Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 30 | Issue 3 Article 2

January 2013

A Witness Against Himself: A Case for Stronger Legal Protection of Encryption

Benjamin Folkinshteyn

A WITNESS AGAINST HIMSELF: A CASE FOR STRONGER LEGAL PROTECTION OF ENCRYPTION

Benjamin Folkinshteyn†

Abstract

This Article examines the application of the Fifth Amendment privilege against self-incrimination to compelled disclosure of unencrypted data. Such disclosure can include provision of passwords to access encrypted data as well as, increasingly, providing unencrypted data after compelled decryption.

The pervasiveness and persistence of electronic data drastically increases the availability of information with potential evidentiary value that has not previously existed with physical evidence. The courts have struggled with finding the appropriate balance in determining the scope and applicability of the privilege against self-incrimination to electronic evidence. The lack of precise physical world analogues to encryption has led to particular difficulties in this regard. I argue that encrypted data deserves broader consideration under the Fifth Amendment than heretofore established by relevant precedent. The changing technology should not be used as a reason to eviscerate the privilege against self-incrimination.

TABLE OF CONTENTS

† LL.M., *magna cum laude*, Fordham University School of Law (2012); J.D., *cum laude*, University of Pennsylvania Law School (2006); B.A., University of Pennsylvania (2002). Sk Crjjbr, gkn yee irn ekur yja qtllkns. Yja, sk Yerw, vik, arqlbsr ibq yor, iyq sytois fr fknr yhkts lysbrjpr bj sir eyqs grv fkjsiq siyj B erynjra bj sibnsx sinrr xrynq.

INTRODUCTION

The proliferation of electronic data and digitization, both as a storage medium and communication, has been a boon to law enforcement. In particular, technologically enhanced surveillance techniques, off-site storage, and "cloud" computing have dramatically increased the amount of information available to law enforcement. The pervasiveness and persistence of such electronic data drastically increases the availability of information with potential evidentiary value that has not previously existed with physical evidence.

Electronic data has also presented a number of challenges. The business community and individuals are increasingly aware and protective of their electronic data (from prying eyes, both lawful and unlawful) as the use of such data exponentially increases. Stakeholders have attempted to secure such data by encryption. Encryption can prevent even the most determined and technologically-equipped third party from discovering the contents without the requisite passwords.

Encryption technology presents an obstacle to those who seek to gain access for traditionally illicit purposes, *e.g.*, to misappropriate money or property of another. It is also presents an obstacle to those who desire to gather information in pursuit of a law enforcement function.[1] Law enforcement personnel may come upon encrypted data in a variety of ways, including from electronic wiretapping or eavesdropping, seizing evidence, or seeking documentary evidence from a witness or defendant through use of a subpoena.

This paper examines the scope of the Fifth Amendment privilege against self-incrimination as it applies to encryption. It examines a variety of situations in which a defendant or witness may be compelled to disclose unencrypted forms of encrypted data (including documents and electronic mail) alleged to be in his possession, either through provision of passwords to decrypt the data or through the provision of underlying data after compelled decryption. Part I of the paper discusses the basics of the cryptographic process. It presents a four-scenario framework which illustrates the circumstances under which self-incrimination conflicts with law enforcement interests. Part II provides an overview of Fifth Amendment jurisprudence and the judicial gloss on the individual's ability to exercise the right

1. It is beyond the scope of this paper to discuss the variety of law enforcement functions for which information gathering is an essential part, as well as the constitutional limitations of such functions.

against self-incrimination. Parts III and IV discuss the relevant judicial decisions tackling Fifth Amendment issues in the context of encrypted data. Part V covers the various analogies courts and commentators have used in debating the appropriateness of the privilege against self-incrimination in resisting disclosure. Part VI proposes that in the context of illegal content, courts should be particularly mindful of compelling disclosure. Part VII cautions against overreaction to perceived threats from encryption to law enforcement and points to pre-existing drastic capabilities of law enforcement in electronic surveillance. Finally, Part VIII discusses the latest developments in Fourth Amendment jurisprudence with respect to electronically stored information. The paper concludes by calling for a careful balancing of the various law enforcement and individual interests in order to avoid creating unintended negative effects on constitutional protections of individual rights.

I. WHAT IS ENCRYPTION?

Encryption is a process by which the content of a particular message or document becomes unintelligible to a third party by a predesignated scrambling protocol.[2] As a simple example, imagine that Bob wants to convey a number to Alice over an observable and interceptable transmission medium (such as an email, a letter in the mail, or a shout across a crowded room), without anyone being able to tell what the number actually is. To accomplish this task, Bob and Alice could agree in secret that before transmitting his message, Bob will add 143 to the real number. Thus, when Bob wants to convey the number 20, he will actually send the "encrypted" message of 163. Alice can easily "decrypt" it by subtracting 143 and realize that the real message is 20. No other observer can determine what the real message is without knowing the encryption protocol (addition), or the particular encryption key (143). Real-world ciphers in use today are more complex for a number of reasons, but this example serves to illustrate the basic framework under discussion.

A related concept is steganography which is employed to hide the very existence of a message from the third party.[3] Thinking back to our example of Alice and Bob, imagine that Bob not only wants to convey a message to Alice via a publicly observable medium, but also wants to do it in such a way that observers do not realize a message

2. SIMON SINGH, THE CODE BOOK: THE SCIENCE OF SECRECY FROM ANCIENT EGYPT TO QUANTUM CRYPTOGRAPHY 6 (2000).

3. *Id.* at 5.

was transmitted. Again, in private, Bob and Alice will agree on a scheme ahead of time. Then Bob posts some flyers around town saying something like, "Join the Springfield Baking Club on Friday, October 20, for a baking presentation, to be held at the Basketball court on 3rd and Spruce. Rain or shine. We will talk about sourdough and tofu breads." Because Bob and Alice agreed that the message will be conveyed via the number of non-whitespace characters in a flyer about the Springfield Baking Club, Alice correctly gets the message of "163" and subtracts 143 to get the real message of 20. We assume that they agreed to keep the same encryption scheme as before. Everyone else can observe the message, but doesn't know there was a secret message hidden within, or who it was intended for.

Modern encryption software can be roughly categorized into "file-level encryption" and "disk-level encryption." File-level encryption allows the user to encrypt the contents of individual files. The presence of the file and the file metadata—filename, modification and access dates, file size—remain available to an attacker who gains possession of the storage medium. Email encryption software, such as GNU Privacy Guard (GPG), falls into this category, since each email is encrypted individually for transmission. The existence of the message as well as the sender and recipient are known to observers. Disk-level encryption creates an encrypted container on the entire disk so that all files stored are automatically encrypted into one giant glob of bits. An attacker might suspect that the disk is not just filled with gibberish and is likely encrypted, but would have no idea as to the number and size of the files on the disk, if any, their names, or possible content. Some software, such as TrueCrypt, goes a step further and allows the creation of nested hidden volumes. Even if the key/passphrase is revealed for the outer volume, there is no way to tell if there are interior encrypted volumes with more data.[4]

Free and open source encryption software, along with the knowledge of how to use it, is available to anyone with an Internet connection. Without a passkey, it is impossible to decrypt data where there is properly implemented, strong encryption software. Even law enforcement agencies with large budgets and access to significant computing power cannot decrypt such data. Where traditional intelligence gathering and wiretapping techniques fail or are not attempted prior to arrest, it has become necessary to seek cooperation

4. *See Hidden Volume*, TRUECRYPT, http://www.truecrypt.org/docs/hidden-volume#Y0 (last visited Nov. 2, 2013).

from defendants to divulge their passkeys despite assertions of Fifth Amendment privilege.

The earliest Fifth Amendment encryption issue surfaced in connection with the prosecution of Edward Leary, a disgruntled computer analyst who planted two homemade gasoline bombs on a train in Manhattan in December 1994, injuring dozens of people.[5] In the course of pretrial hearings, Leary refused to divulge his computer password for "personal reasons" as his attorneys argued that such disclosure would violate Leary's Fifth Amendment rights.[6] The prosecution, in turn, asserted that self-incrimination was not at issue since the requested "[code] words themselves don't create evidence."[7] Judge Rena Uviller did not rule from the bench immediately, although she analogized the request "to breaking a lock on a diary while exercising a search warrant."[8] Ultimately, no judicial decision was issued as the state's forensics team was able to break Leary's password without his assistance.[9]

I propose that there are four types of fact scenarios which can arise in the application of Fifth Amendment privilege against self-incrimination to encrypted content. All of these permutations may be encountered in situations where it may be necessary to seek a court order compelling a defendant to divulge his passkey on penalty of civil or criminal contempt. They are as follows: (1) content altogether inaccessible and the substance of which is unknown, (2) content initially accessible by law enforcement personnel which subsequently became cryptographically inaccessible, (3) inaccessible content, the substance of which later becomes collaterally apparent from other sources, (4) content which becomes accessible after a duly issued court order. Each of these scenarios requires a somewhat different approach under current jurisprudence and, ultimately, a better understanding of the nature of encryption and its relationship to self-incrimination.

II. BASIC OVERVIEW OF RELEVANT JURISPRUDENCE

The Fifth Amendment of the U.S. Constitution reads, in relevant

5. George James, *Man Convicted in Bombings on Subway*, N.Y. TIMES, Mar. 8, 1996, at B4.

6. Barbara Ross, *Bomb Suspect Won't Yield Code*, N.Y. DAILY NEWS, Jan. 12, 1996, at 22.

7. *Id.*

8. *Id.*

9. Interview with Peter Casolaro, Assistant Dist. Attorney, N.Y. Cnty. (Feb. 4, 2013).

part, that "[n]o person shall be compelled in any criminal case to be a witness against himself."[10] The early impetus for this privilege was the prevention of confessions obtained through duress or torture.[11] It is also thought to logically flow from the fact that "the American system of criminal prosecution is accusatorial, not inquisitorial, and that the Fifth Amendment privilege is its essential mainstay."[12] The scope of the privilege encompasses all incriminating evidence used to establish the accused's guilt—such evidence must be "independently and freely secured, and may not by coercion prove a charge against an accused out of his own mouth."[13]

The privilege, however, does not treat an individual as a "witness against himself" under all circumstances. It "protects an accused only from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature."[14] To be deemed "testimonial," the person's "communication must itself, explicitly or implicitly, relate a factual assertion or disclose information."[15]

As to documentary and physical evidence, the Fifth Amendment applies to disclosures which are (1) compelled, (2) involve a testimonial act, and (3) tend to incriminate the person so compelled.[16] Additionally, even if documentary evidence is not in itself testimonial, the act of production may be sufficiently testimonial to give rise to Fifth Amendment protections.[17]

10. U.S. CONST. amend. V.

11. *See* Ullmann v. United States, 350 U.S. 422, 447 (1956) ("[T]here are indications in the debates on the Constitution that the evil to be remedied was the use of torture to exact confessions.").

