RETHINKING THE APPLICATION OF THE FIFTH AMENDMENT TO PASSWORDS AND ENCRYPTION IN THE AGE OF CLOUD COMPUTING

JOSHUA A. ENGEL*

I. INTRODUCTION

The Fifth Amendment privilege against self-incrimination protects a person from being compelled to provide a testimonial communication that is incriminating in nature.[1] In a number of cases starting to wind through state and federal courts, the government has sought to compel suspects and defendants to provide passwords and encryption keys despite claims of Fifth Amendment Privilege by witnesses and suspects. For example, in a Colorado case, the government sought to compel the defendant to enter a password into a laptop or otherwise provide access to encrypted data stored on her computer.[2] The government apparently believed that the encrypted

* Vice President and General Counsel, Lycurgus Group, LLC. J.D. *cum laude* Harvard University 1995, B.A. *magna cum laude* University of Pennsylvania 1992.

1. The Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." U.S. CONST. amend. V. *See* Maness v. Meyers, 419 U.S. 449, 461 (1975) (noting that the Fifth Amendment protects an individual from being compelled "to produce evidence which may later be used against him as an accused in a criminal action" (citing Arndstein v. McCarth, 254 U.S. 71, 72-73 (1920); Counselman v. Hitchcok, 142 U.S. 547, 562 (1892))); Schmerber v. California, 384 U.S. 757, 761 (1966) (holding that the Fifth Amendment grants persons the privilege not to "provide the State with evidence of a testimonial or communicative nature").

2. United States v. Fricosu, No. 10-cr-00509-REB-02, 2012 U.S. Dist. LEXIS 11083, at *6 (D. Colo. Jan. 23, 2012). *See also* Gov't's Reply to Amicus Curiae Brief

computer files contained evidence of fraudulent real estate transactions.[3]

Encryption means the process by which a person changes plain, understandable information into unreadable letters and numbers using a mathematical algorithm.[4] Encrypted data is accessible only through the use of a password or encryption key.[5] The use of encryption technology by consumers has grown in recent years; computer and software manufacturers consider disk encryption a basic computer security measure and include disk encryption tools as a standard feature on most new computers.[6]

Recent cases have focused on information stored on portable devices such as cell phones or computers.[7] Because these devices are easy to steal or lose, consumers commonly use passwords to limit access to the devices, and encryption to prevent any unauthorized users from accessing sensitive data.

The government may gain access to password protected electronic devices and encrypted data through a number of legal means. In many cases, the government may have seized the electronic devices after executing a search warrant. In other cases, the government may have conducted a warrantless search of password protected electronic

at 3-4, *Fricosu*, 2012 U.S. Dist. LEXIS 11083 (No. 10-cr-00509-REB), ECF No. 177.

3. Application Under the All Writs Act Requiring Defendant Fricosu to Assist in the Execution of Previously Issued Search Warrants at 4-5, *Fricosu*, 2012 U.S. Dist. LEXIS 11083 (No. 10-cr-00509), No. 111 [hereinafter *Application Under All Writs Act*].

4. *Protecting Data by Using EFS to Encrypt Hard Drives*, MICROSOFT, technet.microsoft.com/en-us/library/cc875821.aspx (last visited May 15, 2012).

5. *Id*.

6. Apple includes encryption features in the most recent version of Mac OS. *See Disk Utility*, APPLE, http://www.apple.com/macosx/apps/all.html (last visited May 15, 2012). Windows 7 also includes encryption capability. *See Help Protect Your Files Using BitLocker Drive Encryption*, MICROSOFT, http://windows.microsoft.com/en-US/windows7/Help-protect-your-files-using-Bitlocker-Drive-Encryption (last visited May 15, 2012). Consumers are also more likely to begin to encrypt files stored on third party storage systems instead of relying upon encryption provided by the service. Dropbox, a popular online storage system, claimed that all files stored by users were encrypted by the service. However, the service held the encryption key and could turn over nonencrypted files to the government in response to a subpoena. Ryan Singel, *Dropbox Lied to Users About Data Security*, WIRED (May 13, 2011, 4:54 PM), http://www.wired.com/threatlevel/2011/05/dropbox-ftc/.

7. *See, e.g.*, People v. Diaz, 244 P.3d 501, 511 (Cal. 2011); *Fricosu*, 2012 U.S. Dist. LEXIS 11083, at * 1.

devices and encrypted data under an applicable exception to the Fourth Amendment's warrant requirement.[8] Most recently, the third party service providers received subpoenas from law enforcement or private entities to provide information stored for users by the third party service providers.[9]

This article addresses the question of whether the Fifth Amendment prevents the government from forcing a witness to provide a password or encryption key to permit access to digital files.[10] The Fifth Amendment generally protects citizens from being compelled to give incriminating testimony.[11] The privilege extends not only to "answers that would in themselves support a conviction," but also includes statements "which would furnish a link in the chain of evidence" needed by the prosecution.[12]

The question of whether passwords and encryption keys are covered by the Fifth Amendment privilege against self-incrimination

8. *See* Joshua A. Engel, *Doctrinal Collapse: Smart Phones Cause Courts to Reconsider Fourth Amendment Searches of Electronic Devices*, 41 U. MEM. L. REV. 233, 253 (2010) (noting that cell phones may be lawfully seized and the contents searched without a warrant under the search incident to arrest doctrine).

9. *See, e.g.*, Application for a Search Warrant at 4, *In re Search of Yahoo! Inc*., No. 1:10-sw-05056-MEH (D. Colo. Jan. 25, 2010); *See also* Matthew Perpetua, *RIAA Targets Cloud-Storage Company Box.net*, ROLLING STONE (May 20, 2011, 12:55 PM), http://www.rollingstone.com/music/news/riaa-targets-cloud-storage-company-box-net-20110520 (noting that Recording Industry Association of America filed legal action against Box.net, a company that provides cloud-based storage for businesses, with the allegation that its users have been pirating music and requesting a subpoena to investigate specific users believed to be abusing the service by hosting pre-release music files); Kevin Poulsen, *Spam Suspect Uses Google Docs; FBI Happy*, WIRED (Apr. 16, 2010, 3:20 PM), http://www.wired.com/threatlevel/2010/04/cloud-warrant (noting that this "appears to be the first publicly acknowledged search warrant benefiting from a suspect's reliance on cloud computing").

10. The Fifth Amendment protects persons against prosecution of particular crimes without indictment, double-jeopardy, self-incrimination, and the deprivation of life, liberty or property without due process. U.S. CONST. amend. V. *See, e.g.*, Chavez v. Martinez, 538 U.S. 760, 770 (2003); McKune v. Lile, 536 U.S. 24, 35 (2002).

11. *See* United States v. Hubbell, 530 U.S. 27, 34 (2000); Lefkowitz v. Turley, 414 U.S. 70, 77 (1973) (citing McCarthy v. Arndstein, 266 U.S. 34, 40 (1924)).

