THE INTERSECTION OF THE FOURTH AND FIFTH AMENDMENTS IN THE CONTEXT OF ENCRYPTED PERSONAL DATA AT THE BORDER

John Duong[*]

INTRODUCTION

On December 17, 2006, Sebastian Boucher crossed the U.S.-Canadian border into the United States.[1] At the border inspection point in Vermont, the interviewing border agent either thought something was suspicious or perhaps just randomly chose to send Boucher to secondary inspection.[2] Or maybe it was just plain bad luck. Whatever the specific reason, travelers regularly get sent to more thorough secondary inspections at the border every day. But on that particular day, it was the beginning of Boucher's problems.

Agents from Customs and Border Protection[3] (CBP) and Immigration and Customs Enforcement[4] (ICE) conducted a search of Boucher's laptop and found thousands of images of adult pornography and file names that seemed to reference

---

[*] J.D. Candidate 2010, The Earle Mack School of Law at Drexel University; B.S. Computer Science 2000, University of Toronto. I would like to thank Professor David S. Cohen for his helpful comments on an earlier draft of this Note.

1. *In re* Boucher, No. 2:06-mj-91, 2007 WL 4246473, at *1 (D. Vt. Nov. 29, 2007), *rev'd*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

2. *Id.*

3. Customs and Border Protection is an agency of the Department of Homeland Security. CBP.gov, This is CBP, http://www.cbp.gov/xp/cgov/about/mission/cbp_is.xml (last visited Nov. 29, 2009). CBP is responsible for enforcing federal laws and protecting the U.S. border from terrorism, human and drug smuggling, illegal migration, and agricultural pests while facilitating the flow of legitimate trade and travel. *Id.*

4. Immigration and Customs Enforcement is an agency of the Department of Homeland Security. U.S. Immigration and Customs Enforcement, About, http://www.ice.gov/about/index.htm (last visited Nov. 29, 2009). ICE is the largest and primary investigative arm of Homeland Security. U.S. Immigration and Customs Enforcement, Office of Investigations, About Us, http://www.ice.gov/investigations/ (last visited Nov. 29, 2009). ICE is responsible for enforcing federal law, ensuring national security, and public safety. U.S. Immigration and Customs Enforcement, Programs, http://www.ice.gov/pi/topics/index.htm (last visited Nov. 29, 2009). This Note will refer to CBP and ICE generically as "Customs" where the distinction between the two agencies is irrelevant.

child pornography.[5] The agents, however, were not successful in opening these suspected child pornography files to view their contents.[6] Boucher was read his *Miranda* rights but chose to waive them and assisted the Customs agents by showing them the location of the pornographic files on "drive Z" of his laptop.[7] The agents searched the Z drive and found several images and videos of child pornography and then took the fateful step of turning the laptop off.[8] Boucher claimed that during the course of his downloads of adult pornography, he inadvertently downloaded child pornography files, but deletes them when he discovered their contents.[9] Boucher was charged with transportation of child pornography in interstate or foreign commerce in violation of 18 U.S.C. § 2252A(a)(1).[10] Weeks later, a forensic expert undertook an investigation of the contents of Boucher's seized laptop, but the Z drive was inaccessible because it was encrypted with the software program Pretty Good Privacy (PGP).[11]

A grand jury later subpoenaed[12] Boucher to disclose the passphrase required to access the encrypted Z drive.[13] Boucher then sought to quash the subpoena on the basis of his Fifth

---

5. *In re Boucher*, 2007 WL 4246473, at *1.

6. *Id.*

7. *Id.* The facts are not clear surrounding the circumstances of why the agents did not notice the Z drive during their initial search of Boucher's laptop. It could be that the Z drive was a virtual container or partition that was not mounted and therefore not accessible. At the same time, however, the agents did not see Boucher enter a passphrase so it is possible that the drive was mounted and the agents simply missed it. A more thorough discussion of the use of encryption programs is beyond the scope of this Note.

8. *Id.* at *2.

9. *Id.* at *1.

10. *Id.* 18 U.S.C. § 2252A(a)(1) makes it unlawful for any person to "knowingly mail[], or transport[] or ship[] using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography." 18 U.S.C. § 2252A(a)(1) (effective Oct. 13, 2008).

11. *In re Boucher*, 2007 WL 4246473, at *2. Pretty Good Privacy is a widely-used encryption software program for email and data. PGP CORP., CORPORATE BACKGROUNDER 4 (2008), http://download.pgp.com/pdfs/datasheets/PGP-Corporate-Backgrounder.pdf. PGP was originally created by Philip Zimmermann, who was investigated for possible violations of U.S. export laws on encryption technology during the early 1990s. For a discussion of the investigation, see Elizabeth Lauzon, Note, *The Philip Zimmermann Investigation: The Start of the Fall of Export Restrictions on Encryption Software Under First Amendment Free Speech Issues*, 48 SYRACUSE L. REV. 1307 (1998).

12. A subpoena compels "the witness to produce any books, papers, documents, data, or other objects the subpoena designates." FED. R. CRIM. P. 17(c)(1). This type of subpoena is also called a subpoena *duces tecum*. BLACK'S LAW DICTIONARY 1467 (8th ed. 2004).

13. *In re Boucher*, 2007 WL 4246473, at *2.

Amendment privilege against self-incrimination.[14] In *In re Boucher*,[15] the issue before the court was whether compelling Boucher to enter the passphrase to decrypt the protected contents of his laptop would violate the Fifth Amendment privilege against self-incrimination.[16] Applying Supreme Court case law, the court held that Boucher was entitled to Fifth Amendment protection and did not have to disclose his passphrase.[17]

In re Boucher is the first court case where the government tried to compel a person to reveal the passphrase necessary to gain access to encrypted data.[18] However, the situation Boucher found himself in is not unique. It occurs every day to anyone wishing to enter the United States at the border or its functional equivalent, an international airport.[19] A person may randomly get sent to secondary inspection and asked by Customs agents to turn on his or her electronic device to verify that it is functioning properly and not a hollow container for contraband or an explosive device.[20] Customs agents may then proceed to inspect the device for contraband, which implicates the search and seizure provision of the Fourth

---

14. *Id.*

15. No. 2:06-mj-91, 2007 WL 4246473 (D. Vt. Nov. 29, 2007), *rev'd*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

16. *Id.* at *2.

17. *See id.* at *5.

18. Actually, there was an even earlier case that involved encryption: United States v. Burr (*In re* Willie), 25 F. Cas. 38 (C.C. Va. 1807) (No. 14,692e). That case concerned the treason trial of former Vice President Aaron Burr. Burr was indicted for attempting to lead a rebellion against the United States in the western territories. The only physical evidence against Burr was an encrypted letter that Burr sent to his collaborators. Burr's secretary knew how to decrypt the letter and was subpoenaed to testify as to the contents. Chief Justice John Marshall held that Burr's secretary could not refuse to testify based on the Fifth Amendment privilege. Eventually, Burr was acquitted of treason. Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?,"* 33 CONN. L. REV. 503, 528–29 (2001). Unlike the *Burr* case, *In re Boucher* is the first case where the government tried to compel the person, rather than a third party, to disclose the encryption passphrase.

19. United States v. Arnold, 523 F.3d 941, 944 (9th Cir. 2008) ("Searches of international passengers at American airports are considered border searches because they occur at the 'functional equivalent of a border.'" (citing Almeida-Sanchez v. United States, 413 U.S. 266, 273 (1973))).

20. Daniel Engber, *What Makes Laptops So Dangerous?: Why They Get Special Attention at the Airport*, SLATE, Nov. 22, 2005, http://www.slate.com/id/2130910/.

Amendment.[21] But at the border, there is an exception to the Fourth Amendment which gives the government broader search powers than in the interior.[22] This power includes the ability to search and seize virtually any tangible object without any prior suspicion of any wrongdoing.[23]

With the increasing use of electronic devices[24] in people's lives, searches at the border raise troubling questions as to whether people can protect their private data from government intrusion after travelling abroad.[25] The storage capacities and portability of these electronic devices have increased tremendously within the past few years with the result that people tend to put an ever-increasing amount of personal data on such devices. Certainly, not everyone is carrying illicit materials in their electronic devices, but the extent and scope of the government's search powers at the border is cause for concern due to the asymmetry of power between the government's right to inspect property for contraband and the individual's constitutional right not to be compelled to reveal materials that may be self-incriminating.

This Note discusses whether a U.S. citizen can successfully use encryption technology to protect private data in electronic devices against a government search at the border. In particular, this Note will argue that the use of encryption implicates the Fifth Amendment privilege against the compelled disclosure of the encryption passphrase and the digital contents protected by that passphrase.

Part I of this Note provides an overview of the border search exception to the Fourth Amendment, current border policies,

---

21. Austin Bogues, *Laptop Searches in Airports Draw Fire at Senate Hearing*, N.Y. TIMES, June 26, 2008, at A17, *available at* http://www.nytimes.com/2008/06/26/washington/26airports.html.

22. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985) ("[T]he Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior. Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant . . . .") (citation omitted).

23. *See Arnold*, 523 F.3d at 946 (stating that reasonable suspicion was not required to search laptop).

24. The phrase "electronic device" will be used to refer generally to laptops, mobile phones, digital cameras, digital music players, or any other device that contains electronic components. This Note will mainly discuss laptop devices, but will use the more general category of electronic devices when the discussion is not solely confined to laptops.

25. Joelle Tessler, *Laptop Searches at Border Might Get Restricted*, ASSOCIATED PRESS, Dec. 8, 2008, *available at* http://www.usatoday.com/tech/news/2008-12-08-laptop-searches_N.htm.

and recent case law concerning searches at the border. Part II provides background on encryption: what it is and why it presents a problem to law enforcement. Part III reviews and discusses the meaning of the Fifth Amendment and Supreme Court cases interpreting it, how the Court has narrowed the Fifth Amendment privilege against self-incrimination, and a possible shift back to a broader interpretation of the Fifth Amendment. Part IV applies the Supreme Court's modern Fifth Amendment analytical framework to travelers with encrypted devices at the border, and then analyzes whether the *Boucher* case was correctly decided. Part V discusses the implications of providing Fifth Amendment protection to encrypted data in light of the concern over national security at the border. Finally, Part VI concludes that the use of encryption implicates Fifth Amendment protection under the Constitution.

I. THE FOURTH AMENDMENT AT THE BORDER

The Fourth Amendment guarantees that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[26]

The Supreme Court of the United States has stated that a search is reasonable when it is conducted pursuant to a search warrant that is supported by probable cause and issued by a member of the judiciary.[27] The requirement that a search warrant must be obtained from an independent judiciary ensures that individuals within the nation's borders are protected from overreaching government powers. But things are different at the periphery.

The executive, legislative, and judicial branches of government have all recognized that the situation at the border is different from that in the interior and merits an exemption from

26. U.S. CONST. amend. IV.

27. *See, e.g.*, Katz v. United States, 389 U.S. 347, 357 (1967).

the probable cause and warrant requirements. This exception to the Fourth Amendment is known as the "border search exception."

A. The Border Search Exception to the Fourth Amendment

At the border, the Fourth Amendment does not play the same role in safeguarding individual rights against searches and seizures as in the interior. The border search exception has a long history, dating back to the First Congress that enacted the first customs statute in 1789, two months prior to proposing the Fourth Amendment to the states.[28] The significance of the acts of the First Congress has not gone unnoticed by the Supreme Court: "Since the founding of our Republic, Congress has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country."[29] Indeed, this historical backdrop has been the primary rationale attributed to justifying the border search doctrine.[30]

The border search exception thus enables the government to conduct suspicionless routine searches without probable cause at the boundaries of the country.[31] The evidence obtained from such a search could then be used to indict the person on possible criminal charges. This is exactly the opposite of what happens in the interior where the government must meet the burdensome particularity and probable cause requirements of the Fourth Amendment in obtaining a search warrant prior to a search.[32] This "reverse" probable cause situation raises con-

---

28. United States v. Ramsey, 431 U.S. 606, 616 (1977) (explaining origins and historical importance of the border search exception).

29. United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985) (citing *Ramsey*, 431 U.S. at 616–17 (citing Act of July 31, 1789, ch. 5, 1 Stat. 29)).

30. *See Ramsey*, 431 U.S. at 619 ("This longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless 'reasonable' has a history as old as the Fourth Amendment itself.").