12. Malloy v. Hogan, 378 U.S. 1, 7 (1964); *see also* Murphy v. Waterfront Comm'n, 378 U.S. 52, 55 (1964) ("It reflects many of our fundamental values and most noble aspirations: our unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt; our preference for an accusatorial, rather than an inquisitorial, system of criminal justice . . . .").

13. *Malloy*, 378 U.S. at 8. The privilege is construed to include not only those proceedings where a person's testimony is sought in his *own* criminal prosecution, but also "that a person shall not be compelled, when acting as a witness in any investigation, to give testimony which may tend to show that he himself has committed a crime." Counselman v. Hitchcock, 142 U.S. 547, 547 (1892).

14. Doe v. United States (*Doe I*), 487 U.S. 201, 210 (1988) (requiring defendant to sign a consent form authorizing foreign banks to disclose any and all accounts which defendant may have with the banks does not violate the Fifth Amendment).

15. *Id.*

16. United States v. Authement, 607 F.2d 1129, 1131 (5th Cir. 1979) (production of brass knuckles).

17. Fisher v. United States, 425 U.S. 391, 410 (1976) ("The act of producing evidence in response to a subpoena nevertheless has communicative aspects of its own, wholly aside from

Two recent oft-cited Supreme Court decisions inform the discussion on self-incrimination through compelled production of documents by the defendant. In *Fisher*, defendant taxpayers had given certain tax documents prepared by their accountants to their attorneys in the course of two IRS investigations.[18] The IRS sought production of these documents from the taxpayers' attorneys.[19] The Supreme Court held, in relevant part, that the documents were not entitled to Fifth Amendment protection and, more importantly, that the act of production itself is not testimonial because in that particular instance "implicitly admitting the existence and possession of the papers [does not rise] to the level of testimony within the protection of the Fifth Amendment."[20] As a practical matter, "[t]he existence and location of the papers are a *foregone conclusion* and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers."[21]

The flip side of *Fisher* is *Hubbell* where, subsequent to a grant of immunity by the Government, the defendant produced thousands of pages of documents pursuant to a grand jury subpoena.[22] In dismissing the grand jury indictment based in part on the content of the immunized documents, the Supreme Court held that the foregone conclusion rationale did not apply to the defendant's production (which was also entitled to derivative use immunity) because "the Government has not shown that it had *any* prior knowledge of either the existence or the whereabouts of the [documents] ultimately produced."[23]

The Court further held that with respect to the defendant's response to the broadly worded eleven categories of documents sought by the subpoena requests, the collation and gathering of documents necessarily required the defendant to divulge "the contents of his own mind" and that such production was akin to "telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox."[24]

Even if a defendant or witness exercises his right against self-

the contents of the papers produced."). *See also* United States v. Doe (*Doe II*), 465 U.S. 605, 612 (1984) (production of subpoenaed records of a sole proprietorship).

18. *Fisher*, 425 U.S. at 394.
19. *Id.*
20. *Id.* at 411.
21. *Id.* (emphasis added).
22. United States v. Hubbell, 530 U.S. 27 (2000).
23. *Id.* at 44-45.
24. *Id.* at 43.

incrimination in appropriate circumstances, he can still be compelled to testify when granted use and derivative use immunity pursuant to 18 U.S.C Section 6002 or similar state statutes. The Supreme Court has held that such immunity is "coextensive with the privilege and suffices to supplant it."[25] State practice differs and may provide for more or less protection than the federal rules.[26]

III. INACCESSIBLE AND UNKNOWN CONTENT

Very few courts, and no circuit court prior to 2012, have dealt with compulsion of disclosure of encrypted data in decrypted form. Those courts struggled with the nature of encryption. They also struggled with the consequences of and differences in compelling a defendant to produce either the unencrypted content, or the passwords that would allow the Government to access the unencrypted content.

The most recent circuit court case represents the first scenario proposed and, perhaps, the easiest to resolve on the facts alone.

A. Facts and Legal Issues

In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011 (*Doe*) from the Eleventh Circuit is the latest and the only appellate decision to date that discusses the issues head on.[27] The case arose out of a lawful seizure of several hard drives allegedly belonging to the defendant (Doe) during a child pornography investigation.[28] In the course of the investigation, law enforcement officers determined that Doe accessed the Internet from Internet Protocol addresses assigned to certain hotels. [29] Eventually, the officers applied for a search warrant to Doe's room when he was tracked to a hotel in California.[30] In the process of executing the search warrant, several large external hard drives and other storage media were seized.[31] When the Government's forensic examiners attempted to analyze the data on the hard drives, they were unable to access certain portions of

25. Kastigar v. United States, 406 U.S. 441, 462 (1972).

26. Absent a waiver, New York State automatically provides for transactional immunity to witnesses testifying in a legal proceeding, such as in front of a Grand Jury. *See* N.Y. CRIM. PROC. LAW §§ 50.10, 190.40.

27. *In Re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011 (United States v. Doe), 670 F.3d 1335 (11th Cir. 2012).

28. *Id.* at 1339.

29. *Id.*

30. *Id.*

31. *Id.*

those drives because they were strongly encrypted.[32]

As a result, the Government sought and obtained a grand jury subpoena, requiring Doe to "produce the unencrypted contents of the digital media, and any and all containers or folders thereon."[33] Doe challenged the subpoena on Fifth Amendment self-incrimination grounds.[34] To overcome the challenge, the Government requested that Doe be granted immunity "limited to the use [of Doe's] act of production of the unencrypted contents."[35] The district court granted the Government's request.[36] Nevertheless, Doe, appearing before the grand jury, refused to decrypt the hard drives on Fifth Amendment grounds because the grant of immunity did not cover derivative use of his testimony, i.e., the decryption.[37] At the order to show cause hearing, Doe argued that the Government at trial would need to prove that "(1) the hard drives belonged to [him] (which was not in dispute) and (2) contained child pornography."[38] Since the grant of immunity was limited to act-of-production immunity, proving the second point would be a result of the derivative use of his testimony since "by decrypting the contents, he would be testifying that he, as opposed to some other person, placed the contents on the hard drive, encrypted the contents, and could retrieve and examine them whenever he wished."[39] The district court did not accept Doe's position, finding that Doe's decryption and production is not testimonial and found him to be in contempt.[40]

In overturning the lower court, the Eleventh Circuit held that it was an error (1) to consider Doe's decryption and production of hard drives as a non-testimonial act not entitled to Fifth Amendment protections and (2) to limit the grant of immunity to use immunity only, thus allowing the Government derivative use of the contents of the hard drives once they are disclosed.[41]

B. Reasoning

There was no dispute that the production and decryption of the

32. *Id.*
33. *Id.* (internal quotation marks omitted).
34. *In Re* Grand Jury Subpoena Duces Tecum, 670 F.3d at 1338.
35. *Id.*
36. *Id.*
37. *Id.*
38. *Id.* at 1339.
39. *Id.* at 1339-40.
40. *In Re Grand Jury Subpoena Duces Tecum*, 670 F.3d at 1340.
41. *Id.* at 1341.

data was both compelled and incriminatory within the meaning of the Fifth Amendment.[42] The core of the *Doe* decision rested on the analysis of whether "the Government sought *testimony* within the meaning of the Fifth Amendment" in seeking the production of decrypted contents of Doe's computer.[43]

1. Little Protection for Voluntarily Created Documents

As a general matter, pre-existing documents voluntarily created by the person from whom they are sought are not deemed to be protected under the Fifth Amendment because their creation was not initially compelled.[44] They are not protected despite the fact that they may contain incriminating statements, since the privilege "protects a person only against being incriminated by his compelled testimonial communications."[45] Thus, the court had no difficulty determining that as a threshold matter "the files, if there are any at all in the hidden portions of the hard drives, are not themselves testimonial."[46]

Despite the non-testimonial nature of the files themselves, under certain circumstances the *act of production* may have sufficient communicative qualities apart from the underlying documents sought, triggering Fifth Amendment protections against self-incrimination. Thus, constitutional privileges may be implicated where "[c]ompliance with a subpoena tacitly concedes the existence of the papers demanded and their possession or control by the [party]" or where production would indicate the party's "belief that the papers are those described in the subpoena."[47]

2. Application of Act of Production Principles to Encrypted Contents

In applying the principles spelled out in *Fisher and Hubble* (discussed in Part II above), the Eleventh Circuit in *Doe* reasoned that under the foregone conclusion principle "where the location, existence and authenticity of the purported evidence is known with reasonable particularity, the contents of the individual's mind are not

42. *Id.*

43. *Id.* at 1342.

44. *See, e.g.*, *Doe II*, 465 U.S. 605, 611-12 (1984). This so-called "private papers" doctrine has drastically evolved since the early years of American jurisprudence when such documents were considered to be protected both under the Fourth and the Fifth Amendments. *See* Boyd v. United States, 116 U.S. 616 (1886).