12. Hoffman v. United States, 341 U.S. 479, 486 (1951) (citing Blau v. United States, 340 U.S. 159, 161 (1950)). *See also* Doe v. United States, 487 U.S. 201, 212 (1988) (noting that the protection that the Fifth Amendment provides "reflects 'a judgment…that the prosecution should [not] be free to build up a criminal case, in whole or in part, with the assistance of enforced *disclosures* by the accused' ") (alteration in original) (quoting Ullmann v. United States, 350 U.S. 422, 427 (1956)).

turns on courts' views of the nature of this information. The privilege against self-incrimination is limited to "testimonial" evidence, or evidence that, explicitly or implicitly, provides or discloses information.[13] The privilege does not apply to physical evidence, such as fingerprints or blood samples.[14]

This issue has appeared infrequently in courts. The few courts to address this issue have generally concluded that the provision of a password on encryption key is testimonial because the provision of this information is essentially an admission that the person had possession and control over, and access to, the computer, files, or data.[15] Yet this is not the end of the analysis. Some of the early publications concerning this issue suggested that circumstances where suspects will successfully raise Fifth Amendment challenges to government efforts to compel the production of passwords and encryption keys were likely to be "rare."[16] A significant basis for this hypothesis was that, in many cases, production of the incrimination evidence would be exempt from Fifth Amendment protections under the foregone conclusion doctrine. Under the foregone conclusion doctrine, the provision of information is not subject to the Fifth Amendment privilege against self-incrimination when the existence and location of information are known to the government, and the act of providing the evidence adds little or nothing to the government's case.[17]

The foregone conclusion doctrine has been applied in limited instances to encrypted files stored on laptops and personal computers.[18] However, recent changes in the technological landscape suggest that this issue is likely to become more prevalent in future litigation. The use of cloud computing services to store documents and images has

13. *Doe*, 487 U.S. at 209-10.

14. Pennsylvania v. Muniz, 496 U.S. 582, 589, 591 (1990) (citing Schmeber v. California, 384 U.S. 757, 764 (1966)) (noting a defendant may be compelled to appear in a lineup, speak aloud for purposes of identification, and give blood for analysis).

15. *See infra* notes 73-76 and accompanying text.

16. *See* Adam M. Gershowitz, *Password Protected? Can a Password Save Your Cell Phone From the Search Incident to Arrest*, 96 IOWA L. REV. 1125, 1174-75 (2011) (explaining that because of the dynamics of police interrogations, successful Fifth Amendment challenges along these lines will be rare). Professor Gershowitz also notes that many suspects are likely to voluntarily provide the password without compulsion. *Id*. at 1175.

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

18. *See infra* notes 128-31 and accompanying text.

grown significantly. Users of cloud services are less likely to actually save images and documents on handheld or personal devices but, instead, use handheld or personal devices to access images and documents saved on remote computers.[19] In those situations, the possession of an encryption key or password may become important in order for the government to show ownership or access to records, websites or communications. As a result, suspects and defendants may be successful in arguing that the foregone conclusion doctrine does not make the privilege against self-incrimination inapplicable.

II. FIFTH AMENDMENT

A. *BACKGROUND AND NATURE OF THE PRIVILEGE*

The Fifth Amendment privilege against self-incrimination protects a person from being compelled to provide a testimonial communication that is incriminating in nature.[20] The privilege protects a person from being called to testify against himself at his own trial and permits him to refuse to "answer official questions put to him in any other proceeding, civil or criminal, formal or informal, where the answers might incriminate him in future criminal proceedings."[21] The

19. *See, e.g.*, WAYNE JANSEN & TIMOTHY GRANCE, NAT'L INST. OF STANDARDS AND TECH., U.S. DEP'T OF COMMERCE, SPECIAL PUB. NO. 800-144, GUIDELINES ON SECURITY AND PRIVACY IN PUBLIC CLOUD COMPUTING 39-40 (2011) *available at* http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf (noting growth of public cloud computing services along with possible security vulnerabilities); *Capturing the Cloud: Strategy for Service Providers*, ALCATEL-LUCENT, http://www.alcatel-lucent.com/new-thinking/market-growth/Capturing-The-Cloud.pdf (noting that the total value of cloud services will grow from approximately $68 billion in 2010 to almost $150 billion in 2014).

20. The Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." U.S. CONST. amend. V. *See also* Maness v. Meyers, 419 U.S. 449, 461 (1975) (noting that the Fifth Amendment protects an individual from being compelled "to produce evidence which may later be used against him as an accused in a criminal action" (citing Arndstein v. McCarth, 254 U.S. 71, 72-73 (1920); Counselman v. Hitchock, 142 U.S. 547, 562 (1892))); Schmerber v. California, 384 U.S. 757, 761 (1966) (holding that the Fifth Amendment grants persons the privilege not to "provide the State with evidence of a testimonial or communicative nature").

21. Minnesota v. Murphy, 465 U.S. 420, 426 (1984) (quoting Lefkowitz v. Turley, 414 U.S. 70, 77 (1973)). The Fifth Amendment right against self-incrimination is not a self-executing right. McKune v. Lile, 536 U.S. 24, 65 n.10. (2002) (citing Roberts v. United States, 445 U.S. 552, 559 (1980)). Rather, a person who wishes the protections

protections provided by the Fifth Amendment "reflects 'a judgment . . . that the prosecution should [not] be free to build up a criminal case, in whole or in part, with the assistance of enforced *disclosures* by the accused.' "[22]

The Fifth Amendment is not unlimited, however. The Self-Incrimination Clause "prohibits only compelled testimony that is incriminating."[23] A claim of Fifth Amendment privilege must be based on a fear of prosecution that is "real and appreciable, with reference to the ordinary operation of law in the ordinary course of things; not a danger of an imaginary and unsubstantial character, having reference to some extraordinary and barely possible contingency, so improbable that no reasonable man would suffer it to influence his conduct."[24] Thus, the scope of the Self-Incrimination

---

of the Fifth Amendment "must assert the privilege rather than answer if he desires not to incriminate himself." *Murphy*, 465 U.S. at 429. Professor Gershowitz has suggested that, for this reason, litigation on this issue may be rare because many suspects or defendant may freely provide the requested information. He explains:

> [M]ost arrestees will never be in a position to assert a self-incrimination claim because they will have revealed the password voluntarily. If police simply ask, rather than demand, that an arrestee enter the password to his phone and he consents, there is no compulsion and hence no Fifth Amendment violation. As explained above, while police should be obligated to read an arrestee his *Miranda* warnings before requesting his password, in reality, the warnings provide virtually no protection because individuals typically waive them.

Gershowitz, *supra* note 16, at 1172. However, Professor Gershowitz may not give sufficient credit to the knowledge of defendants and suspects of criminal procedure. One court has noted that while

> [t]he intricacies of who may assert the privilege, when it may be asserted, and what constitutes a testimonial act is probably completely lost on the public. . . . The right to remain silent and to plead the Fifth at trial or before the grand jury is well known throughout our case law and culture.

United States v. Swanson, 635 F.3d 995, 1007-08 (7th Cir. 2011). *See also* Joshua A. Engel, *Frequent Fliers at the Court: The Supreme Court Begins to Take the Experience of Criminal Defendants into Account in* Miranda *Cases*, 7 SETON HALL CIRCUIT REV. 303, 338 (2011) (noting that suspects who are familiar with the criminal justice system are "more likely to make an uncoerced choice to waive *Miranda*" and provide a statement).

22. Doe v. United States, 487 U.S. 201, 212 (1988) (alteration in original) (quoting Ullmann v. United States, 350 U.S. 422, 427 (1965)).

23. Hiibel v. Sixth Judicial Dist. Court of Nev., 542 U.S. 177, 189-90 (2004) (citing Brown v. Walker, 161 U.S. 591, 598 (1896) (noting that where "the answer of the witness will not directly show his infamy, but only tend to disgrace him, he is bound to answer")).

24. *Brown*, 161 U.S. at 599-600 (quoting Queen v. Boyes, 1 B. & S. 311, 330 (Q. B.

