosu* and adopting a similar rule as those cases in dicta).

[251] *See Doe II*, 487 U.S. 201, 219 (1988) (Stevens, J., dissenting) ("The forced execution of this document differs from the forced production of physical evidence just as human beings differ from other animals.").

[252] United States v. Hubbell, 530 U.S. 27, 43 (2000).

[253] *Id.*

[254] *Id.*

[255] *Id.* ("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.") (emphasis added); *see also* Cole, *supra* note 75, at 182 ("The Court concluded that the mental efforts required by a witness *to assemble and produce* subpoenaed documents was like testifying to the combination to a wall safe . . . .").

[256] *Doe II*, 487 U.S. at 215.

[257] *See id.*; *see also* Philip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171, 204 (1997) (noting an analogy between decryption and executing a directive).

assemble anything.[258] Also in both cases, the accused does some physical act to give the government *access* to the information.[259] The accused in no way "points" the government to incriminating information but allows the government to use "the independent labor of its officers" to conduct the investigation.[260] The government, after compelling the accused to decrypt, does not force the accused to go through huge amounts of data and identify incriminating evidence—that would bring it much more in line with *Hubbell*.

Consider the following. Decryption generally requires one to enter a password into a device to make it readable.[261] However, technology is also available which allows one to lock a device biometrically (e.g., fingerprint locking).[262] If the government sought to compel decryption of a biometrically locked device, it could do so without implicating the Fifth Amendment.[263] Decryption using a biometric lock would involve a purely physical act, no different really than compelling someone to provide a blood sample or stand in a line up for identification.[264] In other words, it would be a non-testimonial act.[265] It would no more communicate what was within an encrypted device than providing a DNA sample would communicate a DNA sequence.[266]

If a court would find that using a biometrical lock does not implicitly communicate the contents of a device, then it should also find that entering a password does not implicitly communicate the contents of a device. In neither case is the accused required to identify or collect evidence against

[258] *See* Reitinger, *supra* note 257, at 177-78 ("[E]ncryption is far more like storing a document on a computer or locking it in a safe than translating it. . . . Encryption . . . is a purely mechanistic process that does not of necessity add, subtract, or alter information . . . .") (footnotes omitted).

[259] *Id.*

[260] *See Doe II*, 487 U.S. at 215.

[261] *See generally* Section II.A.

[262] *See, e.g.*, *Fingerprint Lock Free*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=com.nb.fingerprint.lock.free (last visited Mar. 28, 2014) (fingerprint lock on Android phone); *iOS Fingerprint Lock Screen*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=com.creativeinc.iphone5s.fingerprint.lockscreen&hl=en (last visited Mar. 28, 2014) (fingerprint lock on iPhone); *Iron Key F200 Flash Drives*, IRON KEY, http://www.ironkey.com/en-US/encrypted-storage-drives/f200.html (last visited Mar. 28, 2014) (fingerprint lock on USB drive). *See generally* Colin Soutar et al., *Biometric Encryption*, *in* ICSA GUIDE TO CRYPTOGRAPHY (Randal K. Nicols ed. 1999).

[263] *See* Marcia Hofmann, *Apple's Fingerprint ID May Mean You Can't 'Take the Fifth'*, WIRED (Sept. 13 2013, 9:23 AM), http://www.wired.com/opinion/2013/09/the-unexpected-result-of-fingerprint-authentication-that-you-cant-take-the-fifth/.

[264] *Id.*

[265] *Id.*

[266] Providing a DNA sample is a non-testimonial act. *See, e.g.*, United States v. Hook, 471 F.3d 766, 774 (7th Cir. 2006). *Cf.* Schmerber v. California, 384 U.S. 757 (1966) (holding that a blood sample is non-testimonial).

himself or herself but instead is required to allow the government to read the device.[267]

The major distinguishing feature between decryption and executing the bank records is that, as I have already discussed, decryption implicitly communicates that the accused has access to the device. But the directive in *Doe II* was carefully written as to *not* communicate that the accused had access to the foreign bank accounts.[268]

This distinction goes away when the accused's ability to access the device is a foregone conclusion. The Supreme Court said the execution of the directive in *Doe II* was like a handwriting exemplar.[269] The Court has also said that an exemplar has testimonial qualities, but that these testimonial qualities are almost always a foregone conclusion.[270] Thus if it is a foregone conclusion that one is able to decrypt, then the act of decryption is really no different, at least in testimonial value, from a handwriting exemplar.