45. United States v. Fisher, 425 U.S. 391, 409 (1976).

46. United States v. Doe (*Doe III*), 670 F.3d 1335, 1342 (11th Cir. 2012).

47. *Doe II*, 465 U.S. at 612-13 (1984) (citations omitted) (*citing Fisher*, 425 U.S. at 410).

used against him, and therefore no Fifth Amendment protection is available."[48] At the same time, an act of production may be testimonial where it conveys "some explicit or implicit statement of fact" of the alleged material's existence within the individual's possession or the material's authenticity.[49] The court thus used a two-step approach in tackling the encryption problem. To be deemed non-testimonial, an act of production must arise from (1) an individual being compelled to perform a physical act rather than "make use of the contents of his or her mind," for example, to produce a key to a safe containing documents, or (2) the testimonial aspects of production are defeated by the "foregone conclusion" doctrine.[50]

Under the above framework, the court disagreed with the Government that requiring Doe to produce the unencrypted contents would be akin to requiring Doe to produce a key to a lockbox—"nothing more than a physical non-testimonial transfer."[51] The court reasoned that "requiring Doe to use a decryption password is most certainly akin to requiring the production of a combination" as it demands him to produce the "contents of his mind."[52] More importantly, however, the act of production would also carry testimonial implications that Doe has "knowledge of the existence and location of potentially incriminating files; of his possession, control and access to the encrypted portions of the drives; and of his capability to decrypt the files."[53]

Turning to the second exception, the court held that unlike in *Fisher*, the testimonial aspects of Doe's production were not a "foregone conclusion." The foregone conclusion doctrine operates to defeat the constitutional ramifications of acts of production where the testimonial aspects are otherwise known to the Government.[54] Thus, the witness's concessions add "little or nothing to the sum total of the Government's information."[55] In compelling a witness to testify under such circumstances, "no constitutional rights are touched[; t]he question is not of testimony, but of surrender."[56]

48. *Doe III*, 670 F.3d at 1344.

49. *Id.* at 1345.

50. *Id.* at 1345-46.

51. *Id.* at 1346.

52. *Id.* See also *In re* Boucher, 2009 U.S. Dist. LEXIS 13006 (D. Vt. Feb. 19, 2009), for its narrowed subpoena request in *Boucher*, i*nfra* Section IV.A, note 63.

53. *Id.*

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

55. *Id*.

56. *Id.*

While the Government was able to demonstrate that "the combined storage space of the drives *could* contain files that number well into the millions" it was unable to show that "the drives *actually* contain any files, nor has it shown which of the estimated twenty million files the drives are capable of holding may prove useful."[57] While the IRS, in *Fisher*, was fully aware of the specific documents (though, not necessarily all of them) it sought and knew that they were in the possession of the taxpayers' attorneys, the Government here could not show that "it possessed even a remotely similar level of knowledge of the *files* on the hard drives at the time it attempted to compel production from Doe."[58] Even though exact specificity in subpoena requests is not required, "categorical requests for documents the Government anticipates are likely to exist simply will not suffice."[59]

As a result, the court found that the Government was unable to carry its burden under the foregone conclusion exception "to show any basis, let alone shown a basis with reasonable particularity, for its belief that encrypted files exist on the drives, that Doe has access to those files, or that he is capable of decrypting the files."[60]

3. Limited Immunity Was Not Sufficient

The remainder of the court's opinion reversing the district court's civil contempt order against Doe was thus predetermined. Since Doe's act of production was sufficiently testimonial to warrant Fifth Amendment self-incrimination protections, the district court's grant, per the Government's request of only use immunity, to compel Doe to testify was improper because such limited immunity is not co-extensive with the privilege against self-incrimination.[61] Relying on *Kastigar v. U.S.*, the court reasoned that only "use and derivative use immunity establishes the critical threshold to overcome an individual's invocation of the Fifth Amendment privilege against self-incrimination."[62] It was not sufficient for the Government to request and for the district court to grant such limited immunity to compel

57. *Doe III*, 670 F.3d 1335, 1347 (11th Cir. 2011) (emphasis in original). The nature of the encryption program in this case, TrueCrypt, was such that it would also encrypt any unused space rendering any distinction between unused space and actual data impossible to determine. *Id.*

58. *Id.*

59. *Id.*

60. *Id.* at 1349.

61. *Id.* at 1350.

62. *Id.* at 1351 (*citing* Kastigar v. United States, 406 U.S. 441, 460 (1972)).

Doe's production since the files thus decrypted could still be used against him and they are "directly or indirectly derived from" compelled testimony.[63]

IV. INACCESSIBLE BUT "KNOWN" CONTENT

The two cases highlighted here represent Scenarios II and III, respectively. They are conceptually more nuanced and the correctness of the outcome in each situation is more debatable. To the extent that each holding may be jurisprudentially sound, questions still remain as to whether the outcomes would have been the same had the Eleventh Circuit case (discussed in Part III) preceded these two decisions. The third case straddles the two categories. However, it was ultimately resolved without a final judicial ruling and thus it still remains to be seen how the Eleventh Circuit framework would play out at the district court level.

A. Grand Jury Subpoena to Sebastian Boucher

The facts of *Grand Jury Subpoena to Sebastian Boucher (In re* Boucher) arose out of a border search and a seizure of Boucher's laptop as he was entering the U.S. by car from Canada.[64] When Boucher's laptop (which he admitted to be his) was inspected at secondary screening, the inspector conducting the screening observed that the computer contained over 40,000 images, some of which appeared to be involving child pornography based on their file names.[65] After being given *Miranda* warnings, Boucher directed the border agents to the location on his hard drive where he stored pornographic material.[66] A further inspection of that location on the hard drive, led to the finding of a number of videos and images that appeared to involve child pornography, at which point Boucher was arrested, and his laptop was seized and shut down.[67] When a forensic

63. *Doe III*, 670 F.3d at 1351.

64. *In re* Boucher, No. 2:06-mj-91, 2009 U.S. Dist. LEXIS 13006 (D. Vt. Feb. 19, 2009). Generally, the border search doctrine provides an exception to Fourth Amendment's protections against unreasonable search and seizure. Thus, "[s]earches of closed containers and their contents can be conducted at the border without particularized suspicion under the Fourth Amendment." United States v. Arnold, 533 F.3d 1003 (9th Cir. 2008). This includes computers and files contained therein. *Id.* Under the border search doctrine, electronic media may be seized and transported away from the border for further forensic analysis for a limited period of time. *See, e.g.*, United States v. Cotterman, 637 F.3d 1068 (9th Cir. 2011).

65. *In re Boucher*, 2009 U.S. Dist. LEXIS 13006, at *4.

66. *Id.* at *5.

67. *Id.*

examination was attempted at a later time and the computer was rebooted, the particular portion of the hard drive containing pornography was found to be encrypted by Pretty Good Privacy (PGP), an encryption program, and thus, inaccessible.[68] As a result, the Government applied for and received a grand jury subpoena directing Boucher to produce the password.[69] At a later date, the request was narrowed to require Boucher only "to produce an unencrypted version of the [drive.]"[70]

The district court held that the testimonial nature which may have existed with respect to the incriminatory act of production was superseded by the Government's knowledge of the existence and location of the documents as per the foregone conclusion doctrine.[71] Here, Boucher admitted that the computer was his at secondary screening and, more importantly, accessed the drive in the presence of the border agents who observed the general character of the files present on the drive, including images of potential child pornography.[72]

In a holding that appears more permissive in applying the foregone conclusion doctrine, the district court observed that the doctrine "does not require that the government be aware of the incriminating *contents* of the files; it requires that the government demonstrate with reasonable particularity that it knows the existence and location of subpoenaed documents."[73]

The conditions in *In re Boucher* as to the Government's knowledge were not present in the *Doe* decision. To the extent that it needed distinguishing, the Eleventh Circuit observed that although the Government need not have shown that it knew of the contents of the files it sought in *In re Boucher*, a showing of the Government's knowledge that the files actually exist was still required thereunder.[74]

68. *Id.*

69. *Id.* at *6. Government experts specifically testified that they were unable to access the relevant drive. *Id.* at *5.

70. *In re Boucher*, 2009 U.S. Dist. LEXIS 13006, at *6.

71. *Id.* at *10.

72. *Id.* at *9.

73. *Id.* at *8. In doing so, the district court overturned the Magistrate's finding that the foregone conclusion did not apply because the government did not see every file on the drive and therefore it did not know whether most files were incriminating. *Id.* Nonetheless, the district court prohibited the Government from using Boucher's act of production in their case to authenticate the contents. *Id.*

74. *Doe III*, 670 F.3d 1335, 1349 (11th Cir. 2011). Thus, in *Boucher*, the Government need not have shown what was contained in a file labeled "2yo getting raped during diaper change;" it was "crucial that the Government knew that there existed a file with such a name."

Further, there was no indication that the Government, "at the time it sought to compel production [by Doe], knew to any degree of particularity, what, if anything, was hidden behind the encrypted wall."[75] The Eleventh Circuit seems to also require some independent knowledge (as opposed to mere suspicion) as to the contents, in addition to the location and the existence of the subpoenaed documents.[76] Such a limitation was apparent in the reasoning of the *Boucher* court inasmuch as it did find that the border agents were initially able to view certain files and "ascertained that they may consist of images or videos of child pornography."[77]

Under either approach, the fact that decryption[78] and production of the unencrypted data may provide the Government with additional incriminating information as yet unknown to it is not necessarily relevant for Fifth Amendment purposes.[79] So long as the Government makes the relevant threshold showing of knowledge, the potential for revelation of additional information is not a bar to production.[80]

B. United States v. Fricosu

In *United States v. Fricosu*,[81] Ramona Fricosu (along with her ex-husband) was accused of engaging in certain fraudulent real estate transactions and money laundering.[82] In executing a search warrant

Id.

75. *Id.*

76. Doe's act of production would be very similar to Hubbell's inasmuch as prior to the act of production; the Government has no knowledge as to the documents' existence. Thus, while the contents themselves are non-testimonial in nature (since their creation was not compelled), the testimonial nature of the act of production which reveals the documents' existence requires both use and derivative use immunity to meet the requirements of *Kastigar*.

77. *In re* Boucher, No. 2:06-mj-91, 2009 U.S. Dist. LEXIS 13006, at *9 (D. Vt. Feb. 19, 2009).

78. Perhaps even the provision of a password may be compelled under this line of cases, though it seems likely that such a request would be deemed a "product of the mind" in itself and thus protected directly under the Fifth Amendment protections against self-incrimination. *See, e.g.*, United States v. Kirschner, 823 F. Supp. 2d 665, 666 (E.D. Mich. 2010) (quashing grand jury subpoena which called for defendant "to provide all passwords used or associated with the . . . computer . . . and any files.").