Clause is broadly available to prevent any compelled disclosure that may later be used against the witness or suspect in a criminal prosecution.[25] The Self-Incrimination Clause of the Fifth Amendment does not, however, grant a blanket privilege to ward off any and all efforts by government authorities to obtain information.[26] Rather, a suspect or defendant may only assert the privilege with respect to specific questions or requests for the production of documents or other evidence.[27]

In order to qualify for the Fifth Amendment privilege, a communication "must be testimonial, incriminating, and compelled."[28] A testimonial communication "must itself, explicitly or implicitly, relate a factual assertion or disclose information."[29] This generally is understood to exclude from the protections afforded by the Fifth Amendment compelled acts that, while leading to the discovery of incriminating evidence, do not themselves make incriminating factual assertions.[30]

1861)). *See also* Kastigar v. United States, 406 U.S. 441, 445 (1972).

25. *Maness*, 419 U.S. at 461 (citing *Aronstein*, 254 U.S. at 72-73; *Counselman*, 142 U.S. at 198). "The privilege afforded not only extends to answers that would in themselves support a conviction under a federal criminal statute but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant for a federal crime." Hoffman v. United States, 341 U.S. 479, 486 (1951) (citing Blau v. United States, 340 U.S. 159, 161 (1950)). Claims of Fifth Amendment privilege demand that a reviewing court make inferences about the potential consequences of disclosure. The Supreme Court has not noted clear lines of demarcation to determine definitively what is or is not within the scope of the Self-Incrimination Clause. Rather, a court "must be governed as much by [its] personal perception of the peculiarities of the case as by the facts actually in evidence." *Id.* at 487 (quoting *Ex parte* Irvine, 74 F. 954, 960 (C.C.S.D. Ohio 1896)). A party asserting the privilege bears the burden of justifying any reliance on the Self-Incrimination Clause. United States v. Sharp, 920 F.2d 1167, 1170-71 (4th Cir. 1990).

26. United States v. Rodriquez, 706 F.2d 31, 37 (2d Cir. 1983).

27. *Id*.

28. *Hiibel*, 542 U.S. at 189.

29. *Id*. (quoting Doe v. United States, 487 U.S. 201, 210 (1988) ("[I]n order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a 'witness' against himself.")).

30. *See, e.g*., Pennsylvania v. Muniz, 496 U.S. 582, 602-03 (1990) (responding to a field sobriety test); South Dakota v. Neville, 459 U.S. 553, 564 (1983) (taking a Breathalyzer test); United States v. Wade, 388 U.S. 218, 222-23 (1967) (providing a voice exemplar); Gilbert v. California, 388 U.S. 263, 266-67 (1967) (providing a handwriting exemplar); Schmerber v. California, 384 U.S. 757, 765 (1966) (providing

The act of exhibiting physical characteristics is not the same as a statement communication by a witness that relates either express or implied assertions of fact or belief.[31] Thus, for example, in *Schmerber*, the Court upheld against a Self-Incrimination Clause claim the compelled provision of a blood sample on the grounds that "compulsion which makes a suspect or accused the source of 'real or physical evidence' [generally] does not violate [the Fifth Amendment]."[32] The Court explained that it is a "settled proposition that a person may be required to produce specific documents even though they contain incriminating assertions of fact or belief because the creation of those documents was not 'compelled' within the meaning of the privilege."[33]

B. *PROVIDING A PASSWORD OR ENCRYPTION KEY IS TESTIMONIAL*

Providing a password or an encryption key is most likely to be viewed by courts as testimonial. Passwords and encryption keys are likely to be possessed solely within the mind of the suspect and must be communicated verbally, placing them squarely within the Fifth Amendment's traditional protections.

In *United States v. Doe*, the Court had held that "[t]he vast majority of verbal statements . . . will be testimonial."[34] The Court explained: "Whenever a suspect is asked for a response requiring him to communicate an express or implied assertion of fact or belief, the suspect confronts the 'trilemma' of truth, falsity, or silence, and hence the response (whether based on truth or falsity) contains a testimonial component."[35] However, in *Pennsylvania v. Muniz*, the Court expanded on this idea in a way that suggests that written statements could also fall within the privilege.[36]

In *Muniz*, the defendant was suspected of driving while intoxicated.[37] The defendant appeared to have been drinking and, after

a blood sample); Holt v. United States, 218 U.S. 245, 252-53 (1910) (donning a blouse worn by perpetrator).

31. *Muniz*, 496 U.S. at 594-98 (citing *Doe*, 487 U.S. at 210).
32. *Schmerber*, 384 U.S. at 764.
33. United States v. Hubbell, 530 U.S. 27, 35-36 (2000).
34. *Doe*, 487 U.S. at 213-14.
35. *Muniz*, 496 U.S. at 597.
36. *Id*. at 598.
37. *Id*. at 585.

performing poorly on field sobriety tests, was arrested.[38] The relevant question before the Court was whether the defendant's statements during the booking process were testimonial and, therefore, subject to Fifth Amendment protections.[39] In particular, the defendant was asked to provide certain identifying information, such as his name, address, height, weight, eye color, date of birth, current age, and the date of his sixth birthday.[40] The Court held that the descriptions of the defendant's speech as slurred were, although incriminating, not testimonial.[41] The Court believed that the physical characteristics of the speech were similar to other physical characteristics—such as fingerprints or voice or handwriting exemplars—that are not testimonial.[42] The Court explained that physical evidence is not testimonial even when it could only be produced "through some volitional act on the part of the suspect."[43] However, the substance of the defendant's answers—and in particular incorrect answers about his birthday—were held to be testimonial.[44]

The Court rejected the idea that the information provided was evidence of a physical fact (in this case, intoxication).[45] When the defendant was asked about his birthday, he was confronted "with the

38. *Id*. During booking, the defendant struggled to provide his address and age. *Id*. at 586. An officer then asked the Defendant, " 'Do you know what the date was of your sixth birthday?' After Muniz offered an inaudible reply, the officer repeated, 'When you turned six years old, do you remember what the date was?' Muniz responded, 'No, I don't.' " *Id*. While re-performing the field sobriety tests, the defendant "attempted to explain his difficulties in performing the various tasks, and often requested further clarification of the tasks he was to perform." *Id*. (quoting Commonwealth v. Muniz, 547 A.2d 419, 423 (1988)).

39. The Fifth Amendment was implicated because the defendant had not been provided with *Miranda* warnings. *Id*. at 589-90 (citing Miranda v. Arizona, 384 U.S. 436, 444 (1966) (holding that the privilege against self-incrimination during pretrial questioning requires application of special procedural safeguards)).

40. *Id*. at 590 (noting that "[b]oth the delivery and content of Muniz's answers were incriminating").

41. *Id*. at 590-91.

42. *Id*. at 591 (citing Schmeber v. California, 384 U.S. 757, 764 (1966)).

43. *Id*. at 591-92 (citing United States v. Wade, 388 U.S. 218, 222-23 (1967) (presence and speech by a defendant at a lineup was not testimonial)); *see also* United States v. Dionisio, 410 U.S. 1, 7 (1973) (voice exemplar not testimonial); Gilbert v. California, 388 U.S. 263, 266 (1967) (provision of handwriting exemplar not testimonial).

44. *Muniz*, 496 U.S. at 600.

45. *Id*. at 602-03.

choice of incriminating himself by admitting that he did not then know the date . . . or answering untruthfully by reporting a date that he did not then believe to be accurate."[46] The Court focused on the manner in which the evidence was obtained, explaining that the Fifth Amendment protections include evidence obtained in a manner that entails a testimonial act on the part of the suspect.[47] In other words, testimonial statements include the "the contents of his own mind," and communications "written, oral or otherwise" that reveal "consciousness" of facts.[48]

The significance of the *Muniz* decision is found in the observation that the contents of a truthful statement could support a factual inference.[49] This observation essentially decouples the idea that a testimonial statement must be oral. Instead, the question is whether the provision of the information could support an incriminating factual inference. In *Muniz,* the factual inference was that the defendant was or was not under the influence.[50] In regards to the question about whether the provision of a password or an encryption key is testimonial, the question becomes whether a factual inference can be drawn as a result of the provision of the password or the encryption key—regardless of whether the password or encryption key is provided in an oral or written form. In most situations, the factual inference will be ownership or possession of files found on a computer.[51]

---

46. *Id*. at 599.