31. There is a recognition that nonroutine, intrusive searches of the person's body may implicate human dignity and privacy interests, but the Supreme Court has not expressed what standard is required for such searches. *See Montoya de Hernandez*, 473 U.S. at 541 n.4 ("We suggest no view on what level of suspicion, if any, is required for nonroutine border searches such as strip, body cavity, or involuntary x-ray searches.").

32. *See, e.g.*, *Katz*, 389 U.S. at 357.

stitutional questions as to whether a person can independently rely on the Fifth Amendment for protection against giving evidence that may be used against that person.

B. The Government Has Plenary Search Powers at the Border

Currently, Department of Homeland Security (DHS) policies allow for broad searches and seizures of electronic devices at the border for analysis.[33] DHS claims plenary powers at the border because Congress has empowered Customs with expansive border search powers.[34] This practice has been justified on the basis of protecting the country from terrorists and trafficking of child pornography because "[i]n the 21st century, the most dangerous contraband is often contained in laptop computers or other electronic devices, not on paper."[35] According to the Secretary of Homeland Security, laptop searches have uncovered such illicit materials as videos of martyrdom and exploding improvised explosive devices, jihadist materials, and child pornography.[36]

In response to pressure from civil liberties groups,[37] CBP made public its internal policy regarding border searches of

---

33. Ellen Nakashima, *Travelers' Laptops May be Detained at Border: No Suspicion Required Under DHS Policies*, WASH. POST, Aug. 1, 2008, at A01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/08/01/AR2008080103030.html.

34. *See* United States v. Ickes, 393 F.3d 501, 503–05 (4th Cir. 2005) (explaining that Congress's use of the embracive term "cargo" and the use of "any" in the customs statute leads to the conclusion that the customs statute authorized expansive border searches, including searches of a computer and disks). The customs statute reads:

> Any officer of the customs may at any time go on board of any vessel or vehicle at any place in the United States or within the customs waters, . . . or at any other authorized place . . . and examine the manifest and other documents and papers and examine, inspect, and search the vessel or vehicle and every part thereof and any person, trunk, package, or cargo on board . . . .

Ickes, 393 F.3d at 503–04 (citing 19 U.S.C. § 1581(a) (2000)).

35. Michael Chertoff, Op-Ed., *Searches Are Legal, Essential: Examining Electronic Devices Helps Us Catch Terrorists, Pornographers*, USA TODAY, July 16, 2008, at 11A, *available at* http://blogs.usatoday.com/oped/2008/07/opposing-view-s.html.

36. *Id.*

37. The Electronic Frontier Foundation and Asian Law Caucus sued the government under the Freedom of Information Act to obtain Department of Homeland Security policies concerning searches at the border. Press Release, Elec. Frontier Found., Internal DHS Documents Detail Expansion of Power to Read and Copy Travelers' Papers: Quiet Changes in Policy Allow for Searches Without Suspicion of Wrongdoing (Sept. 23, 2008), *available at* http://www.eff.org/press/archives/2008/09/23.

electronic devices.[38] The scope of federal border search power disclosed in the CBP documents is startling. Absent any individualized suspicion, CBP may search and detain "computers, disks, hard drives, and other electronic or digital storage devices" for a reasonable period of time for the purpose of conducting a thorough examination of the contents within.[39] The search need not even take place on-site.[40] Moreover, in the event that CBP encounters information in electronic devices that is in a foreign language or encrypted, "CBP may seek translation and/or decryption assistance from other Federal agencies or entities" even where there is no individualized suspicion.[41]

Perhaps most astonishing is CBP's claim that its search powers enable it to make copies of the contents within electronic devices.[42] To guard against abuse, CBP policy requires that any copies made of the information contained within an electronic device be destroyed if probable cause is not later found to exist to warrant seizure of the device.[43] This is little consolation to the person who may have had copies of his or her private data sent to other federal, state, local, or even foreign agencies, which have their own data retention policies that operate outside the ambit of U.S. law.[44]

The implications of the CBP policy are clear: without any reasonable suspicion[45] of wrongdoing, a person may have his or her electronic device searched and the results of that search may give rise to probable cause leading to seizure of the device and criminal prosecution.

---

38. UNITED STATES CUSTOMS & BORDER PROT., POLICY REGARDING BORDER SEARCH OF INFORMATION 1 (2008), http://www.cbp.gov/linkhandler/cgov/travel/admissibility/search_authority.ctt/search_authority.pdf.

39. *Id.* at 1–2.

40. *Id.* at 2.

41. *Id.* at 2–3 (stating that these other "entities" include state, local, and foreign law enforcement agencies).

42. *Id.* at 2.

43. *Id.*

44. *Id.* at 4.

45. The "reasonable suspicion" standard was first articulated in *Terry v. Ohio*, 392 U.S. 1, 30 (1968). *Cf.* United States v. Montoya de Hernandez, 473 U.S. 531, 551 (1985) (Brennan, J., dissenting) ("Individual travelers also may be singled out on 'reasonable suspicion' and briefly held for further investigation." (citing *Terry*, 392 U.S. 1)).

C. Judicial Approval of Broad Government Search Powers at the Border

1. Flores-Montano *and U.S. Supreme Court deference to the federal government at the border*

The Supreme Court has a longstanding history of deferring to the federal government concerning searches and seizures that take place at the border or its functional equivalent.[46] In *United States v. Flores-Montano,*[47] a unanimous Court held that a search that involved the disassembly of a vehicle gas tank at the U.S.-Mexico border did not violate the Fourth Amendment because reasonable suspicion was not required for the search.[48] The Court was emphatic in declaring that the "Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border."[49] The Court emphasized a more fundamental rationale behind the border search exception that goes beyond its mere historical basis: "It is axiomatic that the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity."[50] Therefore, "searches made at the border . . . are reasonable simply by virtue of the fact that they occur at the border."[51]

With these commanding words, *Flores-Montano* left no doubt of the continuing Supreme Court recognition of the government's plenary search powers at the border.

---

46. *See, e.g.*, Boyd v. United States, 116 U.S. 616, 623 (1886) (noting that the act of the First Congress regulating collection of duties shows that searches and seizures at the border do not fall under the Fourth Amendment); Carroll v. United States, 267 U.S. 132, 154 (1925) ("Travelers may be so stopped in crossing an international boundary because of national self protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in.").

47. 541 U.S. 149 (2004).

48. *Id.* at 155.

49. *Id.* at 152.

50. *Id.* at 153.

51. *Id.* at 152–53 (quoting United States v. Ramsey, 431 U.S. 606, 616 (1977)).

2. *Recent Courts of Appeals decisions allow for border searches of electronic devices*

The Supreme Court has never specifically addressed the question of whether a search of electronic storage devices at the border is constitutional. However, three Courts of Appeals have recently addressed this issue and the consensus among all three circuit decisions echoed the longstanding judicial deference to the federal government at the border.[52]

Of the three circuit opinions, the Court of Appeals for the Ninth Circuit was the most explicit in its endorsement of broad government search powers at the border without any reasonable suspicion. In *United States v. Arnold*,[53] the Ninth Circuit held that reasonable suspicion was not required to search a laptop that was found to contain child pornography.[54] In 2005, Arnold arrived at Los Angeles International Airport after a flight from the Philippines.[55] As Arnold proceeded to customs, a CBP officer randomly selected him for secondary questioning and a more thorough search of his luggage, which included a laptop.[56] Arnold was then told to turn on his laptop to show that it was functioning, and a search was conducted by CBP and ICE agents, resulting in numerous images of child pornography being found.[57]

Arnold sought to suppress the evidence gained from the search of his laptop by arguing that the search was unconstitutional under the Fourth Amendment because it was conducted without reasonable suspicion.[58] The Ninth Circuit cited, with approval, *Flores-Montano* and other Supreme Court decisions that favored the government's interest at the border.[59] Moreover, the court noted that there was no logical difference be-

---

52. *See, e.g.*, United States v. Arnold, 523 F.3d 941 (9th Cir. 2008) (stating that reasonable suspicion was not required to search laptop found to contain child pornography); United States v. Irving, 452 F.3d 110 (2nd Cir. 2006) (stating that Customs had reasonable suspicion to search computer disks found to contain child pornography); United States v. Ickes, 393 F.3d 501 (4th Cir. 2005) (stating that Customs had reasonable suspicion to search laptop found to contain child pornography).

53. 523 F.3d 941 (9th Cir. 2008).

54. *Id.* at 946.

55. *Id.* at 943.

56. *Id.*

57. *Id.*

58. *Id.*

59. *Id.* at 944.

tween the search of the contents of Arnold's laptop and the suspicionless border searches of luggage allowed by the Supreme Court.[60] Thus, there was to be no distinction between containers that hold information and containers that hold contraband "with respect to their quality or nature for purposes of determining the appropriate level of Fourth Amendment protection."[61]

With the government's broad search powers at the border under the customs statute and judicial sanction of the government's interests at the border, questions arise as to how individuals may protect their private data from prying government eyes. But is this concern rational? After all, only a small percentage of the approximately 400 million travelers who enter the United States each year endure more thorough secondary inspections, and an even smaller percentage of those have electronic devices that are searched.[62] However, as more and more people carry electronic devices with vast storage capacities on trips abroad, the idea that our own digital data can be used against us through the reverse probable cause scenario at the border is worrisome. To protect that data, it is not enough to rely on privacy, as the border search exception to the Fourth Amendment will quickly dispose of that defense.[63] The Fifth Amendment may, nonetheless, provide an independent source of protection against a search at the border. How the Fifth Amendment may be invoked lies in the coupling of mathematical theory and computer algorithms: encryption.

---

60. *Id.* at 947 (citing United States v. Ross, 456 U.S. 798, 823 (1982)).

61. *Id.*

62. *See* Chertoff, *supra* note 35.

63. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 539–40 (1985) (noting that the expectation of privacy is less at the border than in the interior).

II. ENCRYPTION: BENEFITS AND PROBLEMS OF DUAL-USE TECHNOLOGY

A. What Is Encryption?

Encryption involves the encoding of information, called "plaintext," into unreadable form, termed "ciphertext."[64] The reverse process of transforming the ciphertext back into readable plaintext is called decryption.[65] The purpose, of course, is to prevent anyone other than the user or intended recipient from reading private information.

B. A Brief History of Encryption Use

Devising means to prevent communications from being intercepted by unauthorized persons has a long history dating back to ancient times. Julius Caesar utilized a method of encrypting military communications by the rather simple act of shifting characters in the Roman alphabet by three spaces.[66] Mary Queen of Scots communicated with her coconspirators using encrypted letters in a failed attempt to overthrow Elizabeth I of England.[67] Furthermore, encryption was not unknown to the Framers of the Constitution: Thomas Jefferson invented the "wheel cipher" during his tenure as Secretary of State to encrypt his correspondence.[68] The military use of encryption technology took a huge leap forward when Germany utilized the "Enigma" machine in World War II.[69]

---

64. NETWORK ASSOCS., AN INTRODUCTION TO CRYPTOGRAPHY 11 (2000), ftp://ftp.pgpi.org/pub/pgp/7.0/docs/english/IntroToCrypto.pdf ("The method of disguising plaintext in such a way as to hide its substance is called *encryption*. Encrypting plaintext results in unreadable gibberish called *ciphertext*." (emphasis in original)).

65. ROBERT CHURCHHOUSE, CODES AND CIPHERS: JULIUS CAESAR, THE ENIGMA, AND THE INTERNET 3 (2002).

66. *Id.* at 2–3, 13–14.

67. SIMON SINGH, THE CODE BOOK: THE EVOLUTION OF SECRECY FROM MARY QUEEN OF SCOTS TO QUANTUM CRYPTOGRAPHY 37–43 (1999).

68. Ann M. Lucas, Thomas Jefferson Foundation, Thomas Jefferson's Wheel Cipher (Sept. 1995, revs. by Chad Wollerton, Dec. 2003 and Apr. 2005), http://www.monticello.org/reports/interests/wheel_cipher.html.

69. CHURCHHOUSE, *supra* note 65, at 110–32 (discussing how Enigma performs and the flawed methods used by the Germans to send messages during World War II which enabled the Allies to decrypt German military communications).

C. U.S. Encryption Policy

Once considered "munitions" and therefore tightly controlled for export,[70] the U.S. government has since considerably relaxed control over encryption technology. In fact, the government has shifted towards a policy of encouraging its widespread use. In 1997, the National Institute of Standards and Technology (NIST) sponsored an open contest to develop a new, Advanced Encryption Standard (AES) capable of protecting sensitive government information into the twenty-first century.[71] The winning entry was an encryption cipher developed by two Belgian cryptographers.[72] After review by the National Security Agency (NSA), the U.S. government adopted AES for use in protecting classified materials.[73] Considering that governments jealously guard the secretive means used to protect confidential information in their operations, this announcement is both unusual and a testament to the strength of the AES cipher.