79. *See Doe III*, 670 F.3d at 1347 ("Case law from the Supreme Court does not demand that the Government identify exactly the documents it seeks, but it does require some specificity in its requests – categorical requests for documents the Government anticipates are likely to exist simply will not suffice."). This topic is discussed later in Section VI.

80. *Compare* United States v. Kim, 677 F. Supp. 2d 930 (S.D. Tex. 2009) (Fourth Amendment and encrypted data) *with* United States v. Payton, 573 F.3d 859 (9th Cir. 2009).

81. United States v. Fricosu, 841 F. Supp. 2d 1232 (D. Colo. 2012).

82. *See* Indictment, United States v. Fricosu, 841 F. Supp. 2d 1232, (D. Colo. 2012) (No. 10-CR-00509).

on her property, the FBI seized a number of computers ostensibly belonging to Fricosu and others in her household.[83] One laptop computer found in Fricosu's bedroom and tagged electronically with her name was found to be encrypted with PGP.[84] As was the case in *Boucher*, the Government was unable to decrypt it on its own.[85] As a result, they sought a writ requiring Fricosu to produce the contents of the encrypted drive based in particular on an intercepted conversation that Fricosu had with her incarcerated husband in which she said, in relevant part, that "it was on my laptop" and that she may have encrypted it.[86]

Relying on the reasoning in *Boucher*, the court held that Fricosu's act of production would not be sufficiently testimonial based on the doctrine of foregone conclusion as the Government met its burden of proof in showing that the laptop in question either belonged to Fricosu or Fricosu was the sole user thereof and that she admitted as much during the intercepted conversation.[87] Additionally, although the holding is somewhat unclear and the discussion of the elements of the foregone conclusion doctrine is absent, the court found that:

> There is little question here but that the government knows of the existence and location of the computer's files. The fact that it does not know the specific content of any specific document is not a barrier to production.[88]

That latter conclusion is not present in *Boucher*. Recall in *Boucher*, the border agents were able to ascertain in part the nature of a number of the files on Boucher's computer and, in particular, the contraband nature thereof. There was no indication in *Fricosu* (and there does not appear to be any discussion in the decision as to the evidence actually sought and the particularity with which the recorded conversation described the contents) that the Government could identify with "reasonable particularity" what "it" was.[89] Nevertheless,

83. *Fricosu*, 841 F. Supp. at 1234.

84. *Id.*

85. *Id.*

86. *Id.* at 1235.

87. *Id.* at 1237.

88. *Id.*

89. The elements of "reasonable particularity" with respect to electronic data seem to be that "(1) the file exists, (2) the file is possessed by the target of the subpoena, and (3) the file is authentic." *See Doe III*, 670 F.3d 1335, 1349 (11th Cir. 2011) (citing United States v. Norwood, 420 F.3d 888, 895-96 (8th Cir. 2005)). *See also* Government's Application under the All Writs Act Requiring Defendant Fricosu to Assist in the Execution of Previously Issued Search

just as in *Boucher*, Fricosu was only offered immunity for the act producing the unencrypted documents, not their contents.[90]

The Eleventh Circuit, in discussing the *Fricosu* opinion, distinguished the case by relying heavily on the recorded conversation between Fricosu and her ex-husband. For all intents and purposes, "Fricosu essentially admitted every testimonial communication that may have been implicit in the production of the unencrypted contents."[91]

Fricosu appealed the finding of the district court. The Court of Appeals for the Tenth Circuit did not resolve the question but instead rejected the appeal as not ripe for adjudication under the rules of finality.[92] Subsequent to the district court decision, although there were some indications by Fricosu's attorney that she may have forgotten or never known the password,[93] she (or likely her ex-husband) eventually provided the passwords which then were used successfully by the Government to decrypt the laptop.[94]

C. In the Matter of the Decryption of a Seized Data Storage System

This last criminal case has seen some interesting twists and reversals of fortune for both the putative defendant and the federal Government. The facts of the case are fairly run-of-the-mill as set forth in the Magistrate's decision.[95] A warrant was issued for Jeffrey Feldman's residence allowing Federal Bureau of Investigations (FBI) agents to enter and search Feldman's premises for evidence of child pornography, including electronic storage media.[96] In the course of

Warrants, United States v. Fricosu, 841 F. Supp. 2d 1232, (D. Colo. 2012) (No. 10-CR-00509-01-REB), *available at* https://www.eff.org/node/58551 (last visited Apr. 25, 2012). There is a potential argument that this is a very restrictive reading of the lowered thresholds set forth in *Fischer*.

90. *Fricosu*, 841 F. Supp. 2d at 1238.

91. *Doe III*, 670 F.3d at 1349, n.27.

92. United States v. Fricosu, No. 12-701, 2012 U.S. App. LEXIS 3561 (10th Cir. Feb. 21, 2012).

93. David Kravets, *Defendant Ordered to Decrypt Laptop May Have Forgotten Password*, WIRED (Feb. 6, 2012, 2:55 PM), http://www.wired.com/threatlevel/2012/02/forgotten-password/.

94. *See* Government's Notice Regarding Compliance with Court's Order of January 23, 2012, United States v. Fricosu, 841 F. Supp. 2d 1232 (D. Colo. 2012) (No. 10-CR-00509-REB-02).

95. Order Denying Application to Compel Decryption, In the Matter of the Decryption of a Seized Data Storage System, No. 13-M-449 (E.D. Wis. Apr. 19, 2013) (Callahan, J.).

96. *Id.* at 2.

the search, before invoking his right to counsel, Feldman, a software engineer, stated that he was the sole occupant of the residence searched and that he had lived there for over 15 years.[97]

The FBI seized a number of storage devices, a number of which it found to be encrypted.[98] One of the unencrypted devices was found to contain a peer-to-peer file-sharing program, the logs of which seemed to indicate that certain files potentially suggestive of child pornography were transferred therewith.[99] Other unencrypted computer logs appeared to indicate that the files so-named were downloaded to the encrypted devices.[100]

As a result, the Government applied for an order under the All Writs Act to compel Feldman to "assist in the execution of a federal search warrant by providing federal law enforcement agents a decrypted version of the contents of his encrypted data storage system."[101]

Initially, Magistrate Judge Callahan denied the order sought by the Government. Applying the Eleventh Circuit rubric, the magistrate found that although (1) the "existence and location of the [files] are foregone conclusion" since circumstantial evidence from unencrypted devices indicates presence of child pornography on the encrypted devices, (2) Feldman may be capable of accessing the encrypted portion of the drives given his computer engineering background and his being the sole occupant of the residence searched, as a "close call" matter, if compelled:

> Feldman's act of production which would necessarily require his using a password of some type to decrypt the storage device would be tantamount to telling the government something it does not already know with 'reasonable particularity'—namely, that Feldman has personal access to and control over the encrypted storage devices.[102]

In an interesting twist, however, since Feldman was not charged or brought before a grand jury at the time, the Government sought reconsideration of its motion on an *ex parte* basis.[103] On that motion,

97. *Id.*

98. *Id.*

99. *Id.*

100. *Id.*

101. Order Denying Application to Compel Decryption, In the Matter of the Decryption of a Seized Data Storage System, No. 13-M-449 (E.D. Wis. Apr. 19, 2013) (Callahan, J.).

102. *Id.*

103. Bruce Vielmetti, *Did U.S. Prosecutors Mislead Judge in West Allis Decryption*

the Government showed that, subsequent to the original order, it was able to decrypt on their own a small portion of one of the encrypted drives and was able to observe child pornography files as well as Feldman's personal files.[104] The Government, thus, argued that this discovery mooted any act of production concerns with respect to "access and control" and the magistrate judge agreed, holding that "it is a 'foregone conclusion' that Feldman has access to and control over the subject encrypted storage devices."[105] On penalty of contempt, Feldman was ordered to assist the Government with decrypting the seized encrypted devices.[106]

This decision, however, did not stand for long. Upon finding out about this *ex parte* decision, Feldman filed an emergency motion seeking a stay of the magistrate's latest order before the district court, arguing, *inter alia*, that the *ex parte* nature of the order was improper.[107] Judge Rudolph Randa granted the stay and ordered further briefing.[108] Subsequent briefs have sparred over a number of issues, including the propriety of the prosecutors' actions and, in particular, whether they misled the magistrate about the alleged complexity of the computer system used by Feldman and Feldman's sophistication as a computer user in seeking to have the original order reconsidered.[109] Ultimately, the Government was able to crack one of the drives seized, charged Feldman with possession, distributing or receiving child pornography, and dropped its motion to compel decryption.[110]

Case?, MILWAUKEE WISCONSIN JOURNAL SENTINEL (July 23, 2013), http://www.jsonline.com/news/crime/did-us-prosecutors-mislead-judge-in-west-allis-decryption-case-b9958202z1-216673531.html. The title of the article refers back to the original search warrant which was filed as *In the Matter of the Search of 2051 S. 102nd Street, Apartment E, West Allis*, No. 13-M-421 (E.D. Wis. Feb. 1, 2013).

104. Order Granting *Ex Parte* Request for Reconsideration of the United States's Application Under the All Writs Act, In the Matter of the Decryption of a Seized Data Storage System, No. 13-M-449 (E.D. Wis. May 21, 2013).

105. *Id*. at 3.

106. *Id*. at 4.

107. *See* Declan Mccullagh, *Judge: Child Porn Suspect Doesn't Need to Decrypt Files*, CNET (June 4, 2013, 2:30 PM), http://news.cnet.com/8301-13578_3-57587670-38/judge-child-porn-suspect-doesnt-need-to-decrypt-files/.

108. *See id.*

109. *See* Vielmetti, *supra* note 103. For a further discussion of goal-oriented exaggerations of computer users' abilities, see *infra* Part VII.

110. Bruce Vielmetti, *Federal Shutdown Slows Milwaukee Porn Encryption Case, but FBI Busts Silk Road*, MILWAUKEE WISCONSIN JOURNAL SENTINEL (Oct. 3, 2013), http://www.jsonline.com/blogs/news/226206611.html; *see also* Motion to Dismiss Application, *In re* The Decryption of a Seized Data Storage Sys., No. 13-M449 (E.D. Wis. Aug. 16, 2013).