47. *Id*. at 590-91.

48. *Id*. at 594 (quoting Curcio v. United States, 354 U.S. 118, 128 (1957); Doe v. United States, 487 U.S. 201, 211 (1988) (citing 8 JOHN HENRY WIGMORE, WIGMORE ON EVIDENCE § 2265, at 386 (McNaughton Rev. 1961))).

49. *Id*. at 599.

50. *Id*. at 584.

51. Many commentators continue to tie the conception of what is testimonial under the Fifth Amendment to oral testimony. Professor Brenner, in her cyb3rcrim3 blog, described the Supreme Court cases as follows:

> The Supreme Court has held, basically, that you're giving testimony—testifying—when you're communicating, i.e., when you're revealing your knowledge of certain facts or sharing your thoughts or opinions with the government. *U.S. v. Kirschner*, *supra*. You can't claim the 5th Amendment privilege to refuse to surrender physical evidence such as your blood, hair or saliva; it only applies to communications, i.e., to something that look [sic] like what a witness does when she takes the stand at trial.

Susan Brenner, *Passwords and the 5th Amendment Privilege*, CYB3RCRIM3 (Apr. 28, 2010) http://cyb3rcrim3.blogspot.com/2010/04/passwords-and-5th-amendment-privilege.html (referencing United States v. Kirschner, No. 09-MC-50872, 2010 WL

The question of whether the provision of a computer password can provide the basis of a factual inference was addressed in a case involving child pornography discovered at a border stop.[52] In *United States v. Rogozin* the defendant was stopped by Department of Homeland Security personnel while entering the United States.[53] Because of some suspicious behavior, customs officers detained the defendant for further questioning.[54] As part of the inspection of the defendant's belongings, an officer observed photos of small children in sexually suggestive positions on a digital camera.[55] Agents later observed other alleged child pornography on the defendant's computer.[56] The agents asked the defendant for the password to his computer.[57] The defendant complied.[58]

The Immigration and Customs Enforcement ("ICE") agents in *Rogozin* seized the computer and later conducted a forensic review of the data on the hard drive.[59] As a result of this review, child pornography was discovered and the defendant was subsequently indicted on federal child pornography charges.[60] The defendant sought to suppress his statement providing the password to the computer because he was not provided with *Miranda* warnings.[61] The issue

1257355 (E.D. Mich. Mar. 30, 2010)).

52. United States v. Rogozin, No. 09-CR-379, 2010 WL 4628520, at *6 (W.D.N.Y Nov. 16, 2010).

53. *Id*. at *1.

54. *Id*.

55. *Id*. at *1-2.

56. *Id*. at *2. The Magistrate Judge believed that the warrantless search of the laptop was permissible as a border search. *Id*. at *3-4. The Magistrate cited to opinions permitting routine searches of the contents of a computer at a border without reasonable suspicion. *Id*. at *3 (citing United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008); United States v. Ickes, 393 F.3d 501, 506 (4th Cir. 2005)). Moreover, even if not part of a routine search, the search of the computer was found to be supported by reasonable suspicion because of the defendant's furtive behavior. *Id*.

57. *Id*. at *2.

58. *Id*.

59. *Id*.

60. *Id*.

61. *Id*. at *5. The Court established in *Miranda* a set of "procedural safeguards that require police to advise criminal suspects of their rights under the Fifth and Fourteenth Amendments before commencing custodial interrogation." Florida v. Powell, 130 S. Ct. 1195, 1203 (2010) (quoting Duckworth v. Eagan, 492 U.S. 195, 201 (1989)). The Supreme Court originally defined custodial interrogation as "questioning initiated by law enforcement officers after a person has been taken into custody or otherwise

relevant to this paper is whether the provision of a password would be incriminating.[62] The government argued that *Miranda* warnings were not required during the questioning because such warnings "are not required where a person is questioned in a routine border crossing inquiry."[63] However, the Magistrate rejected this argument, finding that the questioning as to who had access to the computer and the password was designed to obtain incriminating evidence concerning the possession of the child pornography.[64]

A similar issue was presented in *United States v. Kirschner.*[65] In *Kirschner,* the defendant had been indicted on child pornography charges.[66] The prosecution issued a grand jury subpoena to the defendant seeking all passwords used or associated with his computer.[67] The prosecution claimed that the evidence obtained may not be used to support the current indictments, but instead, may be used as part of an effort to discover more incriminating evidence on the defendant's computer.[68]

The defendant in *Kirschner* refused to testify about the passwords based on the privilege established by the Self-Incrimination Clause.[69] The district court, relying on *Hubbell*, agreed that the privilege

deprived of his freedom of action in any significant way." Miranda v. Arizona, 384 U.S. 436, 444 (1966).

62. *Rogozin*, 2010 WL 4628520 at *5.

63. *Id*.

64. *Id*. at *5-6. *See also* United States v. Kirschner, No. 09-MC-50872, 2010 WL 1257355, at *3 (E.D. Mich. Mar. 30, 2010) ("[F]orcing the Defendant to reveal the password for the computer communicates that factual assertion to the government, and thus, is testimonial-it requires Defendant to communicate 'knowledge,' unlike the production of a handwriting sample or a voice exemplar." (citing United States v. Doe, 487 U.S. 201, 217 (1988))).

65. *Kircshner*, 2010 WL 1257355, at *1.

66. *Id*.

67. *Id*.

68. *Id*. The government stated during argument that the request for passwords was to investigate indictment evidence of child pornography potentially contained in encrypted files on the same computer that contained the files, which led to the child pornography charges in the case. *Id.* In other words, the subpoena related to the same computer that provided the evidence for the existing charges, and likely the same type of criminal behavior. While this does not bear on the Fifth Amendment issues, it is important for procedural reasons, as the use of grand jury subpoenas to gather evidence for use in cases in which indictments have already issued is usually improper.

69. *Id*. at *3.

applied.[70] In reaching this conclusion, the district court found that "requiring the Defendant to provide the password is a testimonial communication."[71] The district court reasoned that the government was not seeking documents or objects; rather, the government was seeking testimony from the defendant, which would require the defendant "to divulge through his mental processes his password—that will be used to incriminate him."[72]

The conclusion in *Kirschner*—that providing a password is testimonial[73]—is likely correct and consistent with existing Supreme Court precedent. The reasoning may not, however, be complete. The *Kirschner* court seemed to suggest that the provision of a password is testimonial because the password is contained within the mind of the witness.[74] This analysis is limited because it would fail to distinguish, for example, between a password that is maintained in the mind of the witness, and a password stored on a piece of paper. Instead, whether the provision of a password is testimonial should turn on whether the government can access the information in the absence of the password or encryption key.

The better analysis is the analysis supported by *Muniz*. That analysis was based on the idea that the act of providing a password or encryption key is testimonial because not only is it an admission of the possession of, or access to the documents and further allows the government to identify and authenticate the files, but because without the information the information is not accessible to the government at all.[75] Unlike true physical evidence, such as blood samples or handwriting exemplars, encryption keys and passwords render the files

70. *Id*. (relying on United States v. Hubbell, 530 U.S. 27, 38 (2000)).

71. *Id*. According to the opinion, the Assistant U.S. Attorney described the requested testimony in these terms: "It's like giving the combination to a safe." *Id.* It is unclear why the government made this concession. "The assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox." *Id*. at *4 (quoting *Hubbell*, 530 U.S. at 43).