The NIST contest had another benefit: the AES algorithm was to be unclassified and royalty free.[74] Because the AES algorithm is publicly available, it has been incorporated in a multitude of products, leading to its widespread use worldwide. The public now has unprecedented access to the same powerful encryption technology used by the government to protect classified information.

---

70. Encryption Items Transferred From the U.S. Munitions List to the Commerce Control List, 61 Fed. Reg. 68,572–73 (Dec. 30, 1996) (codified in scattered sections of 15 C.F.R. pts. 730–774).

71. Nat'l Inst. of Standards & Tech., Overview of the AES Development Effort (Feb. 2001), http://csrc.nist.gov/archive/aes/index.html (follow "Overview of the AES development effort" hyperlink).

72. Press Release, Philip Bulman, Nat'l Inst. of Standards & Tech., Commerce Department Announces Winner of Global Information Security Competition (Oct. 2, 2000), *available at* http://csrc.nist.gov/archive/aes/index.html (follow "AES Press Release" hyperlink).

73. THE COMM. ON NAT'L SEC. SYS., FACT SHEET: NATIONAL POLICY ON THE USE OF THE ADVANCED ENCRYPTION STANDARD (AES) TO PROTECT NATIONAL SECURITY SYSTEMS AND NATIONAL SECURITY INFORMATION 2 (2003), *available at* http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf ("The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths. The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use.").

74. Nat'l Inst. of Standards and Tech., *supra* note 71.

D. Ubiquity of Encryption in Society

Far from the military and subversive uses associated with encryption in history, encryption has since become pervasive in our modern, technologically oriented society. In the home, encryption technology can be found in a multitude of devices. DVD and Blu-ray players perform decryption of encrypted, copyrighted movies.[75] Wireless routers utilize encryption for security over the air.[76] Every time someone uses the Internet to pay bills or to make purchases online, that person uses encryption technology.[77] Commercially, companies use encryption to protect their data and to allow employees to securely access company networks from home through a Virtual Private Network (VPN).[78]

Devices, both hardware and software, that utilize various encryption schemes are commonplace. Popular operating systems for computers, such as Microsoft Windows and Mac OS X, have some form of built-in encryption function that makes it easier for the public to use encryption technology.[79] Commercial software is readily available to perform encryption of data and email.[80] In addition to software-only solutions,

---

75. DVD Copy Control Ass'n, Frequently Asked Questions (FAQ), http://www.dvdcca.org/faq.html (last visited Nov. 29, 2009); Sony Pictures Blu-ray Disc, FAQ—What is AACS?, http://www.sonypictures.com/homevideo/bluray/blurayfaq.html (follow "What is AACS?" hyperlink) (last visited Nov. 29, 2009).

76. Barb Bowman, *WPA Wireless Security for Home Networks*, WINDOWS XP EXPERT ZONE, July 28, 2003, http://www.microsoft.com/windowsxp/using/networking/expert/bowman_03july28.mspx.

77. *See* VeriSign, Secure Sockets Layer (SSL): How It Works, http://www.verisign.com/ssl/ssl-information-center/how-ssl-security-works/index.html (last visited Nov. 29, 2009) (listing a range of internet usage situations where encryption technology is utilized).

78. Cisco Sys., Cisco VPN Client: Introduction, http://www.cisco.com/en/US/products/sw/secursw/ps2308/ (last visited Nov. 29, 2009).

79. Microsoft Windows 2000 Professional uses the Encrypting File System (EFS) to encrypt files. *See* Microsoft TechNet, Implementing the Encrypting File System in Windows 2000, http://technet.microsoft.com/en-us/library/dd277413.aspx (last visited Nov. 29, 2009). Windows XP Professional also uses EFS to encrypt files. *See* Microsoft TechNet, Encrypting File System in Windows XP and Windows Server 2003, http://technet.microsoft.com/en-us/library/bb457065.aspx (last visited Nov. 29, 2009). Windows Vista Enterprise and Ultimate Editions offer BitLocker Drive Encryption to encrypt the whole hard drive. *See* Microsoft TechNet, Windows BitLocker Drive Encryption Step-by-Step Guide, http://technet.microsoft.com/en-us/library/cc766295.aspx (last visited Nov. 29, 2009). Mac OS X offers FileVault to encrypt files. *See* Mac OS X 10.4 Help: About FileVault, http://docs.info.apple.com/article.html?path=Mac/10.4/en/mh1877.html (last visited Nov. 29, 2009).

80. PGP is the most commercially successful encryption software program. It can be used to encrypt both hard drive data and emails. *See* Peter Stephenson, *Industry Innovators: Data*

hardware manufacturers have even launched products that have built-in, automatic encryption, making it virtually transparent to the end user who need not understand the underlying encryption technology in order to use it.[81] One thing is certain: encryption exists to protect information, whether commercial or private.[82]

E. Why Does Encryption Present a Problem for Law Enforcement?

The widespread availability of encryption technology, while beneficial to the public in protecting private data and communications, also has a dark side lurking underneath. The fear that criminal and clandestine terrorist organizations may make use of this powerful technology to frustrate government authorities is very real. Terrorist organizations, such as al-Qaeda, have been known to be keen users of encryption.[83]

What makes encryption a dangerous tool in the hands of criminals and terrorists is the same feature that makes it desir-

---

Protection: Encryption: PGP, SC Magazine, Dec. 2008, *available at* http://www.scmagazineus.com/Encryption-PGP/article/121856/ (describing PGP as "the world's largest purveyor of encryption software" and a "perennial innovator"); *see also* PGP, Corporate Overview, http://www.pgp.com/about_pgp_corporation/corporate_overview/index.html (last visited Nov. 29, 2009) ("PGP Corporation is a global leader in email and data encryption software . . . .").

81. Seagate has recently introduced laptop hard drives that automatically encrypt the entire hard drive, making the whole process transparent to the user. *See* Seagate Tech., Introduction to Full Disk Encryption, http://www.seagate.com/ww/v/index.jsp?locale=en-US&name=dn_sec_intro_fde&vgnextoid=1831bb5f5ed93110VgnVCM100000f5ee0a0aRCRD (last visited Nov. 29, 2009). VIA Technologies, Inc. has manufactured computer processor cores with built-in hardware encryption. *See* Via Techs., Inc., VIA PadLock Security Initiative, http://www.via.com.tw/en/initiatives/padlock/index.jsp (last visited Nov. 29, 2009). Intel will soon introduce computer processors with encryption. *See* Matt Hines, *Intel Adds Encryption to vPro*, INFOWORLD, Dec. 10, 2007, http://www.infoworld.com/article/07/12/10/Intel-adds-encryption-to-VPro_1.html.

82. The consequences of not properly securing data are aptly illustrated by the Department of Veterans Affairs' stolen laptop debacle. A Department of Veterans Affairs data analyst had a laptop stolen from his home that contained the personal information of 26.5 million veterans. The data was not encrypted. Christopher Lee, *Worker Often Took Data Home*, WASH. POST, May 26, 2006, at A19, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/05/25/AR2006052501843.html. The government recently settled a class action lawsuit over the matter for a sum of $20 million. Terry Frieden, *VA Will Pay $20 Million to Settle Lawsuit over Stolen Laptop's Data*, CNN.COM, Jan. 27, 2009, http://www.cnn.com/2009/POLITICS/01/27/va.data.theft/index.html.

83. Jack Kelley, *Terror Groups Hide Behind Web Encryption*, USA TODAY, Feb. 5, 2001, at 7A, *available at* http://www.usatoday.com/tech/news/2001-02-05-binladen.htm; Daniel Sieberg, *Bin Laden Exploits Technology to Suit His Needs*, CNN.COM, Sept. 21, 2001, http://archives.cnn.com/2001/US/09/20/inv.terrorist.search/.

able: the ability to prevent any unauthorized person or entity from accessing private data. Realistically, unless there is a defect in the encryption algorithm or the manner in which it is implemented, there is no way to "break" the encryption and retrieve the original text other than trying every possible combination of keys.[84] This technique is highly impractical. Modern encryption ciphers are much more sophisticated than the primitive Caesar substitution cipher. Today's encryption algorithms utilize complex mathematical routines to make it virtually impossible, given the computing power available today and in the foreseeable future, to "brute force" a passphrase.[85]

Even assuming that the government has the necessary computer processing power, there is still the question of whether it is even feasible given the resources necessary to perform the process of decryption. Without even knowing what the encrypted contents hold, it may be prohibitively expensive in time and cost to attempt decryption.[86] This creates a problem for law enforcement because, not only is the data in an inaccessible format, even a successful decryption of the data may arrive too late to timely respond to the threat posed—or pursue charges if the applicable statute of limitations has run. To be sure, computing power increases every year. Even so, it is safe to say that given a strong enough passphrase, any effort expended will take longer than the targeted person's lifetime, which is all that really matters.[87]

---

84. An encryption key specifies the details of the particular encryption algorithm. SINGH, *supra* note 67, at 11. It is usually composed of a passphrase and random bits. *See* Memorandum from B. Kaliski, RSA Labs., PKCS #5: Password-Based Cryptography Specification, at 3–5 (Sept. 2000), http://tools.ietf.org/html/rfc2898.

85. Exhaustively trying all possible combinations of keys is referred to as a "brute force" attack. BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 8 (2d ed. 1996). Brute forcing a 128-bit encryption key using computer technology then existing in 1995 will take about 10^{25} years to find the correct key. *Id.* at 151. By comparison, the age of the universe is approximately 10^{10} years. *Id.* Of course, computing power has increased dramatically since 1995 but this gives an idea of the truly astronomical numbers involved.

86. In 1995, it was estimated that the average cost to break a 56-bit key in less than 30 minutes was $10 million. *Id.* at 153. To break an 80-bit key and 128-bit key, at the same $10 million cost, would take 700 years and 10^{17} years respectively. *Id.*

87. For a current demonstration of the massive difficulties in brute forcing an encryption key, see distributed.net, RC5–72 Overall Project Stats, http://stats.distributed.net/projects.php?project_id=8 (last visited Nov. 29, 2009). The worldwide participants in the project are attempting to break RSA Lab's 72-bit RC5 encryption cipher. Note the tremendous size of the numbers involved. The total number of keys to be searched is 4,722,366,482,869,646,000,000. As of July 19, 2009, only 29,971,662,473,149,810,000 keys were tested after 2,421 days using almost 80,000 computers from around the world. On average, 143,285,519,037 keys were tested

In summary, the virtually unbreakable encryption technology of today presents a real problem to national security at the border. Even if Customs seizes an encrypted device and sends it to another government agency for decryption purposes, the sheer magnitude of effort involved in attempting decryption may not be worth the cost. For this reason, it is far easier for the government to compel disclosure of the encryption passphrase through such devices as issuing a subpoena. But compelling a person to produce possibly self-incriminating evidence raises constitutional issues, the key one being whether the person can rely on the Fifth Amendment for protection against self-incrimination.

III. THE FIFTH AMENDMENT SELF-INCRIMINATION CLAUSE: A SEARCH FOR MEANING

The Self-Incrimination Clause of the Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself."[88] These rather plain words belie the vast confusion that reigns over its precise meaning among courts and legal scholars in this unsettled area of law.[89] Its underlying rationale is still a mystery.[90]

---

per second. Despite harnessing such vast computing power, the project has only completed 0.635% of the total number of keys to be searched. At this rate, the project was estimated to complete in approximately 299,646 days, or over 800 years.

88. U.S. CONST. amend. V.

89. *See, e.g.*, Ronald J. Allen & M. Kristin Mace, *The Self-Incrimination Clause Explained and Its Future Predicted*, 94 J. CRIM. L. & CRIMINOLOGY 243, 259 (2004) ("The Court has failed to provide a definition of 'testimony' that can explain its own cases."); Akhil Reed Amar & Renee B. Lettow, *Fifth Amendment First Principles: The Self-Incrimination Clause*, 93 MICH. L. REV. 857, 857 (1995) ("[T]he Fifth Amendment is an unsolved riddle of vast proportions, a Gordian knot in the middle of our Bill of Rights."); Robert P. Mosteller, *Cowboy Prosecutors and Subpoenas for Incriminating Evidence: The Consequences and Correction of Excess*, 58 WASH. & LEE L. REV. 487, 489 (2001) (describing Supreme Court Fifth Amendment decisions as "complicated and occasionally sweeping in their pronouncements" and the Court's application of the Fifth Amendment to document subpoenas as "particularly esoteric").