This case would have fallen in the gray area between *Doe* and *Boucher*, though, given the precedent developed prior to this case it would have been surprising if Feldman had not been compelled to decrypt. However, since the relevant issue was resolved without a final ruling on the facts, it remains to been seen how district courts would apply the Eleventh Circuit framework.

V. WHAT ARE THE LESSONS OF THESE DECISIONS?

The divergence in the holdings above seems to rest on a number of implicit and explicit premises which underlie the first three Scenarios set out in Section I. One critical difference between the outcomes in *Boucher* and *Fricosu* on one hand, and in *Doe* on the other, is the amount of information revealed by the defendant. In the former two instances, substantial information was arguably made apparent to the Government through either initial cooperation by Boucher or through tapped telephone conversations, respectively, making the finding of foregone conclusion justified. In the latter case, the Government was left wholly grasping at straws.

More generally, the novel nature of encryption issues seems to leave the courts in search of appropriate analogies as to how to apply the "private papers" doctrine. All documents at issue in these cases are voluntarily created but, if they are produced in the condition in which they are found, would be of no assistance to the fact-finder. Although the foregone conclusion doctrine appears to serve as an efficient mechanism to resolve certain questions relating to encryption, better physical world analogs to the cryptographic process are necessary in order to appropriately balance Fifth Amendment protections with technological advances.

A. The Value of Silence

The decision in *Boucher* was predetermined by, in particular, the border search to which Boucher was subjected and his initial cooperation with the border agents which enabled them to actually locate and identify the nature of the contraband files on his computer.[111] Similarly, although in *Fricosu*, as discussed in Part IV.B, the holding is arguably less clear and perhaps even misapplies *Boucher*, the defendant's intercepted conversation with her ex-husband provided a crucial link to strip Fifth Amendment protections from her act of production. Yet, despite the courts' finding in both

111. *See supra* Part IV.A.

cases that the foregone conclusion doctrine defeated the testimonial aspects of the act of production (i.e., decryption), both defendants were given the benefit of limited immunity for the act of production by the district courts. Implicit in that conclusion is the recognition by the courts of the vestigial testimonial nature of production despite the contrary ultimate findings.[112]

Both the *Boucher* and *Fricosu* decisions illustrate the application of Fifth Amendment principles to Scenarios II and III enumerated above. Contemporaneous knowledge of the contents of encrypted data can be used to defeat an assertion of privilege to the act of production by way of application of the foregone conclusion principle. Although one may quibble with the opaque reasoning of the two cases, the conclusions reached in the two decisions do not appear inconsistent with existing jurisprudence. Ultimately, the amount of actual knowledge required to foreclose the assertion of privilege is unclear and is likely to be determined on a case-by-case basis.

The Eleventh Circuit decision is illustrative of Scenario I and is much better at spelling out its reasoning and providing a seemingly straightforward test for when the foregone conclusion operates to defeat the defendant's exercise of his right against self-incrimination. For the first time at the appellate level, the Eleventh Circuit held that decryption and production of encrypted files is not a physical act of non-testimonial nature, akin to providing a key to a lockbox or a handwriting sample.[113] Although the physical comparisons to digital encryption do seem to be lacking,[114] it certainly is a step in the right direction in recognizing the complexity of the digital age. It remains to be seen how the test would operate under circumstances which are not as clear-cut and straightforward, particularly when the putative defendant may not have been as careful about remaining steadfastly silent.

Additionally, the identity of the owner of the storage media was not really in question in any of the three cases that were resolved with finality. Thus, under the rubric of the foregone conclusion doctrine, the elimination of the testimonial aspect of production indicating to

112. It is particularly notable here that the grant of immunity occurred regardless of the apparent foregone conclusion as to the testimonial aspects of production. *Cf. Doe II*, 465 U.S. 605, 613 (1984) ("Unlike the Court in *Fisher*, we have the explicit finding of the District Court that the act of producing the documents would involve testimonial self-incrimination.").

113. *Doe III*, 670 F.3d 1335, 1346 (11th Cir. 2011).

114. *See* discussion *infra* Part V.B.

whom the hardware belonged was obviously not sufficient, standing alone, to overcome constitutional objections. What was in dispute, particularly in *Doe*, was the Government's knowledge as to the contents or, alternatively, the nature or the existence of the contents themselves. In other words, the focus in *Fricosu* was primarily on the physical location and existence of the potentially incriminating information, which was ascertained from collateral sources, namely, an intercepted phone call. In *Doe*, on the other hand, and likely in future cases dealing with encryption issues, the discussion focused in particular on how the Government can meet its burden of showing with reasonable particularity its "level of knowledge as to the *files* on the hard drives at the time it attempt[s] to compel production."[115] In light of *Hubbell*, such knowledge must have an independent confirmation.[116]

In a way, these cases represent two extremes of the foregone conclusion spectrum. In particular, *Boucher* (and to a lesser extent *Fricosu)* is on one end where location and content are known while *Doe* is on the other end where the content is not known. *Doe* is the classic example of when the foregone conclusion doctrine cannot apply in light of the Government's inability to demonstrate any showing of knowledge of the relevant facts to defeat the defendant's assertion of his Fifth Amendment privilege against self-incrimination.

B. The Nature of Encryption

The *Doe* decision is particularly notable for the fact that the court explicitly recognized that encryption by itself cannot be viewed as an act carrying a bad intent. The court noted that:

> We are not persuaded by the suggestion that simply because the devices were encrypted necessarily means that Doe was trying to hide something. Just as a vault is capable of storing mountains of incriminating documents, that alone does not mean that it contains incriminating documents, or anything at all.[117]

There are numerous private legitimate uses for encryption, ranging from protection against identity theft or data theft to protection of information for personal reasons. In some states, certain businesses are mandated by law to encrypt personal consumer data,

115. *Doe III*, 670 F.3d at 1347 (emphasis in original).

116. *See* United States v. Hubbell, 530 U.S. 29 (2000).

117. *Doe III*, 670 F.3d at 1347.

for example, in Massachusetts and Nevada.[118] Some jurisdictions have even obliquely observed that it may be incumbent upon the legal profession to utilize encryption in order to protect clients' confidences under the rules of professional conduct.[119]

As discussed, Courts faced with the issue of encryption have relied on the Fifth Amendment framework applicable to physical world analogs. As a general matter, courts begin their analysis by consistently holding that the private papers line of cases applies to the underlying unencrypted documents—inasmuch as their initial creation was obviously voluntary—be they tax papers,[120] images of child pornography,[121] or business records.[122] The courts then continue by observing (as the Eleventh Circuit decision has recognized) that the password itself is testimonial in nature, in the way a combination to a safe box is testimonial, refusing to accept the key and lock approach.[123]

Whether encrypted files should be treated similarly to other voluntarily created documents is, however, a question worth

118. Miriam Wugmeister, *New Massachusetts Regulation Requires Encryption of Portable Devices and Comprehensive Data*, MORRISON & FOERSTER (Sept. 23, 2008), http://www.mofo.com/news/updates/bulletins/14495.html.

119. New York City Bar Ass'n, Formal Op. 1994-11 (1994) ("A lawyer should exercise caution when engaging in conversations containing or concerning client confidences or secrets by cellular or cordless telephones or other communication devices readily capable of interception, and should consider taking steps sufficient to ensure the security of such conversations."). In Texas, the Computer and Technology Section of the State Bar recommends that attorneys use encryption software to avoid running afoul of consumer data breach notification laws or ethical requirements of keeping client confidences. Jason Smith, Ron Chichester, & Michael Peck, *Keeping Client Data and Your Law License Secure*, 76 TEX. BAR J. 103, 104 (2013). Given the scienter requirement of Texas's Rule 1.05 relating to confidential information, an attorney may be subject to discipline if he loses an electronic device containing confidential client information or such a device is seized by the government at the border. *Id.* To teach attorneys about encryption, the Computer and Technology Section held a hands-on workshop at the State Bar Annual Meeting, providing attendees with a copy of TrueCrypt and other similar applications. *Id.*

120. United States v. Fisher, 425 U.S. 391, 408-09 (1976) (stating that tax and accounting documents voluntarily created should not ordinarily be protected from disclosure). Although the *Fisher* court punted on the ultimate question of actually overruling *Boyd*, "the papers demanded here are not [the taxpayer's] 'private papers.'" *Id.* at 414.

121. *See, e.g.*, *In re* Boucher, No. 2:06-mj-91, 2009 U.S. Dist. LEXIS 13006 (D. Vt. Feb. 19, 2009); *Doe III*, 670 F.3d 1335 (11th Cir. 2012); *see also* United States v. Pearson, No. 1:04-CR-340, 2006 U.S. Dist. LEXIS 32982 (N.D.N.Y. May 24, 2006).

122. *Doe II*, 465 U.S. 605, 611 (1984).

123. Same situation seems to have played out in other cases where the Government appears to have specifically sought the underlying unencrypted contents rather than the passwords themselves. *See, e.g.*, United States v. Kirschner, No. 09-MC-50872, 2010 U.S. Dist. LEXIS 30603 (E.D. Mich. Mar. 30, 2010).

considering in light of the potential conceptual difference between the creation of the original and the encrypted copy.[124] A number of analogies have been proposed for encryption in this context including encryption as translation, as a safe, as well as a "shredded safe."[125] It has been argued that none of these analogies standing alone prevent compelling of a witness to produce decrypted contents under appropriate circumstances with an appropriately worded subpoena.[126] But these analogies do provide avenues (both for the prosecution and the defense) for arguing when such compelled production rises (or does not rise) to the level of a testimonial act of production requiring both use and derivative use immunity.

1. As Translation

The encryption as translation analogy proposes that an encryption algorithm acts on a document as a process of mechanical translation, turning an original voluntarily created plaintext document into a ciphertext incomprehensible to anyone but the document's creator.[127] Even though the analogy may be unsuccessful inasmuch as the original character of the document arguably remains unchanged (once the decryption algorithm is applied) and all electronic documents by definition require "translation" from their essential nature as 1s and 0s into readable documents by means of hardware/software,[128] it may be useful in conceptualizing when translation can be a testimonial act. As we have seen above, courts have generally accepted that an individual's act of production of an unencrypted document is of a testimonial nature inasmuch as it implicitly acknowledges that the individual is able to "read" the encrypted document, although such testimonial aspects may be defeated by the application of the foregone conclusion doctrine.