72. *Id*. (noting the government did not attempt to compel the testimony after providing the defendant with immunity).

73. *Id*. at *3-4.

74. *Id*. This view has been suggested by other observers. For example, in a blog post about this decision, Professor Susan Brenner wrote, "The Supreme Court has held, basically, that you're giving testimony—testifying—when you're communicating, i.e., when you're revealing your knowledge of certain facts or sharing your thoughts or opinions with the government." Brenner, *supra* note 51.

75. Pennsylvania v. Muniz, 496 U.S. 582, 590 (1990).

readable and thus usable by the government.[76]

C. *PROVIDING A PASSWORD OR ENCRYPTION KEY IS INCRIMINATING.*

The provision of a password or encryption key by itself would likely not trigger Fifth Amendment protections because the password or encryption key, by itself, is not incriminating.[77] However, because the information could lead to the discovery or production of further incriminating evidence, providing of the password or encryption key could trigger the privilege.[78] In other words, if by providing law enforcement with a password or encryption key a witness is admitting that the password-protected or encrypted documents exist, are in his possession or control, or are authentic, then the provision of the password or encryption key may be considered to be testimonial. This matches the rationale for the act-of-production doctrine detailed by the Supreme Court in *Fisher v. United States*.[79]

76. *See* Andrew J. Ungberg, Note, *Protecting Privacy Through a Responsible Decryption Policy*, 22 HARV. J. L. & TECH. 537, 548 (2009).

77. *See* Gershowitz, *supra* note 16, at 1168. *See also supra* notes 73-74 and accompany text (discussing United States v. Kirschner) and *infra* notes 136-141 and accompany text (discussing *In re* Boucher).

78. *Cf*. United States v. Sweets, 526 F.3d 122, 127-28 (4th Cir. 2007) (providing the location of a person—"producing the person"—was not testimonial because it merely acknowledged that the suspect (1) knew the other person or (2) that he knew the other person's location); United States v. Hunerlach, 197 F.3d 1059, 1066 (11th Cir. 1999) (noting that the signing of a waiver authorizing the release of bank records is not necessarily a testimonial communication protected by the Fifth Amendment). In some cases, the Court has drawn an arbitrary distinction between information contained in written form and information contained in the head of a suspect. *See* Doe v. United States, 487 U.S. 201, 210 n.9 (1988) (noting that being required to turn over the key to a safe is not testimonial, but being forced to provide a memorized combination would be testimonial). This distinction is arbitrary in that if a person saves a password or encryption key in a written format, then the information could be considered non-testimonial. This distinction may not be as relevant in present times, when people commonly use programs to store passwords to websites or documents. For example, the iPhone App Store contains dozens of apps specifically designed to store and manage passwords. *See, e.g.*, Arnold Zafra, *Top Password Managers for iPhone*, BRIGHT HUB, http://www.brighthub.com/mobile/iphone/articles/66880.aspx (last updated Oct. 18, 2011).

79. *See generally* Fisher v. United States, 425 U.S. 391 (1976). In *Fisher*, the Court recognized that although "[t]he Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence," it does apply "when the accused is compelled to make a *testimonial* communication that is incriminating." *Id*. at 392.

In *Fisher*, Internal Revenue agents were conducting investigations of possible criminal violations of the tax laws.[80] The taxpayers who were the subjects of the investigations obtained certain relevant documents from their accountants and gave the documents to their attorneys.[81] The IRS agents attempted, through the use of subpoenas, to compel the production of the documents.[82] The attorneys refused to provide the documents on various grounds, including that compelling production of the records would violate the taxpayers' privilege against self incrimination as guaranteed by the Fifth Amendment.[83]

The *Fisher* Court initially held that the Fifth Amendment was inapplicable under these facts because the privilege against Self-Incrimination Clause was not violated by compelling the clients' attorneys to produce records in their possession.[84] This is because, the Court reasoned, the "the Fifth Amendment is limited to prohibiting the use of 'physical or moral compulsion' exerted on the person asserting the privilege." [85] Thus, because the attorneys, and not the taxpayers, were compelled to produce the records, the Fifth Amendment would not protect against the production of the documents "whether or not the Amendment would have barred a subpoena directing the taxpayer to produce the documents while they were in his hands."[86] The Court, however, acknowledged the practical concerns this rule presented, as "each taxpayer transferred possession of the documents in question from himself to his attorney in order to obtain legal assistance in the tax investigations in question."[87] Accordingly, because the attorney-client privilege protected this transfer, the Court determined that "the papers, if unobtainable by summons from the client, are unobtainable by summons directed to the attorney by reason of the attorney-client

80. *Id*. at 393-94.

81. *Id*. at 394.

82. *Id*.

83. *Id*. at 395. Other grounds to prevent the production of the document—including attorney-client privilege, accountant-client privilege, and Fourth Amendment issues—were also initially asserted. None of these issues were addressed by the Supreme Court. *See id.*

84. *Id*. at 397.

85. *Id*. (citing Couch v. United States, 409 U.S. 322, 336 (1973); Perlman v. United States, 247 U.S. 7, 15 (1918); Johnson v. United States, 228 U.S. 457, 458 (1913)).

86. *Id*. at 397.

87. *Id*. at 405.

privilege."[88]

The *Fisher* Court's analysis of the Fifth Amendment issues began with the 1886 decision in *Boyd v. United States*.[89] In *Boyd*, the government sought to compel the production of an invoice for a shipment of glass in order to support a claim that the importers were committing a fraud in regards to a tax exemption.[90] The Court held that the production of the records was barred not only by the Self-incrimination Clause, but by the Fourth Amendment.[91] The Court said, "a compulsory production of the private books and papers of the owner of goods sought to be forfeited . . . is compelling him to be a witness against himself, within the meaning of the fifth amendment to the constitution."[92] The *Fisher* Court noted that the *Boyd* decision had been interpreted to mean that "the seizure, under warrant or otherwise, of any purely evidentiary materials violated the Fourth Amendment and that the Fifth Amendment rendered these seized materials inadmissible."[93] However, the Court observed that "[s]everal of Boyd's express or implicit declarations have not stood the test of time."[94]

The *Fisher* Court instead adopted a more modern view of the Self-Incrimination Clause: "the Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a *testimonial* communication that is incriminating."[95] This interpretation leads to a secondary question: what is a testimonial

88. *Id*.

89. *Id*. (citing Boyd v. United States, 116 U.S. 616, 634-35 (1886)).

90. *Boyd*, 116 U.S. at 617.

91. *Id*. at 634-35.

92. *Id*.

93. *Fisher*, 425 U.S. at 407 (citing United States v. Lefkowitz, 285 U.S. 452, 467 (1932); Agnello v. United States, 269 U.S. 20, 33-34 (1925); Gouled v. United States, 255 U.S. 298, 307 (1921)).

94. *Id*.