90. Two common rationales have frequently been mentioned by the courts. The first is the "cruel trilemma" that the defendant would face without the protections of the Fifth Amendment:

> The privilege against self-incrimination registers an important advance in the development of our liberty—one of the great landmarks in man's struggle to make himself civilized. 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; our fear that self-incriminating statements will be elicited by inhumane treatment and abuses; our sense of fair play which dic-

Modern Supreme Court jurisprudence has construed the term "witness" to refer only to the giving of "testimony."[91] Yet, as originally understood by the Framers, "witness" had a much broader meaning, a meaning that provided more protections than is the case today.

A. Original Meaning of the Fifth Amendment

At the time of the Framers, various contemporaneous sources provided substantial support for the proposition that the term "witness" referred to a person who gives or furnishes evidence.[92] Indeed, the influential Virginia Declaration of Rights in 1776 provided that no person may "be compelled to give evidence against himself."[93] Other states modeled their own state constitutions after the Virginia Declaration to provide protections against either being compelled "to give evidence" or "to furnish evidence."[94] During state ratifying con-

---

> tates a fair state-individual balance by requiring the government to leave the individual alone until good cause is shown for disturbing him and by requiring the government in its contest with the individual to shoulder the entire load; our respect for the inviolability of the human personality and of the right of each individual to a private enclave where he may lead a private life; our distrust of self-deprecatory statements; and our realization that the privilege, while sometimes a shelter to the guilty, is often a protection to the innocent.

Murphy v. Waterfront Comm'n, 378 U.S. 52, 55 (1964) (internal citations and quotations omitted).

The second rationale typically given is that the Fifth Amendment has a "zone of privacy" attached to it. *See, e.g.*, Andresen v. Maryland, 427 U.S. 463, 485 (1976) (Brennan, J., dissenting) ("[T]he Fifth Amendment protects an individual citizen against the compelled production of testimonial matter that might tend to incriminate him, provided it is matter that comes within the zone of privacy recognized by the Amendment to secure to the individual 'a private inner sanctum of individual feeling and thought.'" (quoting Couch v. United States, 409 U.S. 322, 327 (1973))); Schmerber v. California, 384 U.S. 757, 778 (1966) (Douglas, J., dissenting) ("[T]he Fifth Amendment marks 'a zone of privacy' which the Government may not force a person to surrender." (quoting Griswold v. Connecticut, 381 U.S. 479, 484 (1965))).

91. *See, e.g.*, United States v. Hubbell, 530 U.S. 27, 34 (2000) ("The word 'witness' in the constitutional text limits the relevant category of compelled incriminating communications to those that are 'testimonial' in character.").

92. *See id.* at 50 (Thomas, J., concurring) (noting that contemporaneous dictionaries defined "witness" as a person who gives or furnishes evidence); *see also* Richard A. Nagareda, *Compulsion "To Be A Witness" and the Resurrection of* Boyd, 74 N.Y.U. L. REV. 1575, 1608–09 (1999) (noting same).

93. *See Hubbell*, 530 U.S. at 52 (Thomas, J., concurring) (quoting Va. Declaration of Rights, § 8 (1776)); Nagareda, *supra* note 92, at 1606 & n.123.

94. Justice Thomas identified seven of the original Thirteen Colonies as having provisions in their state constitutions expressly providing for protection against compulsion to give or furnish evidence: Delaware Declaration of Rights § 15 (1776) ("give evidence"); Maryland

ventions, various state proposals for a federal bill of rights all sought a provision that included a privilege against compelled self-incrimination that used similar language found in their state constitutions.[95]

When James Madison, responding to pressure for a federal bill of rights, finally drafted a Bill of Rights, he conspicuously chose to substitute the phrase "to be a witness" for the phrases "to give evidence" or "to furnish evidence" that had been present in state constitutions and proposals.[96] Despite the change in wording, this modification seemed to have gone unnoticed with virtually no debate over its precise meaning in either the state legislatures that ratified the Bill of Rights or by members of the First Congress in the debates on the Bill of Rights.[97] It seems that Madison's choice of phrasing was a peculiar creation of his own. Though not dispositive, the historical context surrounding the adoption of the Fifth Amendment lends credence to the view that Madison's use of the phrase "to be a witness" was likely understood to be synonymous with "to give evidence," or equivalently "to furnish evidence." If this is true, then the Self-Incrimination Clause was intended to be an absolute bar against compelling a person to provide any evidence that is self-incriminating.[98]

Declaration of Rights, Art. XX (1776) ("give evidence"); Massachusetts Declaration of Rights, Pt. 1, Art. XII (1780) ("furnish evidence"); New Hampshire Bill of Rights, Art. XV (1783) ("furnish evidence"); North Carolina Declaration of Rights, Art. VII (1776) ("give evidence"); Pennsylvania Declaration of Rights, Art. IX (1776) ("give evidence"); Vermont Declaration of Rights, Ch. 1. Art. X (1777) ("give evidence"). *See Hubbell*, 530 U.S. at 52 (Thomas, J., concurring); *see also* Nagareda, *supra* note 92, at 1606 & nn.124–25.

95. These states include Virginia, New York, North Carolina, and Rhode Island. *Hubbell*, 530 U.S. at 52 (Thomas, J., concurring) (citing N. COGAN, THE COMPLETE BILL OF RIGHTS 327 (1997)).

96. *Id.* at 52–53.

97. Apparently, the only member of the First Congress to have addressed the self-incrimination issue treated Madison's phrasing as though it was the same as that used in the Virginia Declaration. *Id.* at 53 (Thomas, J., concurring) (citing 1 ANNALS OF CONG. 753–54 (J. Gales ed., 1834) (statement of Rep. Laurance)); Nagareda, *supra* note 92, at 1608 n.129.

98. It is certainly within the realm of possibility that the Supreme Court may re-examine the doctrine surrounding the narrow view of the Fifth Amendment Self-Incrimination Clause. In *Hubbell*, Justice Thomas, joined by Justice Scalia, contended that "the Fifth Amendment privilege protects against the compelled production not just of incriminating testimony, but of any incriminating evidence" and expressed a willingness to "reconsider the scope and meaning of the Self-Incrimination Clause" in the future. *Hubbell*, 530 U.S. at 49 (Thomas, J., concurring).

B. Boyd v. United States*: Absolute Protection Under the Fifth Amendment*

The first important case to consider both the Fourth and Fifth Amendments was *Boyd v. United States*.[99] In *Boyd*, the Supreme Court held that a person's private papers were absolutely protected under the Fifth Amendment.[100] The dispute in *Boyd* concerned the seizure and forfeiture of glass by the federal government.[101] Boyd and his business partner entered into a construction contract with the government that allowed them to replace their depleted supply of glass with imported glass duty-free.[102] When Boyd tried to bring in a second duty-free shipment, ostensibly to replace broken glass in the first shipment, the government became suspicious and initiated forfeiture proceedings along with obtaining a court order compelling Boyd to produce the invoice for the first duty-free shipment of glass.[103]

On appeal to the Supreme Court, the Court held that the court order compelling production of the invoice was unconstitutional, reasoning:

> that a compulsory production of the private books and papers of the owner . . . is compelling him to be a witness against himself, within the meaning of the Fifth Amendment to the Constitution, and is the equivalent of a search and seizure—and an unreasonable search and seizure—within the meaning of the Fourth Amendment.[104]

In doing so, the Court noted the "intimate relation" between the Fourth and Fifth Amendments, such that "we have been unable to perceive that the seizure of a man's private books and papers to be used in evidence against him is substantially different from compelling him to be a witness against himself."[105]

---

99. 116 U.S. 616 (1886).

100. *Id.* at 633–35.

101. *Id.* at 617.

102. *See* Samuel A. Alito, Jr., *Documents and the Privilege Against Self-Incrimination*, 48 U. PITT. L. REV. 27, 33 (1986) (retelling the facts by reference to the briefs in the case).

103. *See id.*

104. *Boyd*, 116 U.S. at 634–35.

105. *Id.* at 633.

The *Boyd* Court's expansive mixing of the Fourth and Fifth Amendments in holding that compelling production of incriminatory documents is an unreasonable search and seizure under the Fourth Amendment, and that this compulsion to force a person "to be a witness against himself" also violates the Fifth Amendment, is no longer good law.[106] The Court could have simply relied on the Fifth Amendment privilege against self-incrimination without regarding the court order as a search, thereby obviating the need to add the Fourth Amendment into the equation.[107] This would have nicely fit within the original meaning of the Fifth Amendment and could have possibly avoided a century of confusion.[108]

In the years following *Boyd*, various Supreme Court cases concerning physical-body evidence have curtailed *Boyd*'s broad view that the Fifth Amendment categorically protects persons against compelled production of self-incriminatory evidence.[109] However, the absolute protection given to private papers by *Boyd* has never been expressly overruled by the Supreme Court.[110]

---

106. *See, e.g.*, Fisher v. United States, 425 U.S. 391, 407 (1976) ("Several of Boyd's express or implicit declarations have not stood the test of time."); Schmerber v. California, 384 U.S. 757, 760–72 (1966) (treating the Fourth and Fifth Amendments independently of one another); Nagareda, *supra* note 92, at 1585 (stating that *Boyd*'s "conflation of the Fourth and Fifth Amendments . . . [is] not analytically sound"); H. Richard Uviller, *Foreword: Fisher Goes on the Quintessential Fishing Expedition and Hubbell is Off the Hook*, 91 J. CRIM. L. & CRIMINOLOGY 311, 321 (2001) (stating that the *Boyd* doctrine has been "thoroughly discredited").

107. *See Boyd*, 116 U.S. at 639 (Miller, J., concurring) ("The order of the court . . . is in effect a *subpoena duces tecum* . . . . That this is within the protection which the constitution intended against compelling a person to be a witness against himself, is, I think, quite clear."). Unfortunately, Justice Miller did not elaborate further on his reasoning.

108. *See* Amar & Lettow, *supra* note 89, at 884–88 & nn.117–19 (discussing court cases that held using a person's body as physical evidence was equivalent to compelling that person to be a witness against himself, and the change to court cases that held using a person's body as physical evidence does not implicate Fifth Amendment protection).

109. Doe v. United States (*Doe II*), 487 U.S. 201, 210 (1988); Nagareda, *supra* note 92, at 1591 n.60. For cases involving physical evidence, see United States v. Dionisio, 410 U.S. 1, 5–7 (1973) (voice exemplar); Gilbert v. California, 388 U.S. 263, 265–67 (1967) (handwriting exemplar); United States v. Wade, 388 U.S. 218, 222–23 (1967) (standing in a lineup); Schmerber v. California, 384 U.S. 757, 763–64 (1966) (blood test); Holt v. United States, 218 U.S. 245, 252–53 (1910) (putting on blouse).

110. *See Fisher*, 425 U.S. at 414 (declining to consider whether the Fifth Amendment would protect a taxpayer from producing his own tax records).

C. Fisher v. United States*: The Elusive Act-of-Production Doctrine*

Remarkably, it took almost a century until the meaning of the Fifth Amendment as applied to personal documents was reconsidered by the Supreme Court in *Fisher v. United States*.[111] In *Fisher*, taxpayers were under criminal investigation by the Internal Revenue Service (IRS).[112] The taxpayers obtained documents relating to the preparation of their tax returns from their accountants and then transferred the documents to their attorneys.[113] The IRS then served summonses on the attorneys to compel them to produce the documents.[114] The Court rejected the argument that the enforcement of the summonses violated the Fifth Amendment privilege against self-incrimination because a subpoena served on a third party, a lawyer in this case, did not compel any of the individual taxpayers to be a "witness" against himself.[115]

In analyzing whether the Fifth Amendment protects a person from being compelled to produce requested documents, the *Fisher* Court pronounced that the reasoning of *Boyd* "ha[s] not stood the test of time"[116] and proceeded to diverge from *Boyd* by enunciating a new conceptual framework for Fifth Amendment analysis that drew a distinction between acts that are testimonial and those that are not. As stated by the Court: "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."[117] Henceforth, the proper analysis in self-incrimination cases is whether a person is compelled to give self-incriminating "testimony."[118]

---

111. 425 U.S. 391 (1976).

112. *Id.* at 393–94.

113. *Id.*

114. *Id.* at 394.