D. Decryption Does Not Communicate Possession or Control of a Device

Decryption of a device does not communicate either that one has control of contents of a device or possession of a device. In *Fisher*, one necessarily had to have possession or control over the subpoenaed documents to produce them for the government.[271] However, decryption is distinct in several ways. First, someone using encryption can tell someone else the password to one's encrypted device. That third-party can certainly decrypt but does not necessarily have control or possession of the device. Second, usually in these decryption cases, the government possesses and controls the device because it was seized. The accused does not have control over the device but instead *can access it*. Third, in *Doe II*, the Supreme Court never required the government to know that the defendant had control of the foreign bank records before compelling the execution of the directive.[272] Similarly, in entering in a password, one does not implicitly say that one has control over the device's contents.

[267] *See* Phillip R. Reitinger, *supra* note 257, at 177-78.

[268] *Doe II*, 487 U.S. 201, 215 (1988).

[269] *Id.* at 217.

[270] Fisher v. United States, 425 U.S. 391, 411 (1976).

[271] *See id.* at 410. It would be, generally, quite unlikely that a normal citizen could produce someone else's tax records because the citizen does not possess or control them.

[272] *Doe II*, 487 U.S. at 215.

E. If Decryption Did Communicate Contents and Control, then the Lower Courts' Analysis Would Still Be Flawed

Even assuming that decryption did communicate the contents of a device, lower courts are incorrectly applying Supreme Court precedent. If decryption did communicate content, then compelled decryption would be very much like a categorical request for documents. This sort of categorical request was rejected in *Hubbell*.[273]

The Eleventh Circuit, for instance, adopted a rule requiring that the government know of the existence of some files before compelling decryption.[274] But the government, in these cases, is seeking decryption of the entire device—not the production of certain files.[275] The Eleventh Circuit seems to be saying that so long as the government has knowledge of *some* files it can compel the decryption of the *entire* device.[276] The Supreme Court in *Hubbell* did not say that if the government knew of the existence of *some* documents, it could successfully compel the production of an entire *category* of documents.[277] The lower court's analysis, if applied consistently with *Hubbell*, would permit unconstitutional fishing expeditions.[278]

A consistent application of *Hubbell* would require the defendant to produce *specific* files and not the entire content of a device. Alternatively, courts should require a comprehensive listing of every file on a device, or require the prosecution provide use and derivational use immunity for those files it does not know about prior to compelling decryption. Fortunately however, these remedies are not necessary because the premise that decryption communicates contents is incorrect.

IV. A NEW ACT OF DECRYPTION DOCTRINE

I have argued that decryption implicitly communicates that one is able to decrypt but does not communicate the contents of a device or one's control of a device. Following from this, if the witness's ability to decrypt is

[273] United States v. Hubbell, 530 U.S. 27, 44-45 (2000).

[274] *Doe III*, 670 F.3d 1335, 1349 n.28 (11th Cir. 2012).

[275] *Id.* at 1339; United States v. Fricosu, 841 F. Supp. 2d 1232, 1238 (D. Colo. 2012); *Feldman II*, No. 2:13-mj-00449-WEC, 2013 BL 116993 (E.D. Wis. Apr. 19, 2013).

[276] *Id.* at 1249 n.28.

[277] *Hubbell*, 530 U.S. at 45 ("[T]he Government has not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent."); *see also* Cole, *supra* note 75, at 185 (arguing that a broad request for documents became more difficult under *Hubbell* because there is a greater burden on the government to show knowledge of the documents).

[278] *Hubbell*, 530 U.S. at 42; *see In re* Boucher, No. 2:06-mj-91, 2007 WL 4246473 (Nov. 29, 2007) ("By compelling entry of the password the government would be compelling production of all the files on [the device], both known and unknown. . . . [T]he files the government has not seen could add much to the sum total of the government's information.").

a foregone conclusion, then decryption is a non-testimonial act. This non-testimonial act would allow the government to gain access to a potential source of information, but would not assist the government in locating or compiling evidence.

I suggest a two part analysis. First, courts should ask whether the act of decryption is presumptively privileged. As discussed in part III.A, the act of entering the password is generally going to be testimonial—it implicitly communicates an ability to access the device.

For the privilege to attach however, decryption must also be compelled and incriminating. In some cases, decryption may not be compelled. For example, one can voluntarily decrypt either during custodial interrogation[279] or during a grand jury proceeding.[280] Similarly, one's act of decryption is not always incriminating. If the danger of self-incrimination is "imagined and unsubstantial," then the government has the power to compel a testimonial act.[281] For example, if the defendant has child pornography on his or her computer and a witness saw the defendant enter in the password, the witness could be compelled to decrypt the device because there would be no danger that decryption would incriminate the witness. Alternatively, if the government grants immunity for the act of decryption, then one's act is no longer incriminatory and can be compelled.