95. *Id*. at 408. *See also* Gilbert v. California, 388 U.S. 263, 266-67 (1967) (holding that the Fifth Amendment not applicable to the provision of handwriting exemplars); United States v. Wade, 388 U.S. 218, 222-23 (1967) (holding that the Fifth Amendment not applicable to the provision of voice exemplars); Schmerber v. California, 384 U.S. 757, 763-65 (1966) (holding that the Fifth Amendment not applicable to the provision of blood samples); Holt v. United States, 218 U.S. 245, 252-53 (1910) (holding that the Fifth Amendment not applicable to the donning of a blouse worn by the perpetrator).

communication? In *Fisher*, the Court determined that the tax and accounting documents were not testimonial because no "oral testimony" was required and the taxpayer was not required to "restate, repeat, or affirm the truth of the contents of the documents."[96] Accordingly, the Court determined that the Fifth Amendment was not applicable.[97]

The Supreme Court again considered this issue in *United States v. Doe*.[98] *Doe* involved a federal grand jury investigation of corruption in the awarding of county and municipal contracts.[99] Grand jury subpoenas were served on the owner of a business involved in the investigation.[100] The subpoenas sought various business records, including phone and bank records and a list of "virtually all the business records" of one company.[101] The Court refused to limit the subpoenas on the grounds that the production of business records always violated the Fifth Amendment rights of the business owner.[102] The Court said, "the Fifth Amendment protects the person asserting the privilege only from *compelled* self-incrimination. Where the preparation of business records is voluntary, no compulsion is present."[103]

The *Doe* Court went on to consider the situation described in *Fisher* in which, "the contents of a document may not be privileged, [but] the act of producing the document may be [privileged]."[104] In *Doe*, unlike in *Fisher*, the trial court made an "explicit finding . . . that the act of producing the documents would involve testimonial self-incrimination."[105] The Court rejected an argument by the government

96. *Fisher*, 425 U.S. at 409.

97. *Id*. The *Fisher* decision acknowledged the possibility that the act of producing evidence "has communicative aspects of its own, wholly aside from the contents of the papers produced." *Id.* at 410.

98. United States v. Doe, 465 U.S. 605, 610-14 (1984).

99. *Id*. at 606.

100. *Id*.

101. *Id*. at 606-07.

102. *Id*. at 610-11.

103. *Id*. (citing Fisher v. United States, 425 U.S. 391, 396 (1976)). Justice O'Connor wrote a concurring opinion "just to make explicit what is implicit in the analysis of [the majority] opinion: that the Fifth Amendment provides absolutely no protection for the contents of private papers of any kind." *Id*. at 618 (O'Connor, J., concurring).

104. *Id*. at 612-13.

105. *Id*. at 613.

that the production of the records would provide only minimal evidence of possession.[106] The Court noted that the business owner "did not concede . . . that the records listed in the subpoena actually existed or were in his possession."[107] Significantly, the Court left the door open for the government to argue that the foregone conclusion doctrine rendered any Fifth Amendment claim inapplicable in future cases: "This is not to say that the Government was foreclosed from rebutting respondent's claim by producing evidence that possession, existence, and authentication were a 'foregone conclusion.' In this case, however, the Government failed to make such a showing."[108]

In *United States v. Hubbell,* the Supreme Court considered a prosecution by the Independent Counsel appointed to investigate possible violations of federal law relating to the Whitewater Development Corporation. [109] The Independent Counsel had served the defendant with a subpoena *duces tecum* calling for the production of eleven categories of documents before a grand jury.[110] The defendant refused to provide the documents or even to acknowledge possession of the documents, citing his Fifth Amendment privilege against self-incrimination.[111] The Independent Counsel then obtained an order to compel production from the district court, and the defendant complied; the contents of the documents "provided the Independent Counsel with the information that led to [the defendant's

106. *Id*. at 614 n.13.

107. *Id*.

108. *Id*. (quoting *Fisher*, 425 U.S. at 411). The government conceded that the only available route to compel the production would have been to grant immunity to the business owner. *Id.* at 614-15. The Court declined to adopt a judicially constructed "doctrine of constructive use immunity" which would have prohibited the government from using "the incriminatory aspects of the act of production against the person claiming the privilege even though the statutory [immunity] procedures have not been followed." *Id*. at 616.

The Court's decision in *Hubbell* picks up on the intersection between the foregone conclusion doctrine and a grant of immunity issue presented in *Doe*. United States v. Hubbell, 530 U.S. 27, 44-45 (2000). In *Hubbell*, the Government argued that the act of producing records was not testimonial because of the foregone conclusion doctrine established in *Fisher*. *Id*. at 44. The Court in *Hubbell* declined to further clarify the reach of the doctrine, noting that "[w]hatever the scope of this 'foregone conclusion' rationale, the facts of this case plainly fall outside of it." *Id.*

109. *Hubbell*, 530 U.S. at 30.

110. *Id*. at 31.

111. *Id*.

indictment]."[112]

The issue before the Court in *Hubbell* concerned a problem presented by the fact that by producing documents a witness is admitting that papers exist, are in the witness's possession or control, and are authentic.[113] In other words, by producing the records—and answering questions about the act of production before a grand jury or other body—a witness may be compelled to communicate information about the existence, custody, and authenticity of the documents. Thus, in *Hubbell*, the Court was forced to address "[w]hether the constitutional privilege protects the answers to such questions, or protects the act of production itself, [regardless of] . . . whether the unprotected contents of the documents themselves are incriminating."[114]

The government in *Hubbell* claimed that there was no "need to introduce any of the documents produced by [the defendant] into evidence in order to prove the charges against him."[115] Nonetheless, the Court found that the government intended to make a "derivative use of the testimonial aspect of [the act of production] in obtaining the indictment against [the defendant] and in preparing its case for trial."[116] Moreover, the Independent Counsel "needed [the defendant's] assistance both to identify potential sources of information and to produce those sources."[117] Accordingly, the act of producing the documents was testimonial and eligible for the protections of the Self-Incrimination Clause:

> It is abundantly clear that the testimonial aspect of [defendant's] act of producing subpoenaed documents was the first step in a chain of evidence that led to this prosecution. The documents did

112. *Id*. The district court dismissed the indictment, in part, because the Independent Counsel had used the documents in violation of a grant of immunity. *Id*. at 31-32. The District Court also noted characterized the subpoena as "the quintessential fishing expedition." *Id*. at 32 (quoting United States v. Hubbell, 11 F. Supp. 2d 25, 37 (D.D.C. 1998).

113. *Id*. at 35-37.

114. *Id*. at 37. Much of the discussion in *Hubbell* concerns the grant of immunity, and whether the prosecution is barred by this grant. *See id*. at 38-41. This aspect of the decision will not be discussed so that the focus can remain on the Fifth Amendment issues.

115. *Id*. at 41.

116. *Id*. (internal quotation marks omitted).

117. *Id*.

> not magically appear in the prosecutor's office like "manna from heaven." They arrived there only after [the defendant was compelled to produce the records after he] asserted his constitutional privilege. . . .[118]

Hubbell, thus, stands for the proposition that the constitutional privilege against self-incrimination protects a witness "from being compelled to answer questions designed to elicit information about the existence of sources of potentially incriminating evidence."[119] The act of providing the records was testimonial because witnesses must provide the contents of their own minds to produce, identify, and authenticate the records. The Court reasoned that the production was more "like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox."[120]

III. FOREGONE CONCLUSION DOCTRINE

The *Fisher* decision acknowledged the possibility that the act of producing evidence "has communicative aspects of its own, wholly aside from the contents of the papers produced."[121] However, the Court did not take this concern very seriously. The Court dismissed the argument that the act of production could be testimonial, stating that "[i]t is doubtful that implicitly admitting the existence and possession of the papers rises to the level of testimony within the protection of the Fifth Amendment."[122] The Court, instead, created what has since been termed the "foregone conclusion" doctrine by suggesting that the Fifth Amendment might be inapplicable because "the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers . . . 'The question is not of testimony but of surrender.' "[123]

The foregone conclusion doctrine has been applied when the existence and location of documents under subpoena are independently

118. *Id*. at 42.

119. *Id*. at 43.

120. *Id*. at 43-44 (citing Doe v. United States, 487 U.S. 201, 210 n.9 (1988)).

121. Fisher v. United States, 425 U.S. 391, 410 (1976). The Court appeared to dodge the question, stating that "[t]hese questions perhaps do not lend themselves to categorical answers; their resolution may instead depend on the facts and circumstances of particular cases or classes thereof." *Id*.