115. *Id.* at 397.

116. *Id.* at 407–08 (the Court went on to cite cases that limited *Boyd*'s holding in search and seizure cases under the Fourth Amendment).

117. *Id.* at 408.

118. *See id.* at 409 ("[T]he 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.") (citations omitted).

The *Fisher* Court's narrow construction of the term "witness" to refer to a person who makes a "testimonial" communication was a rejection of *Boyd*'s holding that the Fifth Amendment, as originally interpreted, categorically protects a person from being compelled to produce self-incriminating evidence.[119] The *Fisher* Court noted that its interpretation of the Fifth Amendment, as applied to document subpoenas, was consistent with a succession of Supreme Court cases in the past several decades that consistently held that compelling a person to give incriminating physical evidence does not violate the Fifth Amendment because none of those cases involved compelling a person to make a self-incriminating testimonial communication.[120] Thus, the Fifth Amendment privilege "protects a person only against being incriminated by his own compelled testimonial communications."[121]

In determining whether a person is entitled to invoke the Fifth Amendment privilege, it is now necessary to distinguish between the contents of documents and the act of producing them in response to a subpoena.[122] Under this "act-of-production" doctrine, the contents of voluntarily created documents receive no Fifth Amendment protection because they are not compelled testimonial evidence.[123] But, in certain situations, the act of producing evidence in response to a subpoena may have "communicative aspects of its own, wholly aside from the contents of the papers produced."[124] The act, therefore, may be protected if it is testimonial in character, i.e., by implicitly acknowledging the existence of the documents, that the documents were under the possession or control of

---

119. *See id.* at 406–08.

120. *Id.* at 408; *see* cases cited *supra* note 109.

121. *Fisher*, 425 U.S. at 409; *see also* Schmerber v. California, 384 U.S. 757, 764 (1966) ("[T]he [Fifth Amendment] privilege is a bar against compelling 'communications' or 'testimony,' but . . . compulsion which makes a suspect or accused the source of 'real or physical evidence' does not violate it."); Holt v. United States, 218 U.S. 245, 252–53 (1910) (Holmes, J.) ("[T]he prohibition of compelling a man in a criminal court to be witness against himself is a prohibition of the use of physical or moral compulsion to extort communications from him, not an exclusion of his body as evidence when it may be material.").

122. *See* Nagareda, *supra* note 92, at 1594.

123. *See Fisher*, 425 U.S. at 409–10.

124. *Id.* at 410.

the person, and that the documents are authentic.[125] Just what this three-prong test exactly means is unclear. At what point does an act sufficiently cross the testimonial threshold triggering Fifth Amendment protection? *Fisher* left this important question unanswered, only stating that the act-of-production doctrine should be analyzed under "the facts and circumstances of particular cases."[126]

The act-of-production doctrine has been criticized as "excessively abstract" and difficult to apply in practice.[127] To be sure, the government is almost always interested in the contents of the document and not whether the act of producing it is testimonial and deserving of Fifth Amendment protection.[128] In fact, this encourages the possibility that the person served with a subpoena will destroy the evidence and then deny its existence, thereby easily evading the command of the subpoena.[129]

D. Fisher and the Foregone Conclusion Doctrine: Reshaping the Fifth Amendment

In addition to the act-of-production doctrine, *Fisher* also articulated a related "foregone conclusion" doctrine.[130] In applying the *Fisher* three-prong test to determine whether the act of producing the tax documents at issue in the case rose to the level of being a testimonial communication, the *Fisher* Court made it clear that implicitly admitting the existence and possession of the tax documents was not enough for Fifth Amendment protection because "[t]he existence and location of the papers are a foregone conclusion and the taxpayer adds

---

125. *See id.* ("Compliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer. It also would indicate the taxpayer's belief that the papers are those described in the subpoena.").

126. *Id.*

127. *See* Alito, *supra* note 102, at 46–47 (discussing problems with the act-of-production doctrine as it relates to subpoenas); *see also Fisher*, 425 U.S. at 431 (Marshall, J., concurring) (noting that the "technical and somewhat esoteric focus on the testimonial elements of production rather than on the content of the evidence" is contrary to Fifth Amendment protection against self-incrimination).

128. *See* Alito, *supra* note 102, at 46.

129. *Id.* at 47 (noting that a rational witness will only comply with a subpoena if the evidence requested is not incriminating).

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

little or nothing to the sum total of the Government's information by conceding that he in fact has the papers."[131] In other words, if the government already knows of the existence and location of the subpoenaed documents, the Fifth Amendment is not implicated.

Immediately apparent is the Court's imparting of a quantity element into Fifth Amendment analysis. As Justice Brennan rightfully points out, nowhere in the Constitution or Court precedent does the Fifth Amendment privilege depend on a sliding scale of the quantity of the government's preexisting knowledge.[132] Not surprisingly, by enunciating yet another doctrine to an already abstract framework, the *Fisher* Court further complicated the analysis for lower courts.[133]

E. United States v. Doe*: The Metaphysics of Act-of-Production Immunity*

The *Fisher* framework was reaffirmed in *United States v. Doe* (*Doe I*),[134] where the Supreme Court ruled that the contents of voluntarily created business records do not implicate Fifth Amendment protection.[135] In *Doe I*, a grand jury investigation into political corruption in the awarding of county and municipal contracts subpoenaed Doe to produce the business records of several sole proprietorships that he owned.[136] Under the particular facts of the case, the Court deferred to the findings of the lower courts and held that the act of producing the requested business records was equivalent to testimonial self-incrimination.[137] Notably, the Court intimated that the government could have overcome the privilege against self-

131. *Id.*

132. *See id.* at 429 (Brennan, J., concurring) ("I know of no Fifth Amendment principle which makes the testimonial nature of evidence, and therefore, one's protection against incriminating himself, turn on the strength of the Government's case against him."); *see also* Alito, *supra* note 102, at 49 ("[T]he [Fifth Amendment] privilege has never been restricted to testimony that is not cumulative.").

133. *See* United States v. Hubbell, 167 F.3d 552, 601 (D.C. Cir. 1999) (Williams, J., dissenting in part) ("[T]he operational meaning of the 'act-of-production' doctrine . . . will largely turn on district courts' discretion in [the] metaphysical classification of prosecutors' knowledge."), *aff'd*, 530 U.S. 27 (2000).

134. 465 U.S. 605 (1984).

135. *Id.* at 610–12.

136. *Id.* at 606–07.

137. *Id.* at 613–14.

incrimination by granting Doe "use immunity"[138] for the act of producing the documents.[139] Hence, the act itself would be privileged, but not the contents.[140]

Justice O'Connor's short concurring opinion went further, pronouncing that "the Fifth Amendment provides absolutely no protection for the contents of private papers of any kind."[141] This was an overly broad reading of *Doe I* as the case did not involve private documents, but rather business records.[142] Moreover, Justice O'Connor's assertion that *Fisher* "sounded the death-knell for *Boyd*" was premature.[143] The *Fisher* Court in fact did not expressly overrule *Boyd*'s holding that afforded absolute protection to private records.[144] Indeed, a key inference can be drawn that *Boyd* is still good law as applied to private records due to the fact that *Fisher* and its progeny all dealt with business records and third parties—not compelling an individual to produce private records.[145]

1. *The scope of act-of-production immunity*

After *Fisher* and *Doe I*, the scope of the act-of-production immunity led to debate about whether it protected the contents of documents. One view suggests a narrow reading of

---

138. *See generally* Kastigar v. United States, 406 U.S. 441 (1972) (holding that the government may grant "use and derivative use" immunity to overcome a Fifth Amendment privilege claim).

139. *See Doe I*, 465 U.S. at 614–17.

140. As stated by the Court:

> Respondent argues that any grant of use immunity must cover the contents of the documents as well as the act of production. We find this contention unfounded. To satisfy the requirements of the Fifth Amendment, a grant of immunity need be only as broad as the privilege against self-incrimination. As discussed above, the privilege in this case extends only to the act of production. Therefore, any grant of use immunity need only protect respondent from the self-incrimination that might accompany the act of producing his business records.

See id. at 617 n.17 (internal citations omitted).

141. *Id.* at 618 (O'Connor, J., concurring).

142. *Id.* at 606; *see also id.* at 619 (Marshall, J., concurring in part) (noting that the subpoenaed documents were business records which have less privacy protection than if they were personal diaries).

143. *Id.* at 618 (O'Connor, J., concurring).

144. *See* Fisher v. United States, 425 U.S. 391, 414 (1976) ("Whether the Fifth Amendment would shield the taxpayer from producing his own tax records in his possession is a question not involved here; for the papers demanded here are not his 'private papers' . . . .").

145. Interestingly, the *Boyd* Court referred to Boyd's records as "private books and papers" and not as business records. Boyd v. United States, 116 U.S. 616, 631–35 (1886).

the act-of-production immunity grant to only protect the testimonial act of production of documents and never the contents of those documents.[146] This view is the same as that articulated by the *Doe I* Court.[147] The opposing view takes a broader approach and believes that act-of-production immunity is effectively equivalent to use immunity.[148] Just what exactly are the contours of this new form of immunity? To understand the difference in interpretations, it is necessary to distinguish use immunity from act-of-production immunity.

Use immunity provides protection from direct or derivative use of the compelled testimony in a prosecution.[149] But while the testimony is protected, it does not preclude the government from using the revelations disclosed from that testimony in a prosecution setting so long as the government can prove that its evidence was not "tainted."[150] In other words, the government bears the heavy burden of proving that its evidence was not derived directly or indirectly from the witness's disclosure, and that it was obtained from a source wholly independent from the immunized testimony.[151] By contrast, "transactional" or "complete" immunity prohibits any future prosecution for the compelled testimony.[152] The Supreme

---

146. *See* Alito, *supra* note 102, at 57.

147. *Doe I*, 465 U.S. at 617 n.17 (internal citations omitted).

148. *See Fisher*, 425 U.S. at 433–34 (Marshall, J., concurring in part) ("Under the Court's theory, if the document is to be obtained the immunity grant must extend to the testimony that the document is presently in existence. Such a grant will effectively shield the contents of the document, for the contents are a direct fruit of the immunized testimony—that the document exists—and cannot usually be obtained without reliance on that testimony."); *see also* Robert P. Mosteller, *Simplifying Subpoena Law: Taking the Fifth Amendment Seriously*, 73 VA. L. REV. 1, 43 (1987) ("[G]ranting use immunity when the existence of the document is not known to the prosecution will in effect immunize the witness against any use of its contents.").

149. Alito, *supra* note 102, at 57; *see also* Kastigar v. United States, 406 U.S. 441, 453 (1972) ("We hold that such immunity from use and derivative use is coextensive with the scope of the privilege against self-incrimination, and therefore is sufficient to compel testimony over a claim of the privilege.").

150. Alito, *supra* note 102, at 57–58; *see also Kastigar*, 406 U.S. at 453 ("While a grant of immunity must afford protection commensurate with that afforded by the privilege, it need not be broader. . . . The privilege has never been construed to mean that one who invokes it cannot subsequently be prosecuted.").

151. Alito, *supra* note 102, at 55; *see also Kastigar*, 406 U.S. at 460 ("This burden of proof, which we reaffirm as appropriate, is not limited to a negation of taint; rather, it imposes on the prosecution the affirmative duty to prove that the evidence it proposes to use is derived from a legitimate source wholly independent of the compelled testimony.").

152. *See generally* Counselman v. Hitchcock, 142 U.S. 547 (1892) (holding that total immunity against future prosecution was required to overcome a person's claim of the Fifth Amendment privilege).

Court has held that only use immunity is constitutionally sufficient.[153]

Act-of-production immunity, on the other hand, is a narrower version of use immunity. It protects only the testimonial component of the act of producing documents, and does not protect the contents of those documents.[154] In conceptualizing the meaning of this limited form of immunity, one commentator, then Assistant to the Solicitor General, Samuel Alito,[155] has offered an explanation that seemingly delves into the realm of metaphysics. Alito considers a situation where before a subpoena was issued by a grand jury, the incriminating records "magically" appeared in front of them.[156] The grand jury can then make use of the contents of those records because they are an independent source of the same information that would have been provided by subpoena, without the need to know anything about the act of production.[157] The effect, therefore, would be the same as an immunity grant for the act of production.