This recognition also bears parallel examples in the physical realm. In *U.S. v. Ragauskas*, a deponent invoked his right against self-incrimination "in refusing to translate a document presented to

124. Nathan K. McGregor, *The Weak Protection of Strong Encryption: Passwords, Privacy and Fifth Amendment Privilege*, 12 VAND. J. ENT. & TECH. L. 581, 599 (2010).

125. *Id*. at 600-05.

126. *Id*.; *see also* Philip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171 (1996) (holding plaintext should be treated the same way as ciphertext).

127. Production of the ciphertext (a voluntarily created document itself) would thus be in compliance with a potential subpoena and nothing more would be required.

128. *See* McGregor, *supra* note 124, at 604; *see also* Reitinger, *supra* note 126, at 176 ("[L]egal status of encrypted documents should be no different from any other machine-readable or machine-translatable records.").

him for inspection" as well as in refusing to answer questions pertaining to his activities with the Lithuanian military during World War II, his date of birth, the number of languages he speaks and similar issues.[129] Although the decision leaves a lot to be desired in terms of clarity on this issue, the court held that Ragauskas was entitled to invoke the privilege because information thus obtained could be incriminating as it might "demonstrate that Ragauskas belonged to the Lithuanian military units that allegedly committed atrocities during World War II."[130]

A similar analysis should also apply not only to documents written in a foreign language and a witness's understanding thereof, but documents originally written in code. Contrary to a situation where a document is converted into ciphertext from a plaintext original, compelling a witness to produce a deciphered version of the document would not only be precluded by the Fifth Amendment's protections of an individual's "product of the mind" but also the prohibitions spelled out in *Fisher* and *Hubbell* against compulsory creation of new documents.[131] Further, neither the voluntary nature of the document's creation nor the foregone conclusion doctrine would be applicable in a case like this—whether or not the Government has any independent knowledge as to the individual's ability to understand the cipher or to read a document would generally not have any bearing on its ability to compel the individual to forgo the exercise of his Fifth Amendment privilege. To the extent that an original plaintext document is innocently (yet purposefully) destroyed subsequent to the creation of a ciphertext, similar reasoning should apply.[132]

2. As a Coded Safe or Keyed Lockbox

This analogy posits that encryption acts similarly to placing plaintext documents into a safe locked either by means of a key or a combination.[133] In the Eleventh Circuit decision, the court held that requiring an individual to use a decryption password "is most

129. United States v. Ragauskas, No. 94 C 2325, 1995 U.S. Dist. LEXIS 2313, at *2 (N.D. Ill. Feb. 23, 1995).

130. *Id.* at 11.

131. *See, e.g.*, McGregor, *supra* note 124, at 600 (*citing* Fisher v. United States, 425 U.S. 391, 409 (1976)).

132. Interesting questions may arise—thankfully beyond the scope of the paper—as to what effect mandatory document retention policies or willful destruction of documents has on the issues discussed here.

133. *See* McGregor, *supra* note 124, at 601.

certainly more akin to requiring the production of a combination because both demand the use of the contents of the mind."[134] Moreover, the court recognized that the Government's requests for production or subpoenas in such circumstances are never about the password or key in itself—the ultimate goal is the production of the "files being withheld"—further strengthening the combination analogy.[135]

There is an underlying assumption in this analogy that, as is evidenced by the application of the foregone conclusion principles, the nature of the documents thus locked does not change—the original still remains intact, so to speak, waiting to be unlocked.[136] The conservation of the original document is, however, questionable to the extent that the application of the encryption algorithm transforms the original into incomprehensible ciphertext absent the reversal of the process (with or without the creator's input).[137] The ciphertext can be produced and viewed in tangible form and it is, for all intents and purposes, the only document that exists until mechanical mathematical manipulation is applied to it to make it comprehensible. For example, in *Doe*, in seeking to establish that certain files actually existed on the drive, "the Government introduced an exhibit with nonsensical characters and numbers, which it argued revealed the encrypted form of data that it seeks."[138]

Court decisions to date have stopped their analysis here by simply holding that compelling an individual's use of the contents of his mind to decrypt the contents of the drive and provide the same to Government is a testimonial act (which may or may not be defeated by the foregone conclusion principles). However, that approach may be problematic for constitutional purposes because it arguably fails to recognize the dual physical and mental nature of the act of decryption.

The analogy may also be unsatisfactory (to both proponents and opponents of strong encryption) in its lack of recognition of (1) the differences between mechanically securing content in a safe as compared to cryptographically by encryption, and (2) the essentially unlimited breadth of content which may be stored cryptographically as compared to documents stored within the physical limitations of a

134. *Doe III*, 670 F.3d 1335, 1346 (11th Cir. 2012).

135. *See* McGregor, *supra* note 124, at 601.

136. *Id.*

137. *Id.* at 602 (calling this the "shredded safe analogy").

138. *Doe III*, 670 F.3d at 1340.

coded safe.[139] Law enforcement personnel can always gain access to a coded safe by mechanical means if a defendant fails to comply with a court order to provide combination thereto or even without seeking such compulsion. However, a strongly encrypted drive is often unlikely to be breached without a defendant's cooperation. At the same time, the increasing use of electronically stored information for a variety of licit and illicit purposes creates an incentive to properly secure such data by encryption on the one hand and increases its value to those who seek to gain access to it, on the other. The physical parameters of mechanical safe storage, on the other hand, necessarily limit the exposure of content compelled to be disclosed.

3. Reconceptualizing Decryption

As noted above, if a document is originally written in cipher, an individual cannot be compelled to render it readable even if the Government is in possession of the document so created, since such a request would both require the creation of new documents as well as call for the use of the individual's contents of the mind. To take it one step further, if the original document was handwritten in cipher by means of a simple mathematical function for which simple calculations were done on a computing device (e.g. calculator) the use of a mechanical device should not in theory defeat the above analysis either.[140]

It may be logical to extend this hypothetical to the situation (common today) where the ciphertext documents are created wholly by means of mechanical computing without an individual's involvement in higher level calculations beyond the creation of a passphrase for the software that performs the encryption process. Thus under this rubric, "the decryption and production of the contents of the hard drives" may be equal to creation of a new document rather

139. *See, e.g.*, John E. D. Larkin, *Compelled Production of Encrypted Data*, 14 VAND. J. ENT. & TECH L. 253, 272 (2012).

140. For purposes of this hypothetical, I obviously overlook the lack of complexity of such a cipher and the ease with which the Government can break it, thus rendering any subpoena unnecessary. At the same time, generally speaking, book ciphers (technically defined as codes) may be incapable of being decrypted by an unauthorized third party within a reasonable period of time. SINGH, *supra* note 2, at 31. An early example of a book code in American history dates back to the American Revolution when Benedict Arnold employed the first volume of the Fifth Oxford Edition of Blackstone's Commentaries on the Laws of England to pass coded communications to the British. *See* J. Terrence Stender, *Too Many Secrets: Challenges to the Control of Strong Crypto and the National Security Perspective*, 30 CASE W. RES. J. INT'L L. 287, 300 (1998).

than production of an existing decrypted one.[141] The courts today, however, do not view encryption in such a fashion. Instead the mental process of decryption has no significance beyond that of a non-testimonial physical act with possible testimonial implications.

It may be that reconceptualizing decryption is unnecessary in light of the Eleventh Circuit's careful application of the foregone conclusion doctrine. Further, to date, in every precedent referenced herein, when the Government sought grand jury subpoenas or writs for production of the contents of encrypted drives, the courts always acknowledged in their findings that the Government's attempts to decrypt the contents had been unsuccessful.[142] Such observations may serve as a tacit understanding that the testimonial aspects of acts of production are greater than they seem. On the other hand, such grants of immunity may be simply a rote application of precedent without any deeper meaning and thus open to further re-evaluation, particularly when law enforcement need so indicates. Regardless, a more protective stance on compelled decryption does not leave the Government without any tools to proceed. A grant of immunity pursuant to 18 U.S.C. Section 6002 would invalidate any constitutional objections to an order to decrypt. Failure to disclose after a grant of immunity can lead to an imposition of civil and criminal sanctions.

VI. COMPELLED PRODUCTION OF ILLEGAL CONTENTS

In both *Hubbell* and *Fisher*, the Supreme Court dealt with the issue of compulsion in connection with documents that, in and of themselves, were not unlawful to possess. For example, in *Fisher*, the documents in question were retained copies of individual tax returns as well as accountants' work papers pertaining to the returns;[143] in *Hubbell*, the produced documents were various financial documents from which the charging prosecutor later gleaned various tax

141. Should the ability to compel depend on the form of the original document *ab initio*? If a document is created by being typed on a computer, but it is not saved as plaintext and instead saved automatically in encrypted form, is there a plaintext document at all?

142. *See, e.g.*, United States v. Fricosu, 841 F. Supp. 2d 1232, 1234 (D. Colo. 2012) ("[A]gents have been unable to decrypt it."); *In re* Boucher, No. 2:06-mj-91, 2009 U.S. Dist. LEXIS 13006, at *5-6 (D. Vt. Feb. 19, 2009) ("The government is not able to open the encrypted files without knowing the password. In order to gain access to the Z drive, the government is using an automated system which attempts to guess the password, a process that could take years."); *Doe III*, 670 F.3d at 1339 ("The grand jury subpoena issued because the forensic examiners were unable to view the encrypted portions of the drives.").