122. *Id*. at 411.

123. *Id*. (quoting in part *In re* Harris, 221 U.S. 274, 279 (1911)).

established and the "question is not of testimony but of surrender."[124] In order the take advantage of the doctrine, the government must establish three elements: the existence of the material; the authenticity of the material; and the target's possession or control of the documents.[125] This can be accomplished, for example, by having the records independently authenticated.[126] In determining whether the government has met its burdens, reviewing courts must look to the information possessed by the government prior to the issuance of the subpoenas—in other words, the "quantum of information possessed by the government before it issued the relevant subpoena."[127]

A number of courts have, citing the foregone conclusion doctrine, permitted the government to compel the production of passwords and encryption keys.[128] For example, in a child pornography prosecution, the government was able to successfully argue that evidence that the suspect was able to provide a password and an encryption key was unnecessary in order for the government to obtain a conviction and, therefore, not subject to Fifth Amendment protections.[129] This

124. *Id*. (quoting *In re Harris*, 221 U.S. at 279).

125. *See* United States v. Bright, 596 F.3d 683, 693 (9th Cir. 2010); *In re* Grand Jury Proceedings, Subpoenas for Documents, 41 F.3d 377, 380 (8th Cir. 1994) (citing United States v. Rue, 819 F.2d 1488, 1493 n.4 (8th Cir. 1987)).

126. *See, e.g.*, United States v. Sand, 541 F.2d 1370, 1376-77 (9th Cir. 1976) (authenticating records by an independent bank official).

127. United States v. Hubbell, 167 F.3d 552, 569 (D.C. Cir. 1999). *See also Rue*, 819 F.2d at 1493 ("The relevant date on which existence and possession of the documents must be shown is the date on which the [subpoena] is served, for it is at that time that the rights and obligations of the parties become fixed.").

128. *See* United States v. Gavegnano, 305 F. App'x 954, 956 (4th Cir. 2009) (permitting government to compel production of password where "self-incriminating testimony that [the suspect] may have provided by revealing the password was already a 'foregone conclusion' because the Government independently proved that [the suspect] was the sole user and possessor of the computer"). *See also In re* Boucher, No. 2:06-mj-91, 2007 U.S. Dist. LEXIS 87951, at *16 (D. Vt. Nov. 29, 2007) (refusing to compel suspect to provide password, noting that the "foregone conclusion doctrine does not apply to the production of non-physical evidence, existing only in a suspect's mind where the act of production can be used against him"), *rev'd*, 2009 U.S. Dist. LEXIS 13006, at *10 (D. Vt. Feb. 19, 2009) (noting that provision of encryption key was subject to foregone conclusion doctrine because the government could "link [the suspect] with the files on his computer without making use of [the suspect's] production of an unencrypted version").

129. United States v. Pearson, No. 1:04-CR-340, 2006 U.S. Dist. LEXIS 32982, at *58-59 (N.D.N.Y May 24, 2006) ("[T]he existence and use of encryption software on the files recovered from Defendant is all but a forgone conclusion, and knowledge of

supports the argument that there will be few efforts to prevent law enforcement from compelling the production of passwords and encryption keys.

The foregone conclusion doctrine was applied to the provision of a password for an encrypted laptop in *In re Grand Jury Subpoena to Sebastian Boucher.*[130] In *Boucher,* ICE agents seized a laptop from the defendants as he attempted to enter the United States.[131] An initial review of the computer revealed approximately 40,000 images, many of which appeared to be child pornography.[132] An ICE agent attempted to access a file named, "2yo getting raped during diaper change," but was unable to open it because of the encryption.[133] The government obtained a warrant to search the contents laptop, but a computer forensics expert also could not access the data because of encryption.[134] The government then sought a grand jury subpoena compelling the defendant to produce any passwords associated with the laptop.[135]

The defendant in *Boucher* sought to quash the subpoena on the grounds that compelling him to provide the password would violate his Fifth Amendment rights.[136] The government essentially conceded that the provision of the password would be testimonial, but argued that the Fifth Amendment was inapplicable because of the forgone conclusion doctrine.[137] A magistrate judge had concluded that the foregone conclusion rationale did not apply because the government was not aware of the contents of the files that allegedly contained pornographic images.[138] However, the court rejected this approach holding that the government does not need to be aware of the incriminatory contents of

the actual password adds little to what the Government already knows in this regard.").

130. *In re Boucher*, 2009 U.S. Dist. LEXIS 13006, at *2-9.

131. *Id*. at *4-5.

132. *Id*. at *4. The defendant was provided *Miranda* warnings prior to an interview. *Id*. at *4-5. The defendant admitted that he downloaded pornographic files, but claimed to delete any images of child pornography. *Id*. at *5. The defendant permitted the ICE agent to view some files that appeared to contain child pornography. *Id*.

133. *Id*. at *4.

134. *Id*. at *5.

135. *Id*. at *1. The government later changed its approach, arguing only that the defendant should be compelled to provide the contents of the encrypted hard drive in an unencrypted format. *Id*. at *1-2.

136. *Id*. at *2.

137. *Id*. at *9-10.

138. *Id*. at *8.

the files but only must show that it knows of the "existence and location of subpoenaed documents."[139] In applying this doctrine to the facts of *Boucher*, the court found that because the defendant showed an ICE agent viewed the contents of some of the hard drive, the "[g]overnment thus knows of the existence and location of the [hard] drive and its files. Again providing access to the unencrypted [hard] drive 'adds little or nothing to the sum total of the Government's information' about the existence and location of files that may contain incriminating information."[140]

The court further explained:

> [The Defendant's] act of producing an unencrypted version of the [hard] drive likewise is not necessary to authenticate it. He has already admitted to possession of the computer, and provided the Government with access to the [hard] drive. . . . [The Defendant has no] privilege to refuse to provide the grand jury with an unencrypted version of the [hard] drive of his computer. . . .[141]

The approach of the *Boucher* court was followed in *United States v. Fricosu.* In *Fricosu*, the FBI, as part of a mortgage fraud investigation, executed a search warrant at the home shared by the defendant and her children and mother.[142] The FBI seized six computers, including an encrypted laptop.[143] The encrypted machine was found in the defendant's bedroom and the computer had a name suggesting that the defendant used it.[144] In addition, the defendant made statements to her husband suggesting that she knew how to access the computer.[145] The government sought a warrant to search the computer and a writ pursuant to the *All Writs Act* "requiring [the defendant] to produce the unencrypted contents of the computer."[146] She declined, asserting her privilege against self-incrimination under

139. *Id*. (quoting *In re* Grand Jury Subpoena Duces Tecum, 1 F.3d 87, 93 (2d Cir. 1993)).

140. *Id*. at *9 (quoting Fisher v. United States, 425 U.S. 391, 411 (1976)).

141. *Id*. at *9-10 (accepting the government's argument that it could prove that the defendant possessed the files on the hard drive without making use of his production of an unencrypted version of the hard drive).

142. United States v. Fricosu, No. 10-cr-00509-REB-02, 2012 U.S. Dist. LEXIS 11083, at *3 (D. Colo. Jan. 23, 2012).

143. *Id*.

144. *Id*. at *4.

145. *Id*. at *5-6.