Another commentator, Professor Akhil Amar, also seems to support the view that the government can overcome the protection of the Fifth Amendment by granting immunity but nevertheless use the "fruits" derived against that person:

> Under penalty of contempt, a suspect must answer truthfully, but he will be entitled to 'testimonial immunity': that is, the compelled words will never be introduced over the defendant's objection in a criminal trial—the defendant will never be an involuntary 'witness' against himself 'in' a 'criminal case'—but the fruits of these compelled pretrial words will generally be admissible.[158]

Therefore, the lessons of *Fisher* and *Doe I* are that the act of production of subpoenaed evidence may be privileged under the Fifth Amendment if it has a testimonial component, but the contents are never protected. However, the government

---

153. *Kastigar*, 406 U.S. at 453.

154. Alito, *supra* note 102, at 56–57.

155. Alito argued for the government in *United States v. Doe* (*Doe I*), 465 U.S. 605, 606 (1984).

156. Alito, *supra* note 102, at 60.

157. *Id.* at 60–61.

158. Amar & Lettow, *supra* note 89, at 858–59.

may overcome the Fifth Amendment privilege by granting act-of-production immunity.[159]

Even though *Boyd*'s holding that private records have absolute protection under the Fifth Amendment has never been expressly overruled by the Supreme Court, are all these commentators right? Did *Fisher* and *Doe I* do away with the last vestiges of *Boyd*, thereby reducing the Fifth Amendment to a hollow shell of its former self? If these commentators are correct, the consequences for Fifth Amendment protection would be disastrous as such a view would "essentially eviscerate[] the act-of-production doctrine, as well as the Fifth Amendment protection it secures."[160]

F. United States v. Hubbell*: Reinvigorating the Fifth Amendment and Derivative Use Immunity*

The Supreme Court finally resolved the question of whether the evidence produced from a grant of act-of-production immunity is protected nearly a quarter century after *Fisher* and *Doe I*. In *United States v. Hubbell*,[161] the Supreme Court held that the scope of Fifth Amendment protection extends to derivative use of the compelled production of evidence in response to a subpoena.[162] During the Whitewater investigation, the Independent Counsel subpoenaed documents from Hubbell.[163] Hubbell invoked his Fifth Amendment privilege against self-incrimination, leading the Independent Counsel to produce a previously obtained court order granting him immunity[164] for the production of the requested documents.[165]

---

159. Alito, *supra* note 102, at 64–65.

160. United States v. Hubbell, 167 F.3d 552, 583 (D.C. Cir. 1999), *aff'd*, 530 U.S. 27 (2000).

161. 530 U.S. 27 (2000).

162. *Id.* at 43.

163. *Id.* at 30.

164. The immunity was granted pursuant to 18 U.S.C. § 6002 which provides that:

> Whenever a witness refuses, on the basis of his privilege against self-incrimination, to testify or provide other information in a proceeding . . . and the person presiding over the proceeding communicates to the witness an order issued under this title, the witness may not refuse to comply with the order on the basis of his privilege against self-incrimination; but no testimony or other information compelled under the order (or any information directly or indirectly derived from such testimony or other information) may be used against the witness in any criminal case . . . .

18 U.S.C. § 6002 (2006).

165. *Hubbell*, 530 U.S. at 31.

The Independent Counsel then used the contents of the documents to indict Hubbell on tax and fraud charges.[166] The Court rejected the government's argument that the contents are not protected under the Fifth Amendment because the government needed Hubbell to make use of "the contents of his own mind" in identifying potential sources of evidence and to produce them such that "the testimonial aspect of respondent's act of producing subpoenaed documents was the first step in a chain of evidence that led to this prosecution."[167]

Although the Court maintained the *Fisher* distinction between the act of producing documents and the contents of those documents,[168] the Court expressly rejected the conceptual view suggested by Alito earlier that the contents of documents are never protected: "The documents did not magically appear in the prosecutor's office like 'manna from heaven.'"[169] In doing so, the Court clarified that the act of production was not a mere physical act that is nontestimonial because Hubbell had to make extensive use of "the contents of his own mind" in identifying the documents requested in the subpoena.[170] Justice Stevens, writing for the majority, provided a helpful "strongbox" analogy to illustrate that Hubbell's act was testimonial: "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."[171] Therefore, Hubbell's act was testimonial because complying with the broadly worded subpoena was "the functional equivalent of the prepa-

166. *Id.*

167. *Id.* at 41–43.

168. *See id.* at 42 ("Entirely apart from the contents . . . providing a catalog of existing documents fitting within any of the 11 broadly worded subpoena categories" is an act with testimonial aspects to it.).

169. *Id.*

170. *Id.* at 43 (quoting Curcio v. United States, 354 U.S. 118, 128 (1957) (second citation omitted)). *Curcio* held that forcing a custodian of union records to testify as to where the records are "requires him to disclose the contents of his own mind. . . . That is contrary to the spirit and letter of the Fifth Amendment." *Curcio*, 354 U.S. at 128.

171. *Hubbell*, 530 U.S. at 43 (citing Doe v. United States (*Doe II*), 487 US 201, 210 n.9 (1988)). This part of *Hubbell* has been criticized by Professor Uviller who argues that the Court's reasoning "goes too far" because "[v]irtually every custodian who complies with a subpoena *duces tecum*, must use his or her mind to sort out the files and to cull and organize documents." Uviller, *supra* note 106, at 320.

ration of an answer to either a detailed written interrogatory or a series of oral questions at a discovery deposition."[172]

1. *Rejection of the metaphysics of* Doe I*: Restoration of Fifth Amendment protection to the contents of documents*

Under *Fisher* and *Doe I*, the government can overcome an individual's assertion of the Fifth Amendment privilege and compel the disclosure of the subpoenaed materials sought by granting act-of-production immunity. The act of producing the evidence would then be privileged but the contents would not be. The *Hubbell* Court delineated the scope of this act-of-production immunity and held that it must extend to any derivative use of the immunized testimony.[173] The Court reasoned that any "[c]ompelled testimony that communicates information that may 'lead to incriminating evidence' is privileged even if the information itself is not inculpatory."[174] This was a firm rejection of Alito's "manna from heaven" approach and the *Fisher* and *Doe I* view that the contents of documents are never protected.

2. *Narrowing the foregone conclusion doctrine*

While the *Hubbell* Court performed admirably in clarifying the breadth of Fifth Amendment protection as it pertains to subpoenaed documents, the Court declined to provide any guidance on the application of the foregone conclusion doctrine and merely stated that it did not apply in the case.[175] The Court arrived at this conclusion by distinguishing the facts from *Fisher* in that, unlike in *Fisher* where the government already knew the existence and possession of the tax records, "here the Government has not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced."[176] The significance of this is that in determining whether the foregone conclusion doctrine applied, the key question is the extent of

---

172. *Hubbell*, 530 U.S. at 41–42.

173. *See id.* at 43.

174. *Id.* at 38 (citing *Doe II*, 487 U.S. at 208 n.6).

175. *See id.* at 44 ("Whatever the scope of this 'foregone conclusion' rationale, the facts of this case plainly fall outside of it.").

176. *Id.* at 45.

the government's prior knowledge of the particular items subpoenaed.[177] It is not enough to claim that certain broad categories of records, such as general business and tax records, will always be possessed by the person being subpoenaed.[178] The government must bear the heavy burden of showing that it actually knew such records existed and where they were located.[179] If the government is unable to show that it had prior knowledge of the existence and location of the subpoenaed items, then the foregone conclusion doctrine does not apply.

3. *Implications of the* Hubbell *Decision*

The Supreme Court's decision in *Hubbell* significantly broadened the protections afforded to individuals under the Fifth Amendment. Although the Court was careful to maintain the prior precedent laid out in *Fisher* and its progeny, the *Hubbell* decision was arguably more *Boyd*-like in its effect.[180] No longer can the government engage in a "fishing expedition" by issuing subpoenas demanding the production of incriminating evidence of which it had no prior knowledge, and then in turn use that evidence against the witness. *Hubbell* requires that the government grant use and derivative use immunity to gain access to such evidence, which effectively prevents the evidence from being used in a future prosecution.

Whether *Hubbell* marks the beginning of a new shift in the Court's Fifth Amendment doctrine is unclear. One thing is certain though: *Hubbell*'s derivative use doctrine breathed life back into the Fifth Amendment, and this has considerable implications for encryption.

---

177. Lance Cole, *The Fifth Amendment and Compelled Production of Personal Documents After* United States v. Hubbell—*New Protection for Private Papers?*, 29 AM. J. CRIM. L. 123, 168 (2002).

178. *Hubbell*, 530 U.S. at 45.

179. *Id.*

180. *See* Cole, *supra* note 177, at 190 (stating that "*Hubbell* has, at least in practical effect, overruled *Fisher* and restored full, meaningful (as opposed to 'act of production') Fifth Amendment protection to most private papers in the possession of the individual."); Uviller, *supra* note 106, at 333 (stating that "one of the disturbing characteristics about the *Hubbell* decision" is its suggestion that the *Boyd* doctrine may be resurrected).

IV. APPLICATION OF THE FISHER FRAMEWORK TO ENCRYPTED DEVICES

At the border, or its functional equivalent, the border search exception to the Fourth Amendment gives U.S. Customs broad authority to conduct searches. The government's plenary power to search under the customs statute, in tandem with judicial approval, is a powerful statement by all three branches of government recognizing the sovereign's unquestioned power to control who and what may enter the country. However, the Constitution is the "supreme law of the land"[181] with the result that at the periphery, the power of the sovereign and the rights of the individual under the Constitution collide. It is precisely in the border context that the tension between the government's power to "take evidence" pursuant to the border search exception to the Fourth Amendment and an individual's right not to be compelled to "give evidence" pursuant to the Fifth Amendment is most evident.

Under *Boyd*, "private papers" would receive absolute protection. In modern terms, this presumably would extend to its digital equivalent: personal computer data. As discussed earlier, *Boyd*'s broad view is in keeping with the original meaning of "witness" as understood by the Framers, and this would lead to protection of any digital data, including encrypted data. *Boyd* has not been expressly overruled so arguably the Supreme Court could still establish a *Boyd*-like bright-line rule that private data is always protected under the Fifth Amendment. So far the Supreme Court has resisted establishing such a strict demarcation point.

Instead, the Supreme Court favors the factual inquiry framework enunciated in *Fisher*. The *Fisher* framework distinguished testimonial acts in the context of producing subpoenaed documents, which may be privileged, from non-testimonial acts, which never receive Fifth Amendment protection. In the context of encrypted data, the critical question is whether compelled disclosure of the encryption passphrase is subject to the Fifth Amendment privilege against self-incrimination. If a passphrase is written down on paper and the government knows of its existence and location, it would not be protected because voluntarily created documents are

181. U.S. CONST. art. VI, cl. 2.

never protected under *Fisher* and its progeny.[182] The government could subpoena the person to produce the written document with the passphrase or unilaterally seize it.[183] The Fifth Amendment is not implicated because there is no "testimonial" communication involved. But the more interesting situation occurs where the passphrase is not written down on paper and exists only in the mind of the individual. It is helpful to analyze the various situations that may occur at the border.

A. Scenario 1: The Electronic Device Is Not Encrypted

As discussed earlier, the government's expansive search powers at the border allow for searches of electronic devices that are encompassed within the broadly construed meaning of "cargo" in the customs statute. If the electronic device is not encrypted, then a search of the contents of the device does not implicate the Fifth Amendment since there is no "testimonial" communication involved.[184] Rather, the proper analysis concerns the search and seizure provision of the Fourth Amendment. Due to the border search doctrine, a person cannot claim that the Fourth Amendment protects an electronic device from being searched. Thus, the government has the inherent power to inspect and search any property entering the country.

B. Scenario 2: A Portion of the Electronic Device Is Encrypted

In the situation where only a portion of the electronic device is encrypted, there is the possibility that the encryption key[185]

---

182. Fisher v. United States, 425 U.S. 391, 409–10 (1976); *see also Hubbell*, 530 U.S. at 35–36 ("More relevant to this case is the 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."); United States v. Doe (*Doe I*), 465 U.S. 605, 612 n.10 (1984) ("If the party asserting the Fifth Amendment privilege has voluntarily compiled the document, no compulsion is present and the contents of the document are not privileged.").

183. This is assuming, of course, that the person is honest enough or foolish enough to admit that the passphrase was written down on paper. If the written passphrase was completely unknown to exist, then it would be protected under *Hubbell*. Perhaps the easiest solution would be for the target to simply destroy the paper.

184. *Boyd*'s fusion of the Fourth and Fifth Amendments is no longer good law. *See* sources cited *supra* note 109.