143. Fisher v. United States, 425 U.S. 391, 394 (1976).

crimes.[144] Neither case dealt specifically with documents the possession of which alone constitutes a crime. Nor have any cases tackled directly a situation where a defendant's compelled decryption lead to the discovery of evidence relating to unrelated criminal acts.[145]

Courts are likely to be faced with situations where they are required to compel putative defendants to decrypt contents when the individual stands accused of crimes of possession, for example, child pornography, pirated media content, and the like. Under current precedent, such evidence (whether encrypted or not) is likely voluntarily created and thus is not entitled to self-incrimination protections absent testimonial act of production characteristics.[146] Similarly, as per Scenario IV above, use of evidence which was gleaned from compelled decryption of data, portions of which turn out to be relevant for prosecution of unrelated criminal acts (i.e., the existence of which was not a foregone conclusion), would not be foreclosed by the application of the Fifth Amendment privilege. They are likely to be deemed discovered in "plain view". Whether recent developments in Fourth Amendment jurisprudence will or should preclude such evidence being used in the prosecution of unrelated offenses is discussed below in Part VIII.

But, in such a case, the compelled production of unencrypted contents may be reasonably likened to Hubbell's assembly and production of specifically designated categories of documents "where the prosecutor needed respondent's assistance both to identify potential sources of information and to produce those sources" rather than a mere act of non-testimonial act of production.[147] And, as seen above in Parts II and III, none of the cases dealing with compelled decryption have involved the Government seeking the issuance of a *subpoena duces tecum* or a writ as a primary investigative tool without first attempting to decrypt the data on its own. Such an act of production would have greater testimonial significance than in cases involving business records or tax records which are in and of

144. United States v. Hubbell, 530 U.S. 27, 32 (2000).

145. The extent to which the *Boucher* decision contemplated the plain view exception is a debatable issue. *See In re Boucher*, 2009 U.S. Dist. LEXIS 13006, at *8 ("Second Circuit precedent, however, does not require that the government be aware of the incriminatory *contents* of the files; it requires the government to demonstrate with reasonable particularity that it knows of the existence and location of subpoenaed documents." (emphasis in original)).

146. See McGregor, *supra* note 124, at 605-08, for discussion as well as logical difficulties in giving greater protection to encrypted contraband as opposed to encrypted documentary evidence such as dairies.

147. *Hubbell*, 530 U.S. at 41.

themselves not criminal to possess and whose creation may be required by the relevant law.[148]

In fact, some precedent is available to support this stricter proposition. Ordinarily, production of physical evidence is not testimonial in nature—a defendant may be compelled to produce a blood sample or a handwriting sample, to put on a shirt, or to participate in a line up.[149] But, under certain circumstances, such compelled production may carry significant testimonial aspects and greater Fifth Amendment concerns.

In *People v. Havrish*, the Court of Appeals of the State of New York held that a defendant's production of an unlicensed handgun which led to his prosecution for possession of same was privileged under the Fifth Amendment.[150] The defendant was originally charged with unrelated crimes of assault and kidnapping among others.[151] As a condition of the bail, the defendant was required to "[s]urrender any and all firearms owned or possessed."[152] He complied with the order, surrendering a number of long guns as well as a pistol which was later confirmed to be unlicensed.[153] As a result, the defendant was subsequently charged with a criminal possession misdemeanor.[154]

In holding that the defendant's act of production was testimonial and incriminating in nature, and thus was subject to the application of the privilege against self-incrimination, the court ruled out the application of the foregone conclusion doctrine.[155] The defendant's act of production was the sole confirmation of the handgun's existence and possession of same by the defendant.[156] The court observed that "[b]efore defendant revealed that he had possessed a revolver [pursuant to court order] neither the court nor the police were aware that defendant owned a handgun."[157] Furthermore, the production was in itself incriminating inasmuch as "by the time defendant produced the weapon, he had provided the police with

148. See Shapiro v. United States, 335 U.S. 1 (1948), for a discussion of the required records exception to the Fifth Amendment privilege.

149. *Fisher*, 425 U.S. at 408 (collecting cases).

150. People v. Havrish, 8 N.Y.3d 389, 397 (2007). Of note here, however, is the automatic application of the privilege under New York state law.

151. *Id.* at 391.

152. *Id.*

153. *Id.*

154. *Id.*

155. *Id.* at 395.

156. *Havrish*, 8 N.Y.3d at 395.

157. *Id.*

proof of virtually every element of the offense of criminal possession of a weapon."[158] As a result, the handgun's suppression "was warranted in the weapon possession prosecution" and "the suppression of this evidence necessitated the dismissal of the accusatory instrument."[159]

VII. THE DANGERS OF REACTIONARY OVERREACTION

The difficulties in separating the testimonial aspects of the act of production from the non-testimonial aspects require courts to approach such situations without a predisposition against a defendant who chooses to engage in lawful conduct of encrypting his or her data.[160] As argued by Paul Ohm, such a person should not be viewed as a mythical "Superuser" who wanders the digital highways with anonymous destructive impunity; courts should be wary of accepting the Government's insinuations in that regard as well.[161] Although "the Fifth Amendment would not be violated by the fact alone that the papers on their face might incriminate the taxpayer, for the privilege protects a person only against being incriminated by his own compelled testimonial communications,"[162] the testimonial character of acts of production lack clarity and requires fact-intensive examination on a case-by-case basis. Of note here is the concurrence by Justice Thomas in *Hubbell*, which noted that *Fisher* has introduced "difficult parsing of the act of responding to a subpoena *duces tecum*."[163]

Lowering the hurdles to cover self-incrimination issues with respect to encryption would result in an imprudent disconnect between the treatment of physical and digital evidence.[164] Law

158. *Id.* at 396.

159. *Id.* at 397.

160. The consequences of a refusal to comply with a subsequently determined incorrect order can be particularly dire. For example, in *Doe III*, the witness spent about 8 months in jail for civil contempt before the 11th Circuit ordered his release after hearing Doe's oral argument on appeal. *Doe III*, 670 F.3d at 1340 n.12.

161. Paul Ohm, *The Myth of the Superuser: Fear, Risk and Harm Online*, 41 U.C. DAVIS L. REV. 1327, 1333-35 (2008). The article also discusses the investigatory breadth already possessed by the state with respect to virtually warrantless Internet surveillance. *Id.* at 1352.

162. *Fisher*, 425 U.S. at 409 (questioning the expansive "private papers" doctrine established by *Boyd*).

163. *Hubbell*, 530 U.S. at 56.

164. *See, e.g.*, Ohm, *supra* note 161, at 1353-54. *Contra* Andrew Ungberg, Note, *Protecting Privacy through a Responsible Decryption Policy*, 22 HARV. J.L. & TECH 537 (2009) (calling for a separate approach to decryption which requires special particularized warrant requirements and a circumscribed use of the plain view exception).

enforcement personnel are constantly confronted with facts the discovery of which is impossible without self-incriminating compulsion, for example, the location of a murder weapon or other document or object necessary to prosecute a particular defendant. Yet, in such situations, an individual may not be compelled to disclose the location of such evidence despite law enforcement's inability to locate or identify the same. To force a suspect to decrypt data in the absence of strong indications of foregone conclusion places digital evidence on lesser footing than physical evidence at a time when evidence (in the form of information) is increasingly stored electronically and more crimes relate to use or misuse of electronically stored information. To the extent that data is encrypted by means resulting in "plausible deniability," compelled decryption without significant indicia of the foregone conclusion principle would be an obvious violation of the right against self-incrimination.[165] Similarly, to treat physically encrypted evidence memorialized in fixed form differently from evidence encrypted electronically, does not make much sense.

Further, the effect encryption has on the investigative function should not be overestimated. While encryption may make certain information inaccessible in a specific instance, it does not prevent law enforcement personnel from engaging in the multitude of other investigative techniques available to them. For example, law enforcement has a relatively free hand in conducting Internet surveillance without notice to the investigative target.[166] Similarly, cell tracking, which includes both caller location and text message content, is conducted without the involvement of the target through subpoena and non-subpoena requests to cellphone carriers.[167] In 2011 alone, the number of such requests totaled over 1.3 million.[168] As information is increasingly communicated wirelessly, this relationship is bound to get more intrusive.[169] Further, since a grant of use and derivative use immunity legally overcomes any self-incrimination concerns, it still remains one of the most powerful tools available to

165. Such a method of encryption was involved in *Doe III*. *See* discussion *supra* Part III.

166. Ohm, *supra* note 161, at 1353-54.

167. Eric Lichtblau, *Wireless Firms are Flooded with Requests to Aid Surveillance*, N.Y. TIMES, July 9, 2012, at A1.

168. *Id*.

169. The recent disclosures of surveillance capabilities of the U.S. intelligence community, although thankfully beyond the scope of this paper, further illustrate the vulnerability of electronic data of all kind.

overcome constitutional objections to decryption.[170] The perceived threat posed by encryption to the investigative function should not be used as a pretext to criminalize previously innocent behavior or to limit constitutional protections.

In light of the novelty of encryption issues and the lack of precise mapping to existing precedent and physical world parallels, courts should tread very carefully in this arena and find an appropriate non-reactionary balance between protecting individual rights and privileges on the one hand, and law enforcement needs on the other. It remains to be seen whether the foregone conclusion principles as clarified in *Doe* are sufficient in this regard, particularly because of the relative simplicity of the facts therein as well as the arguably broader testimonial characteristics implicit in relevant acts of production relating to encrypted documents as discussed above.

VIII. FOURTH AMENDMENT RAMIFICATIONS

A similar conflict is currently developing under the rubric of the Fourth Amendment with respect to the plain view exception and search and seizure of electronically stored information (ESI). The resemblance between the challenges of compelled decryption and discovery of unrelated incriminating evidence and seizure of electronically stored information and discovery of same requires a closer examination of the underlying principles behind the Fourth Amendment protections and the recent developments in the issuance of search warrants relating to ESI. Ultimately, I propose that a stronger protective stance under the Fourth Amendment but not under the Fifth Amendment would be an untenable outcome leading to an inappropriate equilibrium between individual rights and state power.

A. Overview of Relevant Jurisprudence

The Fourth Amendment speaks to the prohibitions on searches and seizures and sets forth the basic requirements of probable cause and particularity in the issuance of warrants and the extent of searches and seizures conducted pursuant thereto. It states that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,

170. To the extent that a court order does not result in the target's disclosure of the unencrypted contents, it will, of course, result in a criminal contempt order and, subsequently, a civil contempt order. *See, e.g.*, *In re* Grand Jury Witness Chanie Weiss, 703 F.2d 653 (2d Cir. 1983). The situation is no different than any other court order requiring an individual to testify, who, subsequently, refuses to do so.