146. *Id*. at *6.

the Fifth Amendment.[147]

The court in *Fricosu* ordered the defendant to provide the encryption keys.[148] The court said, "[t]here is little question here but that the government knows of the existence and location of the computer's files. The fact that it does not know the specific content of any specific documents is not a barrier to production."[149] The court explained that the government had "has met its burden to show by a preponderance of the evidence that" the computer belonged to the defendant, or that the defendant "was its sole or primary user, who, in any event, can access the encrypted contents of that laptop computer."[150]

In response to the expansion of the Fifth Amendment privilege against incrimination to include the provision of passwords and encryption keys, the government may seek to provide witnesses with immunity prohibiting the use of the fact of the password or encryption key in any proceedings against a witness. This is similar to the approach followed in *Boucher*. In *Boucher*, although it does not appear that there was a formal grant of immunity, the government agreed to not use the act of providing the password as evidence of possession of the incriminating files.[151] In fact, this approach was suggested as early as 1996.[152] At that early time, one argument published in the University of Chicago Legal Forum noted that because "courts likely will find that compelling someone to reveal" encryption keys violates the Fifth Amendment privilege against compulsory self-incrimination, law enforcement will be forced to "grant some form of immunity to the owners of these documents to gain access to them."[153]

The possibility of law enforcement and prosecutors granting

147. *Id*.

148. *Id*. at *14.

149. *Id*. at *10-11.

150. *Id*. at *11.

151. *In re* Boucher, No. 2:06-mj-91, 2009 U.S. Dist. LEXIS 13006, at.*10 (D. Vt. Feb. 19, 2009).

152. Adam C. Bonin, Comment, *Protecting Protection: First and Fifth Amendment Challenges to Cryptography Regulation*, 1996 U. CHI. LEGAL F. 495, 514 (1996).

153. *Id*. *See also* Phillip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171, 172 (1996) (noting that "the ability of law enforcement to obtain access to encrypted evidence will depend largely on its ability either to compel the production of a key or password necessary to decrypt encrypted material" (footnote omitted)).

immunity to compel the provision of passwords and encryption keys is likely to not be successful in defeating Fifth Amendment arguments by witnesses. This is because the grant of immunity is not "coextensive with the scope of the privilege."[154] Generally, in order to compel testimony that otherwise would be subject to the Fifth Amendment privilege against self-incrimination, any grant of immunity must include not only the information provided, but also any evidence on the derived from information.[155] In regards to passwords and encryption keys, this means that the government must not only provide immunity for the act of providing the password or encryption key, but also for any charges arising out of information received as a result of the provision of the encryption key or password.

IV. CONCLUSION: IMPLICATIONS OF CLOUD COMPUTING

The ability to store files in the cloud gives significant life to the Fifth Amendment privilege against incrimination. The traditional Fifth Amendment doctrines were developed in a world where documents were stored in file cabinets or desks. The early cases dealing with electronic data considered records stored on electronic versions of file cabinets: hard drives and laptops.[156]

Cloud based storage is different in two significant ways. First, users typically employ much stronger security than traditional measures.[157] Industry experts have "strongly recommended" that cloud users and providers encrypt data.[158] Second, cloud based storage services may be established by anonymous users and are designed to

154. Kastigar v. United States, 406 U.S. 441, 453 (1972).

155. *Id*.

156. *Cf*. United States v. Williams, 592 F.3d 511, 523 (4th Cir. 2010) ("[W]e conclude that the sheer amount of information contained on a computer does not distinguish the authorized search of the computer from an analogous search of a file cabinet containing a large number of documents."). *But see* United States v. Carey, 172 F.3d 1268, 1274-75 (10th Cir. 1999) (noting that the government argued that the search of a computer hard drive was "similar to an officer having a warrant to search a file cabinet containing many drawers," but noting that "the file cabinet analogy may be inadequate").

157. *Cf*. JANSEN & GRANCE, *supra* note 19, at 24 (noting that organizations moving "data into the cloud . . . must account for the means by which access to the data is controlled and the data is kept secure").

158. Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*, 60 (December 2009), https://cloudsecurityalliance.org /csaguide.pdf.

allow easy collaboration on documents by multiple individuals.[159] The result is that, in many instances, an encrypted file stored in the cloud will be very difficult to trace back to an individual, whether because of technical issues or because the file locations are shared among many individuals.[160] This means: (1) the act of producing a password or encryption key will show ownership, possession or control of the files; and (2) the foregone conclusion doctrine will not be applicable because without the password or the encryption key, the government cannot establish who possessed or controlled the documents

Regardless of whether the password or encryption key is contained solely in a suspect's mind or on a written document, the act of providing the password or encryption key implicitly communicates that the person with the password or key has access to or possession of electronic files.[161] This evidence can be important, for example, in prosecutions where an element of the offense involves the use or possession of the digital files.

The policy implications for this issue are significant. Perhaps

159. *Id*. at 15.

160. The reasons for this are very technical and rapidly changing. The technical issues are beyond the scope of this paper and, for this reason, not worth addressing in this forum. Interested readers may consult a recent Note by David Colarusso, a Boston University law student. Colarusso has provided an excellent and technical detailed description of the methods criminals and non-criminals may use to avoid tracking of the placement of encrypted files in the cloud. David Colarusso, Note, *Heads In The Cloud, A Coming Storm The Interplay Of Cloud Computing, Encryption, and the Fifth Amendment's Protection Against Self-Incrimination*, 17 B.U. J. SCI. & TECH. L. 69, 69-73 (2011). For one example, Colarusso provides the following hypothetical:

> Consider what this means for a computer user who accesses cloud computing services only from wifi hotspots, who makes use of incognito mode, and who has scheduled Eraser to clean her hard drive daily or has reset her Apple settings to securely empty her "trash" by default. Unless the government knew for sure that she already had an account with some cloud provider, the act of production doctrine appears to present the functional equivalent of a complete bar to retrospectively accessing any files stored in the cloud.

Id. at 94.

161. *See* United States v. Hubbell, 530 U.S. 27, 36 (2000); Smith v. Richert, 35 F.3d 300, 302 (7th Cir. 1994) ("If a subpoena demanded all the documents possessed by the subpoenaed person concerning some subject, by producing them the person would be acknowledging that he possessed them and that they concerned the subject in question, and if this acknowledgment was self-incriminating he could not be forced to produce them." (citing Doe v. United States, 487 U.S. 201, 209-10 (1988); United States v. Doe, 465 U.S. 605, 612-14 (1984); United States v. Fisher, 425 U.S. 391, 409-14 (1976))).

most significantly, the inability of law enforcement to access the files will be more significant.[162] If people who use advanced encryption techniques are not compelled provide passwords and encryption keys, then potential criminals will be able to defeat the efforts of law enforcement officers to obtain such evidence, even when warrants have been obtained. Prosecution of child pornography and terrorism cases, for example, will become exceedingly difficult if not impossible if law enforcement cannot compel suspects or defendants to provide passwords or encryption keys.[163]

162. The challenges posed the encryption of documents and password protection of emails stored in the cloud are not new developments. For example, in 2001, shortly after the terrorist attacks of September 11 and the adoption of the *Patriot Act*, news reports stated that "Encrypted E-mail has bedeviled the FBI for years" and described the development by the FBI of a keystroke recording software in order to obtain emails that might be protected by passwords and encryption keys. Bob Port, *Spy Software Helps FBI Crack Encrypted Mail*, DAILY NEWS (N.Y.), Dec. 9, 2001, at 8 (describing "a program that records each keystroke made on a target computer and transmits that data to the bureau" and noting that the program was "intended to sidestep one of the most difficult eavesdropping hurdles: encryption").

163. *See, e.g.*, Declan McCullagh, *FBI to Announce New Net-Wiretapping Push*, CNET NEWS, Feb. 16, 2011 *available at* http://news.cnet.com/8301-31921_3-20032518-281.html (noting statement by FBI because of the rise of Web-based e-mail and social networks, it's "increasingly unable to conduct certain types of surveillance that would be possible on cellular and traditional telephones" (internal quotation marks omitted)).