185. Typically, the input to an encryption key is in the form of a passphrase. However, the use of biometric data, such as a face, fingerprint, iris or retina, or voice scan, can be used in

may be found in the RAM[186] of the laptop or on disk[187] if the user previously entered the passphrase. Again, a person cannot prevent Customs from performing a search for illegal materials. If Customs agents are successful in discovering the passphrase through a search of the RAM or the storage disk, then they may lawfully "seize" the passphrase and use it to decrypt the encrypted portion.[188] This is completely constitutional under the rubric of the border search exception to the Fourth Amendment.

But what if a portion of the device is encrypted and the government wants access? The fact that the data is concealed through encryption does not place it out of the bounds of Customs.[189] The government, however, cannot physically compel a person to provide the passphrase to decrypt the device; although there is the aspect of tacit compulsion through the threat of seizure of the device, detention of the person for questioning, and possible entry of the person's name into a

---

place of passphrases. For Fifth Amendment purposes, it is vital that the encryption key be a passphrase as the Supreme Court has consistently held that physical evidence (including physical-body evidence) does not implicate the Fifth Amendment. *See supra* Part III.C.

186. RAM refers to Random Access Memory. Passphrases and by extension encryption keys are decrypted in RAM and remain unencrypted in RAM, allowing anyone with access to the laptop to perform a forensic analysis of the contents of RAM by searching for the encryption key. This can only occur if the laptop is on and the user has already entered the passphrase to access their encrypted data. For a discussion of retrieving encryption keys from RAM, see Brian Kaplan, RAM is Key: Extracting Disk Encryption Keys from Volatile Memory (May 2007) (unpublished Master's thesis, Carnegie Mellon University), *available at* http://www.contrib.andrew.cmu.edu/~bfkaplan/KaplanRAMisKeyThesis.pdf.

187. Microsoft Windows uses a swap file as "virtual memory" when there is insufficient RAM. The user has no control over what Windows writes to the swap file, including a passphrase in RAM. In addition, when the user places a laptop in "hibernation" mode, the laptop writes the contents in RAM to disk. A forensic analysis of the contents of the swap or hibernation files on disk could possibly recover the passphrase. Thomas C. Greene, *Clearing Swap and Hibernation Files Properly*, THE REGISTER, May 5, 2007, http://www.theregister.co.uk/2007/05/05/wipe_swap_file/.

188. This was what the Customs agents in *In re Boucher* failed to do. *See In re* Boucher, No. 2:06-mj-91, 2007 WL 4246473, at *1–2 (D. Vt. Nov. 29, 2007). There is growing recognition of the importance of leaving the computer on to seize evidence. Microsoft has developed a tool for law enforcement to search for evidence on-site, which can be useful in the border context, especially when a person voluntarily provides access to an encrypted device. Benjamin J. Romano, *Microsoft Device Helps Police Pluck Evidence from Cyberscene of Crime*, SEATTLE TIMES, Apr. 29, 2008, http://seattletimes.nwsource.com/html/microsoft/2004379751_msftlaw29.html.

189. *See* United States v. Arnold, 523 F.3d 941, 944 (9th Cir. 2008) (quoting United States v. Ross, 456 U.S. 798, 823 (1982) ("[L]uggage carried by a traveler entering the country may be searched at random by a customs officer . . . no matter how great the traveler's desire to conceal the contents may be.")).

government database to be flagged for future secondary inspection every time they cross the border. Still, even if the person does not know if they have incriminating data, they can refuse to cooperate and allow the device to be searched with the likely result that Customs will seize the device. If Customs requests that the individual provide a passphrase to decrypt the data on the electronic device and the person complies, the government now has unfettered access to search, copy, and extract any and all information from that device. In short, cooperation may not be rewarded if incriminating data is discovered that could then be used to indict that person on criminal charges through the reverse probable cause scenario at the border.[190]

If, however, a person refuses to disclose the passphrase, the electronic device will most likely be seized by Customs. A thorough forensic investigation of the device may be successful in producing the encryption key, which the government can then use to decrypt the contents of the device.[191] But if such a search is fruitless, a person can expect to receive a subpoena directing him or her to disclose the passphrase, just like in the *Boucher* case. In response, the person can attempt to invoke the Fifth Amendment privilege against self-incrimination. At this point, the analysis of whether the Fifth Amendment protects a person from disclosing the passphrase to a partially encrypted device merges with the analysis of an electronic device that is entirely encrypted.

C. Scenario 3: The Entire Electronic Device Is Encrypted

With an electronic device completely encrypted, Customs cannot access the contents to perform a search of the data.

---

190. This was the situation in *In re Boucher*. *See In re Boucher*, 2007 WL 4246473, at *1.

191. An innovative means of circumventing encrypted devices has been discovered by a team of researchers at Princeton University and other professionals. The method involves reading the residual traces of the encryption key in RAM at low temperatures when the laptop is in "suspend" mode, locked, or in hibernation mode. J. Alex Halderman et al., *Lest We Remember: Cold Boot Attacks on Encryption Keys*, PROC. 17TH USENIX SECURITY SYMP. (2008), *available at* http://citp.princeton.edu/pub/coldboot.pdf; *see also* John Markoff, *A Method for Stealing Critical Data*, N.Y. TIMES, Feb. 22, 2008, at C1, *available at* http://www.nytimes.com/2008/02/22/technology/22chip.html?ex=1361509200&en=c39d2f67cf1004ca&ei=5088&partner=rssnyt&emc=rss (discussing the findings of the Princeton researchers). However, if the laptop was off, a search can still be performed to see if the encryption key was written to a swap or hibernation file on disk.

There are only two options available: attempt to brute force the passphrase or convince the owner of the electronic device to disclose the passphrase. A brute force approach is infeasible both in time and cost.[192] Thus, Customs must rely on the cooperation of the device owner. If the person refuses, Customs has no other alternative but to compel the person to provide the passphrase in order to access the contents of the device, and this implicates the Fifth Amendment.

Certainly, the physical act itself of entering a passphrase is nontestimonial and would not receive Fifth Amendment protection under current Supreme Court jurisprudence.[193] But the act involves more than simply the physical act alone. It involves disclosing the passphrase, which may have testimonial aspects to it under the *Fisher* framework if it implicitly involves statements of fact by admitting that the evidence exists, is in the person's possession or control, and is authentic.[194] By entering a passphrase, the person will implicitly admit the fact that he or she knows the passphrase, it is within his or her control, and the passphrase is authentic in the sense that it is what the person believes the government wants. In this case, the act of disclosing a passphrase will lead to the inference that the contents decrypted were created and in the control of that person, which may be highly incriminating and therefore testimonial.

The *Hubbell* Court has articulated a "strongbox" analogy that can be useful in determining whether an act is fundamentally testimonial: an act is testimonial if it discloses "the combination to a wall safe" as distinguished from "being forced to surrender the key to a strongbox."[195] In the encryption context, a passphrase is more analogous to a combination to a safe in the sense that both exist only in the mind of the individual.[196] Unlike physical evidence, which exists independently from the person, there is no such separation between a person and his

---

192. *See supra* notes 85–87 and accompanying text.

193. *See* sources cited *supra* note 109.

194. *See* Fisher v. United States, 425 U.S. 391, 409–10 (1976).

195. United States v. Hubbell, 530 U.S. 27, 43 (2000) (citing Doe v. United States (*Doe II*), 487 U.S. 201, 210 n.9 (1988)).

196. *Cf. Doe II*, 487 U.S. at 212–13 (stating that the policies underlying the Fifth Amendment privilege are served "when the privilege is asserted to spare the accused from having to reveal, directly or indirectly, his knowledge of facts relating him to the offense or from having to share his thoughts and beliefs with the Government") (footnote omitted).

or her passphrase. The passphrase is inherently intertwined within the chasms of the mind of the individual. In other words, being compelled to produce a passphrase involves mining and extracting the contents of one's mind and that act itself inherently involves revealing the contents of that mind, which makes it a testimonial communication. This link simply cannot be conceptually severed.

It is arguable that encrypted data is more properly analogized to locking a document in a safe, and therefore, the encrypted data must be produced in an unencrypted, usable form in response to a subpoena.[197] In this sense, the encryption key is similar to a physical key that is used to unlock a safe. But this argument ignores the fact that encryption keys are almost always composed of a passphrase as input and that the passphrase is memorized. A physical key has an independent existence of its own, but a passphrase exists only within an individual's mind. It is this fundamental difference that makes the analogy invalid. Proponents of this "safe" or "strongbox" argument have not provided a satisfying answer to rebut the common scenario where passphrases only exist in the mind of the individual, and therefore, are more akin to a combination to a safe.[198]

Having established that the act of providing a passphrase is testimonial under *Fisher*, the next question is whether a grant of act-of-production immunity can be used to overcome the Fifth Amendment privilege. In such a case, the government can compel production of the passphrase by granting act-of-production immunity, which makes the testimonial compo-

---

197. *See, e.g.*, Phillip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171, 176–77 (1996).

198. *See id.* at 203, 205 (stating that "[a]n unrecorded password poses more difficulties" and that "only truly memorized passwords might defeat the government's subpoena power"). Reitinger claims that "the government is more likely to subpoena recorded passwords than memorized ones" because "keys" are too long to memorize. *Id.* at 204. This is a flawed understanding of how modern encryption works. An encryption key can be composed of a passphrase. The passphrase is combined with random bits to produce the encryption key. Thus, an encryption key itself is not "memorized." *See* Memorandum from B. Kaliski, RSA Labs., PKCS #5: Password-Based Cryptography Specification, at 3–5 (Sept. 2000), http://tools.ietf.org/html/rfc2898. A person can easily remember a passphrase of sufficient length to make it unbreakable so it is not necessary to write it down. It is highly unlikely that an individual would admit to possessing and producing a recorded passphrase in response to a subpoena. Finally, Reitinger's acknowledgment that a memorized passphrase implicates the Fifth Amendment defeats his earlier argument that the government may subpoena encryption keys. *See* Reitinger, *supra* note 197, at 195–96.

nent of the act of producing the passphrase privileged, but does not afford any protection against the government's use of the contents as revealed by the passphrase. The act of producing the passphrase would then be privileged, but the decrypted contents would not be.

As discussed earlier, Justice O'Connor believed that *Fisher* and *Doe I* stood for the proposition that the contents of any voluntarily produced documents are never protected, including private documents.[199] If this is true, the analysis into whether an act is testimonial is virtually moot, as the government is interested in what the act discloses and not the act itself. Alito agreed with Justice O'Connor's view and believed that the government can overcome a claim of the Fifth Amendment privilege by granting act-of-production immunity because the contents of the evidence are never protected.[200]

The Supreme Court decision in *Hubbell*, although not expressly overruling *Fisher* and its progeny, had the effect of restoring much needed protections to the Fifth Amendment. If the government grants act-of-production immunity, thereby making production of the passphrase privileged, the rationale of the *Hubbell* Court leads to the conclusion that this immunity grant must extend to derivative use of the immunized testimony of producing the passphrase. Therefore, in the encryption context, that would lead to the result that the contents decrypted by the passphrase are protected because they were "derived" from the compelled testimonial act of producing the passphrase. The testimonial act of producing the passphrase would certainly be "the first step in a chain of evidence" that would lead to giving the government the necessary evidence to prosecute.[201]

Moreover, in the encryption context, the government cannot make an argument that the foregone conclusion doctrine applies, which would obliterate Fifth Amendment protection. The reasoning of *Hubbell* effectively does away with this doctrine as applied to encrypted devices. *Hubbell* stated that the extent of the government's prior knowledge is the key question in determining whether the foregone conclusion doctrine applies. Because the data is encrypted, the government cannot

199. *See supra* notes 141–43 and accompanying text.

200. *See* Alito, *supra* note 102, at 54–56, 64–65.

201. *See* United States v. Hubbell, 530 U.S. 27, 42 (2000).

possibly have pre-existing knowledge of the contents within the encrypted data.[202] After all, if the information is encrypted, the government cannot even articulate whether the particular materials it is looking for exist.

Thus, so long as the electronic device is entirely encrypted or partially encrypted with no incriminating data or successful retrieval of the encryption key on the portion of the device that is not encrypted, an individual is entitled to Fifth Amendment protection against producing the encryption passphrase or the contents derived from production of the passphrase.