If the defendant can meet the initial burden of showing that decryption is (1) testimonial, (2) compelled, and (3) incriminatory, then the privilege against self-incrimination attaches. However, as the Court in *Doe I* stated, the government then can offer evidence to show that the defendant's ability to decrypt is a foregone conclusion. If the government can meet this burden, then, it may compel the witness to decrypt the device because decryption would not increase the "sum total" of the government's knowledge.

One could argue that the act of decryption analysis above may permit the government to compel decryption as part of fishing expeditions. In other words, because the government is not required to know anything about the contents of a device, it could compel decryption and ransack the device should one's ability to decrypt be a foregone conclusion. This would implicate privacy interests along with granting the government an overbroad power to search one's personal, digital effects.

In response, the discussion here is just in regard to the Fifth

[279] An example of this occurred when the defendant in *Boucher* entered in the password to his laptop after waiving his *Miranda* Rights.

[280] *Cf.* Minnesota v. Murphy, 465 U.S. 420, 427 (1984) (holding a communication at a grand jury proceeding is voluntary if one incriminates oneself but does not assert a privilege against self-incrimination).

[281] Mason v. United States, 244 U.S. 362, 365-66 (1917); Marchetti v. United States, 390 U.S. 39, 88 (1968).

Amendment. There are other protections and parts of the Constitution; the Fifth Amendment privilege against compelled self-incrimination is just one check against government power.[282] The Fourth Amendment for example still restrains the government's ability to search one's digital devices.[283] Additionally, the Fifth Amendment's concern is not that of privacy.[284] The Court has recognized that the government's access to a person's papers is mostly unfettered regardless of a paper's personal nature so long as the Fourth Amendment requirements are met.[285] Similarly, having private information contained on a computer is irrelevant for a Fifth Amendment analysis.

V. AN UNSOLVABLE PROBLEM: THE ACCUSED'S REFUSAL TO DECRYPT

As this Comment argues, the law is equipped to adjudicate whether a

[282] *Cf. Doe II*, 487 U.S. 201, 214 (1988) ("[I]t should be remembered that there are many restrictions on the government's prosecutorial practices in addition to the Self-Incrimination Clause. Indeed, there are other protections against governmental efforts to compel an unwilling suspect to cooperate in an investigation, including efforts to obtain information from him. We are confident that these provisions, together with the Self-Incrimination Clause, will continue to prevent abusive investigative techniques.") (footnotes omitted).

[283] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."); *see* John E. D. Larkin, *Compelled Production of Encrypted Data*, 14 VAND. J. ENT. & TECH. L 253, 258 (2012). *See generally* Orin S. Kerr, *Searches and Seizures in A Digital World*, 119 HARV. L. REV. 531 (2005) (discussing ways of analyzing the searches of computers).

[284] Fisher v. United States, 425 U.S. 391, 400-01 (1976) ("The proposition that the Fifth Amendment protects private information obtained without compelling self-incriminating testimony is contrary to the clear statements of this Court that under appropriate safeguards private incriminating statements of an accused may be overheard and used in evidence, if they are not compelled at the time they were uttered, and that disclosure of private information may be compelled if immunity removes the risk of incrimination. If the Fifth Amendment protected generally against the obtaining of private information from a man's mouth or pen or house, its protections would presumably not be lifted by probable cause and a warrant or by immunity. The privacy invasion is not mitigated by immunity; and the Fifth Amendment's strictures, unlike the Fourth's, are not removed by showing reasonableness. The Framers addressed the subject of personal privacy directly in the Fourth Amendment. They struck a balance so that when the State's reason to believe incriminating evidence will be found becomes sufficiently great, the invasion of privacy becomes justified and a warrant to search and seize will issue. They did not seek in still another Amendment the Fifth to achieve a general protection of privacy but to deal with the more specific issue of compelled self-incrimination."); *see In re* Grand Jury Subpoena Dated Oct. 29, 1992, 1 F.3d 87, 93 (2d Cir. 1993) (citing *Fisher*, 425 U.S. at 401) ("[T]he Supreme Court's more recent opinions indicate that Boyd's foundations have eroded. The Court no longer views the Fifth Amendment as a general protector of privacy or private information, but leaves that role to the Fourth Amendment. . . . Self-incrimination analysis now focuses on whether the creation of the thing demanded was compelled and, if not, whether the act of producing it would constitute compelled testimonial communication."); *Doe I*, 465 U.S. 605, 610 n.6 (1984); Terzian, *supra* note 1, at 307.