> 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.[171]

Although simple on its face, the Fourth Amendment jurisprudence is not a model of judicial clarity.[172] For example, the developed standard of "reasonable expectation of privacy" is employed to determine whether a particular state action constitutes a "search."[173] This doctrine's application witnesses a spectrum of seemingly related exceptions and case-by-case rules. One of the relevant exceptions to the warrant requirement relevant to the analysis here is the "plain view" exception. As set forth in *Horton v. California*, the exception applies to situations where (1) law enforcement personnel is present lawfully at the place where evidence can be viewed (e.g., a valid search warrant), (2) law enforcement personnel must have "lawful right of access" to the object itself, and (3) the incriminating nature of the evidence must be "immediately apparent."[174] As a corollary, in the course of a lawful search, law enforcement personnel is not permitted to manipulate an object to bring it into plain view or to make the objects incriminating character apparent.[175]

B. ESI Implications

With the explosion of electronically stored information, the "plain view" exception now faces a wholly unprecedented doctrinal challenge of self-definition. Unlike a search of physical objects and spaces, the enormous storage capacity of a computer makes such searches "extraordinarily invasive."[176] A lawful seizure and search of

171. U.S. CONST. amend. IV.

172. *Cf.* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 479 (2011) (collecting rules and proposing that the Fourth Amendment jurisprudence is an on-going re-calibration of technological advances and law enforcement needs).

173. Katz v. United States, 389 U.S. 347, 359 (1967) (Harlan, J., concurring).

174. Horton v. California, 496 U.S. 128, 136 (1990). The court logically observed that "[i]f an article is already in plain view, neither its observation nor its seizure would involve any invasion of privacy." *Id.* at 133. Doctrinally, the plain view exception speaks more appropriately to seizures rather than searches. *Id.*

175. Arizona v. Hicks, 480 U.S. 321 (1987) (reviewing an exigent circumstances search for weapons where a police officer turned over stereo equipment to check serial numbers). *See also* Matthew Dodovich, Note, *The Plain View Doctrine Strikes Out in Digital File Searches*, 6 I/S J.L. & POL'Y FOR INFO. SOC'Y 659, 664 (2011).

176. *See, e.g.*, Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA.

storage media, for example, hard drives, back-up drives, and the like, puts into play any evidence thus discovered whether or not the evidence was specified in the search warrant or wholly unrelated to the crime investigated arguably through the operation of the plain view doctrine.[177] In fact, judges usually issue extremely broad warrants relating to computer data, spurred on by tales of cyber-criminals' unparalleled abilities.[178] Yet, at the same time, such a broad sweep of the plain view doctrine may cut against the particularity requirement of the Fourth Amendment for warrants to specify "the place to be searched and the . . . things to be seized."[179] Additionally, files stored on electronic media cannot be considered in "plain view" in the traditional sense of the term—they must be manipulated in order to reveal their nature.[180]

To mitigate the severity of the outcome, a number of courts have imposed *ex ante* restrictions on computer searches conducted pursuant to a warrant, including conditions limiting the seizure of computer itself, conditions which impose time limits on the electronic search, conditions on how the electronic search must be conducted, including search terms and data segregation, and lastly, conditions on the return of seized hardware.[181] For example, in *United States v. Comprehensive Drug Testing*,[182] after a previous final and then withdrawn decision which made certain *ex ante* restrictions mandatory, the Ninth Circuit set forth a list of suggested guidelines to be used by magistrate judges in determining the reasonableness of a warrant for electronic data. Among the guidelines were the need to insist on government's waiver of reliance on the plain view doctrine with regard to digital evidence, the use of search protocols and the use of specialized non-investigative personnel to search the seized media.[183] On the other hand, a few courts have approached the problem on an *ex post* basis, deciding the reasonableness of a

L. REV. 1241, 1255 (2010).

177. *Id.*

178. Ohm, *supra* note 161, at 1354.

179. For discussion of issues in application of the plain view doctrine to electronic searches that do not exist with physical searches, see Andy Boulton, *E-Discovery Rules and the Plain View Doctrine: The Scylla and Charybdis of Electronic Document Retention*, 37 J. CORP. L. 435 (2012).

180. *Id.* at 444-45.

181. *See generally* Kerr, *supra* note 176.

182. United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009) (*en banc*).

183. *See* Kerr, *supra* note 176, at 1257. For an in-depth discussion of the case, see Dodovich, *supra* note 175, at 665-78.

conducted search on a case-by-case basis.[184]

Orin S. Kerr has suggested that unrestrained *ex ante* regulation of search warrants is inadvisable and impedes development of proper constitutional outcomes.[185] Others have proposed that searches and seizures of electronic media are conceptually no different than search and seizures of physical property and thus no special oversight is necessary in this realm.[186] On the other side of the debate, proponents argue that such limitations provide a necessary backstop to government overreach and the devolution of narrow warrants into general ones.[187]

What is relevant for the purposes of self-incriminating compulsion under the Fifth Amendment is the potential divergence in the protections provided by the Fourth and Fifth Amendments, resulting in an outcome where certain evidence, which would otherwise not be reachable by the operation of a warrant's particularity and probable cause requirements, could still be obtained through self-incrimination by the operation of the foregone conclusion principles.

First, on balance, the operation of the plain view doctrine in conjunction with the particularity and reasonableness requirements of the Fourth Amendment is much better in tempering the dangers of pretextual searches or fishing expeditions with respect to physical objects.[188] Although the subjective intent of the search is generally not examined by the courts, the particularity requirements limit the type of evidence that may be discovered in "plain view" as the police can only look "in places and containers large enough to contain the specific physical evidence sought."[189] As a result, a search of physical evidence is considered unlikely to result in a general search prohibited by the Fourth Amendment, even if the probable cause for a warrant issued was related to a criminal act that was ultimately not the object of the search.[190]

Digital searches, on the other hand, are more susceptible to

184. *See, e.g.*, United States v. Richards, 659 F.3d 527 (6th Cir. 2011).

185. Kerr, *supra* note 176, at 1277.

186. Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 BERKELEY J. CRIM. L. 112 (2011).

187. Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. IN BRIEF 1 (2011).

188. Orin S. Kerr, *Searches and Seizures in the Digital World*, 119 HARV. L. REV. 531, 577 (2005) (discussing the need to re-evaluate the plain view doctrine in digital searches).

189. *Id.* at 568.

190. *Id.*

government abuses and involve an increasing generality of the search itself. Today, computers store a wealth of information by and about the user with and without the user's input or (sometimes) consent.[191] Absent an *ex ante* limitation on the mechanics of the search, a warrant for computer hardware necessarily subjects the whole universe on the storage media to the search. A warrantless seizure, conducted without any judicial oversight whatsoever, is even more invasive.[192] At the same time, given the virtually limitless capacity of storage media available to the average consumer, a pretextual search sufficiently grounded in probable cause relating to a minor offense (undoubtedly present on many a computer) is virtually guaranteed to bring to the surface not only evidence of criminal wrongdoing but other potentially incriminating or impeaching material that in itself does not constitute a criminal act.[193]

The foregone conclusion jurisprudence under the Fifth Amendment should be mindful of the developments with respect to the plain view doctrine and *ex ante* restrictions relating to digital searches. Lesser protections can not only create new avenues for law enforcement overreach, but are also likely to turn every defendant into a compelled self-informant as use of encryption becomes more widespread to secure increasing volumes of digitally stored personal information.

CONCLUSION

In today's digital world, more and more criminal prosecutions involve dealing with electronic data. The occurrence of electronic data as evidence is not limited to the white collar crime sphere and can be found in the prosecution of traditional street crime as well. Encryption poses a great challenge to the law enforcement function because it makes electronic evidence qualitatively different from physical tangible evidence, and at times, essentially impossible to analyze. At the same time, physical tangible evidence may be actually replaced solely by electronic evidence—so that assigning fewer constitutional protections to the latter could greatly affect the balance of individual rights in criminal prosecutions.

On the other hand, encryption is becoming standard operating procedure by individuals, white collar professionals and corporations

191. Ohm, *supra* note 187, at 6-7 (discussing the proliferation of data stored not only on users' personal computers but also with third parties).

192. *See* Kerr, *supra* note 188, at 569.

193. *Id.* at 582.

for legitimate personal and business reasons. In considering encryption issues, the courts should be mindful not only of the challenges that encryption presents to law enforcement, but also of the unintended consequences of creating rules that can greatly affect individual constitutional rights and protections. Simply demonizing those who choose to use encryption and creating rules to eliminate the effects of encryption on law investigative capabilities, overlooks the realities of today's digital world.

The precedent to date has not been particularly instructive as to how the principles of the Fifth Amendment privilege against self-incrimination will apply to encryption in the gray area in the middle. As the case law reads today, I would argue that it should not matter what kind of encryption program is used and the exact algorithm it applies to, for example, file space versus blank space, or how it operates to hide or otherwise make apparent the use of encryption on a particular device. Under *Doe*, the focus appears to be on the government's independent minimum knowledge of the encrypted contents, which may be obtained not only through a putative defendant's cooperation, but also through advanced wiretapping and eavesdropping as well as more traditional human asset techniques. Under that approach, current jurisprudence leaves a lot of discretion to the courts in determining when a particular act of production rises to the level of a constitutionally protected testimonial deed. It is thus incumbent upon the courts to understand not only how encryption works but also how important and pervasive electronic data has become in today's society. The Supreme Court has already heard cases relating to technological possibilities of electronic tracking and how such technology affects the balance established by the Fourth Amendment.[194] Perhaps, in this technological era, the next challenge in the Fifth Amendment arena will come from a petitioner in a case dealing with encryption issues who heeds the call of Justice Thomas in *Hubbell*, where he concluded his concurrence with the following observation:

> None of the parties in this case has asked us to depart from *Fisher*, but in light of the historical evidence that the Self-Incrimination Clause may have a broader reach than *Fisher* holds, I remain open to a reconsideration of that decision and its progeny in a proper case.[195]

194. *See* Jones v. United States, 132 S. Ct. 945 (2012).

195. United States v. Hubbell, 530 U.S. 27, 56 (2000) (Thomas, J., dissenting).