[285] *See* cases cited *supra* note 284. I say mostly because other privileges may apply. For example, attorney-client privilege, attorney work product, or perhaps some kind of exception applying to national security.

defendant may be compelled to decrypt. The law, however, is not equipped to address what happens after the compulsion. The accused in such situations faces two possibilities: decrypt and allow the government access to the evidence or not decrypt and face contempt of court.[286] While a defendant in contempt can be incarcerated, the device remains encrypted. This hinders law enforcement's ability to use the contents of the device to investigate further crimes such as during a child pornography investigation where the government is seeking the child pornography distributor.

When one is compelled to decrypt, one could say that he or she forgot the password. The defendant in *Fricosu*, after the court ordered her to decrypt her device, "claimed" to have forgotten the password.[287] Whether that claim is true or not is nearly impossible to determine, but the more time that passes, the more likely it is to become true. If the defendant cannot remember the password and can no longer decrypt, then the coercive purpose of contempt would become inapplicable. Holding such a person in contempt would do nothing more than coerce him or her to do something that he or she is unable to accomplish, possibly opening up a defense of impossibility.[288]

One may choose contempt over decryption to avoid conviction for a sufficiently serious crime.[289] One scholar has suggested a missing witness instruction as a means to deal with the problem of a refusal to decrypt.[290] This suggestion could help solve the problem of a refusal to decrypt in some cases but not all. For example, in a case where the specific nature of the records is important to investigate a crime, a missing witness instruction may not be helpful. Also, the content of a drive may be important to future investigations, such as finding the distributor of child pornography. Alternatively, in a situation where there are national security risks, prosecution is of secondary importance to decryption and preventing catastrophe.

Some have argued for increased regulation of encryption technology.[291] First of all, this argument has First Amendment problems.[292]

[286] *See* Larkin, *supra* note 283, at 276.

[287] David Kravets, *Defendant Ordered to Decrypt Laptop May Have Forgotten Password*, WIRED, (Feb. 06, 2012, 2:55 PM), http://www.wired.com/threatlevel/2012/02/forgotten-password/; *Doe III*, 670 F.3d 1335, 1338 (11th Cir. 2012) (defendant claiming in the alternative that he forgot the password to his device).

[288] *See* Shillitani v. United States, 384 U.S. 364, 371 (1966) ("[T]he justification for coercive imprisonment as applied to civil contempt depends upon the ability of the contemnor to comply with the court's order."); Maggio v. Zeitz, 333 U.S. 56, 75 (1948).

[289] *See* Larkin, *supra* note 283, at 276.

[290] *Id.*

[291] *See* Chase Bates, comment, *Unbreakable: The Fifth Amendment and Computer Passwords*, 44 ARIZ. ST. L.J. 1293, 1313 (2012). *See generally* D. Forest Wolfe, *The Government's Right to Read:*

But as a more practical matter, the nature of online distribution and the existence of free and open source encryption software make strict regulation a losing proposition.[293]

Regardless, for all this discussion of compelled decryption, courts may be better off not going down the compelled decryption road. Instead, the solution to these problems lies in technological advancements in cryptology, computer science, and law enforcement techniques.

VI. RECENT DEVELOPMENTS

Between writing the Comment and being selected for publication, another important compelled decryption case was decided, *Commonwealth v. Gelfgatt*.[294] *Gelfgatt*, a 6-2 decision holding the Commonwealth could compel decryption, displays the importance carefully considering the differences between the product of documents and decryption.[295]

In this case, the defendant was accused of several counts of forgery, fraud, and larceny. He had encrypted several electronic storage devices.[296] The Commonwealth believed evidence of the defendant's crimes could be found on those devices.[297] The defendant had informed law enforcement that the devices were encrypted and that he *could* decrypt, but he refused to do so.[298]

The Massachusetts Supreme Court's analysis follows that of *Doe III*, *Boucher*, and *Fricosu* (though includes few citations to those cases).[299] First, it determined that "at first blush" entering in the password is

Maintaining State Access to Digital Data in the Age of Impenetrable Encryption, 49 EMORY L.J. 711 (2000).

[292] *See* Adam C. Bonin, comment, *Protecting Protection: First and Fifth Amendment Challenges to Cryptography Regulation*, 1996 U. CHI. LEGAL F. 495, 505-08 (1996); Robert Post, *Encryption Source Code and the First Amendment*, 15 BERKELEY TECH. L.J. 713 (Spring 2000); Elizabeth Lauzon, note, *The Philip Zimmermann Investigation: The Start of the Fall of Export Restrictions on Encryption Software Under First Amendment Free Speech Issues*, 48 SYRACUSE L. REV. 1307, 1337-51 (1998); *see also* Junger v. Daley, 209 F.3d 481, 485 (6th Cir. 2000) ("Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment.").

[293] *See* Paul Zimmerman, *Why I Wrote PGP*, http://www.philzimmermann.com/EN/essays/ (last visited on Feb. 13, 2014) ("If privacy is outlawed, only outlaws will have privacy. . . . PGP empowers people to take their privacy into their own hands. There has been a growing social need for it. That's why I wrote it.").

[294] 11 N.E.3d 605 (Mass. 2014).

[295] *See id.* at 617. The court also held compelled production did not offend the state constitution. *See id.* at 616-17.

[296] *Id.* at 608.

[297] *Id.* at 611.

[298] *Id.* at 610-11

[299] In fact, the majority only cites *Fricosu* and the dissent cites both *Doe III* (favorably) and *Fricosu* (unfavorably).

sufficiently communicative to trigger Fifth Amendment protection.[300] However, it stated the foregone conclusion exception permitted decryption if the government could show that it knew "(1) the existence of the evidence demanded; (2) the possession or control of that evidence by the defendant; and (3) the authenticity of the evidence."[301] The court concluded that these facts were a foregone conclusion, in part, because of the defendant's own statements indicating he could decrypt if he wanted to.[302] Although the court does not say it clearly, it does seem to indicate that it is sufficient that the government knew that: (1) the defendant had control over the devices; (2) the device was encrypted, and (3) the defendant knew the encryption key.[303]

Curiously missing from the majority's analysis is a discussion of the government's knowledge as to the existence of evidence on the device and the defendant's control over that evidence.[304] In fact, the dissent criticizes the majority saying,

> [T]he court adopts the Commonwealth's contention that, by decrypting the computers and thereby producing their unencrypted contents, the defendant *would be asserting only his ability to decrypt the devices.* On this view, he would not be asserting that he owned them, had exclusive use and control of them, or was familiar with any files on them; that certain files contained the incriminating evidence sought; or that the documents were authentic.[305]

Here, the dissent is correct in recognizing that, notwithstanding the majority's own characterization of the rule, the majority was focused on whether it was a foregone conclusion that the defendant could decrypt and not the other act of production doctrine requirements.

As this Comment argues, decryption does not implicitly communicate exclusive use, control, or familiarity with files contained within a device. If the production of physical documents were anything like compelled decryption, the dissent would be correct to chastise the majority. But it is not.

[300] Gelfgatt, 11 N.E.3d at 614.

[301] *Id.*

[302] *See id.* at 615.

[303] *See id.*

[304] *See id.* at 615-16.

[305] *See Gelfgatt*, 11 N.E.3d at 618 (Lenk, J., dissenting). The dissent took issue with the insufficiency of the government's knowledge as to what was contained within the encrypted devices. *See id.* at 620-21. The dissent would require the government to have particular knowledge of what a device contains. *Id.* at 622-23. The dissent fails to consider (and does not even cite) *Doe II* where the United States Supreme Court held that opening up a potential source of evidence does not implicitly communicate anything about that source of evidence. *See generally id.*

The confused analysis in this case displays the need for a more careful consideration of the act of production doctrine's relationship to compelled decryption. The majority's decision was messy, but perhaps the reason it was messy is that it would not make sense to strictly apply the act of production doctrine to compelled decryption cases without recognizing the differences between decryption and production.

VI. CONCLUSION

This Comment has argued that the lower courts are applying the Supreme Court's act of production doctrine improperly. The courts have failed to recognize that the witness is not, himself, producing anything at all—not in the same way that a defendant produced things in *Hubbell*, *Fisher*, and *Doe I*. Rather, the witness is typing in a password. So long as it is a foregone conclusion that the witness knows the password, the government should be able to compel the witness to enter it. Because the lower courts have misapplied the doctrine, they have provided greater protection for encryption users than what the Constitution requires. This Comment's intent is not to advocate for a limitation on an individual's interest in not incriminating himself or herself but to assist in the creation of a clear rule for when the privilege does or does not apply.

In the end, should someone not wish to decrypt, the government cannot do much to get access to the encrypted material. Although this Comment has argued for clarification in the law, I am unconvinced that the law will have much to do with battling the growing problem with encryption. Judges, prosecutors, academics, and Congress will not solve this problem; cryptographers, forensic investigators, computer scientists, and law enforcement will solve the problem.