D. Analysis of the Boucher *Case*

1. What the government could have done to avoid Fifth Amendment issues

The *In re Boucher* case is interesting because of its factual scenario, which combines two of the previous scenarios discussed above: first cooperating by providing the passphrase to his laptop, which revealed incriminating child pornography that led to his indictment, and then refusing to provide the passphrase after being indicted. Once Boucher voluntarily agreed to assist the Customs agents by entering the passphrase to the encrypted Z drive, all the agents had to do was simply copy the contents of the laptop's RAM, thereby capturing Boucher's encryption key before turning the laptop off. This would have been entirely constitutional under the border search doctrine. Unfortunately, that was not done. As the agents were not trained in the intricacies of encryption, they failed to recognize the importance of keeping the laptop on once Boucher entered the passphrase, and instead turned the laptop off. With the laptop off, the encryption key was lost and the data re-encrypted itself. The government now had no other reasonable means to access the contents of Boucher's laptop other than having Boucher voluntarily cooperate or forcing him to provide the passphrase.

202. This proposition assumes that the individual does not voluntarily assist the government by providing the passphrase to decrypt the encrypted data.

2. *The Court was wrong to conclude that the government was barred from using any of the evidence it already viewed*

The court in *In re Boucher* was correct in holding that compelling Boucher to enter the passphrase has a testimonial aspect that also precluded the use of the files, which would be decrypted from production of the passphrase because it would be an impermissible derivative use of the testimonial act.[203] This directly follows from *Hubbell* as discussed previously. However, the court erred in its analysis of the critical fact that Boucher voluntarily provided the Customs agents with knowledge of child pornography on his laptop. It is for precisely this reason that Boucher is not entitled to full protection under the Fifth Amendment.

Indeed, the government made the argument that the contents of Boucher's laptop were a foregone conclusion and therefore not privileged under the Fifth Amendment.[204] The existence and location of the pornographic images were already known to the government through Boucher's voluntary actions in showing the Customs agents the incriminating child pornography on his laptop. This complicated the analysis of whether Boucher was entitled to Fifth Amendment protection to more than simply providing a passphrase.[205]

Unlike the case in *Hubbell*, Boucher was not initially compelled to provide the first "link in the chain of evidence," which ultimately led to his prosecution.[206] He voluntarily provided that link himself. It was only subsequent to his assistance that the agents were able to view the incriminating child pornography. By actively assisting the agents, Boucher

---

203. *See In re* Boucher, No. 2:06-mj-91, 2007 WL 4246473, at *5 (D. Vt. Nov. 29, 2007), *rev'd*, No. 2:06-mj-91, 2009 WL 424718, at *4 (D. Vt. Feb. 19, 2009).

204. *Id.*

205. This author disagrees with Professor Orin Kerr's analysis that the encryption passphrase was already a foregone conclusion and therefore the Fifth Amendment was not implicated. *See* Posting of Orin Kerr to The Volokh Conspiracy, http://volokh.com/posts/1197763604.shtml (Dec. 19, 2007, 16:38 EST). Professor Kerr misconstrues the actual issue in the case. The issue is not whether the government knew that Boucher possessed the passphrase. Rather, the proper issue concerns whether the contents of Boucher's laptop were a foregone conclusion. As previously discussed above, revealing or entering a passphrase is inherently a testimonial act and protected under the Fifth Amendment. The more interesting question is the effect of the government's prior knowledge of child pornography on Boucher's laptop.

206. *See Hubbell*, 530 U.S. at 41–42.

planted the seeds, the fruits of which eventually led to his own indictment on child pornography charges.[207]

While it is true that the government did not know of the existence of other files, possibly incriminating in nature, on Boucher's encrypted Z drive, this does not negate the fact that they did know of the existence and location of some files on Boucher's laptop. Forcing Boucher to enter the passphrase would certainly result in the production of all the files on the Z drive, including those that were unknown to the government that "could add much to the sum total of the government's" knowledge.[208] But the mere speculation of what is and what is not incriminating is not determinative here. The court's focus on the quantity of evidence that may be made available to the government misses the mark. The government already had ample evidence that was detrimental to Boucher.

In determining whether the foregone conclusion doctrine applied, the court should have engaged in a comparison between what the government already knew and what Boucher's disclosure of the passphrase would add to the government's prior knowledge.[209] The fact that the government did not know of the existence and location of certain files did not preclude them from being used so long as the government could meet the heavy burden of proving that its knowledge of those files was independently obtained and not "tainted" by Bouch-

---

207. The perils of cooperating with a government investigation before a subpoena is issued are illustrated in the D.C. Circuit's discussion of two cases in *United States v. Hubbell*, 167 F.3d 552, 571 (D.C. Cir. 1999), *aff'd*, 530 U.S. 27 (2000). *Compare* United States v. Rue, 819 F.2d 1488 (8th Cir. 1987) (voluntarily allowing IRS to examine records before subpoena was issued effectively waived Fifth Amendment act-of-production privilege) *with* United States v. Fishman, 726 F.2d 125 (4th Cir. 1983) (refusing to cooperate by not admitting the existence and possession of subpoenaed records did not waive Fifth Amendment privilege). *See also* Cole, *supra* note 177, at 153 n.203.

208. *In re Boucher*, 2007 WL 4246473, at *6.

209. This view is supported by the D.C. Circuit opinion in *Hubbell*. According to the D.C. Circuit, "the government must establish its knowledge of the existence, possession, and authenticity of subpoenaed documents with 'reasonable particularity' before the communication inherent in the act of production can be considered a foregone conclusion." *Hubbell*, 167 F.3d at 579, *aff'd*, 530 U.S. 27 (2000) (citing *In re* Grand Jury Subpoena Duces Tecum, 1 F.3d 87, 93 (2d Cir. 1993)). In applying this "reasonable particularity" test, a comparison is made between what the government knew when the subpoena was issued and what the government learned from the target of the subpoena. *See* Cole, *supra* note 177, at 157–60 (praising the D.C. Circuit for articulating the "reasonable particularity" test as a means of applying the foregone conclusion doctrine). This "reasonable particularity" standard, however, has not been specifically adopted by the Supreme Court, but much of the Court's discussion in *Hubbell* parallels the analysis undertaken by the D.C. Circuit.

er's revelation. The government may not have been able to meet this burden as to its prior knowledge of the new files produced by Boucher, but certainly the knowledge it gained through Boucher's own prior actions was sufficient for the files it did know about. *Hubbell* made clear that where the government cannot specify what it already knows and therefore wants, the government cannot gain this information through a broadly worded subpoena. That would be an impermissible fishing expedition. For files of which the government had no prior knowledge, the government would bear the heavy burden of proving that the files were obtained independently.

By misconstruing the quantity continuum of the foregone conclusion doctrine, the court prevented the government from indicting Boucher based on what it already knew of the existence and location of the child pornography on his laptop. Merely speculating as to the quantity of incriminating evidence is not enough. The foregone conclusion doctrine did not necessitate a wholesale bar on files for which the government knew the existence and location in addition to the files that it did not know existed.[210]

---

210. Recently, the U.S. District Court for the District of Vermont released an opinion concerning the government's appeal of the Magistrate Judge's opinion in *In re Boucher* (*Boucher I*), No. 2:06-mj-91, 2007 WL 4246473 (D. Vt. Nov. 29, 2007). *In re* Boucher (*Boucher II*), No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009). The District Court seems to agree with the conclusion in the analysis above that it was already a foregone conclusion as to the child pornography files the Customs agents viewed. *Id.* at *3. However, in a rather short and cursory opinion, the District Court reversed the Magistrate Judge's opinion and held that Boucher must "provide an unencrypted version of the Z drive viewed by the ICE agent." *Id.* at *4. By doing so, the District Court took an almost polar opposite view from that espoused by the Magistrate Judge. Similar to this author's analysis of the *Boucher I* case above, this author believes that the District Court erred in *Boucher II* by claiming that the government already knew "of the existence and location of the Z drive and its files." *Id.* at *3. This is precisely the kind of fishing expedition that the *Hubbell* Court rejected. In *Hubbell*, the Supreme Court stated that a broad-based belief of certain materials is not enough for application of the forgone conclusion doctrine. *See Hubbell*, 530 U.S. at 45. The government must be able to specify that it knew such materials existed and where they were located. *Id.* In this case, the government only knew the existence and location of some of the child pornography files. Contrary to the District Court's assertion that the contents of the entire decrypted Z drive would not add much to the sum total of the government's knowledge, it could in fact add considerably if Boucher had many more incriminating files than were previously viewed by the Customs agents. The District Court should have performed the same analysis and held that Boucher must only produce the files of which the government already had prior knowledge.

V. IMPLICATIONS OF PROVIDING FIFTH AMENDMENT PROTECTION TO ENCRYPTED DATA

The idea of providing absolute or near-absolute protection to encrypted devices is not an easy proposition in the context of today's security-conscious world where national security is at the forefront of any discussions concerning the border. But as in past crises and exigencies, this does not mean that we must derogate our rights under the Constitution. The Fifth Amendment forbids any compulsion to produce self-incriminating evidence.

Providing protection for the use of encryption does not, however, lead to the conclusion that people are free to cross the border with impunity. All it means is that the government cannot compel a person to give incriminating evidence that could then be used in prosecuting that person. The government is still free to use its vast resources to pursue other investigative techniques to gain access to encrypted devices, such as obtaining a search warrant to surreptitiously enter a home and install a keystroke logging device or hidden camera to capture the passphrase as it is entered.[211] In doing so, this would strike a balance between the government's power under the Fourth Amendment to "take evidence" and a person's constitutional right not to "give evidence" under the Fifth Amendment.

Searching electronic devices at the border to protect the nation from illicit digital materials is an illusory measure at best. Criminals and terrorists can easily circumvent border inspection of electronic devices by not carrying any incriminating evidence on their devices to avoid scrutiny. Then, once they safely pass border inspection, they can download the materials from the Internet.[212] No sophisticated criminal or terrorist would draw unnecessary attention to him- or herself through the use of encryption.

---

211. *See* United States v. Forrester, 512 F.3d 500 (9th Cir. 2008) (government used various computer surveillance techniques, including keyloggers, to monitor defendants' email and internet activity which was used as evidence to indict defendants on charges relating to the manufacture of the drug Ecstasy); United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001) (FBI installed a keylogging device on Scarfo's computer to obtain the passphrase to his encrypted business records detailing illegal gambling and loansharking).

212. The past few years have seen an explosion in the availability of free mass storage on the Internet. Free email providers, such as Google, Yahoo, and Microsoft routinely provide gigabytes of storage, while others such as AOL provide unlimited storage capacity.

In addition, criminals[213] and terrorists[214] could just resort to low-tech means to avoid arousing suspicion, such as using invisible ink.[215] This has the benefit of hiding communications in common, everyday documents that are unlikely to draw more than a cursory glance or inspection. Terrorists could also transmit critical messages using human couriers across borders.[216] This has the dual advantage of both using trusted sources and adding to a nascent terrorist cell in another country. Considering that front-line airport screeners, who are supposed to be well trained in bomb detection, have performed poorly in detecting fake bombs, these low-tech methods may be quite successful in thwarting detection.[217]

CONCLUSION

Encryption presents a unique challenge to the sovereign's power to police its borders. It is undeniable that the government has an interest in controlling who and what may enter the country. The border search exception to the Fourth Amendment emphatically reveals the plenary search powers of the government at the border. However, the use of encryp-

---

213. The Aryan Brotherhood gang was able to communicate with members in prison using invisible ink. Brian Kates, *Aryan Prison Gang Links with Mafia*, N.Y. DAILY NEWS, Nov. 3, 2002, http://www.nydailynews.com/archives/news/2002/11/03/2002-11-03_aryan_prison_gang_links_with.html.

214. A suspected al-Qaeda operative was recently apprehended in Britain with a contacts book listing other al-Qaeda members written in invisible ink. Daily Mail Reporter, *British Muslim 'Had Al Qaeda Contacts Book with Terrorists' Numbers Written in Invisible Ink,'* MAIL ONLINE, Sept. 24, 2008, http://www.dailymail.co.uk/news/article-1061190/British-Muslim-Al-Qaeda-contacts-book-terrorists-numbers-written-invisible-ink.html; Russell Jenkins, *Terrorist Contact Book Hid Information on Al-Qaeda Leaders in Invisible Ink, Trial Told*, TIMES ONLINE, Sept. 25, 2008, http://www.timesonline.co.uk/tol/news/uk/crime/article4821501.ece.

215. The CIA has refused to declassify invisible ink technology. Presumably, this means that the use of invisible ink is still relevant. Bill Miller, *The Very Visible Battle over Invisible Ink*, L.A. TIMES, June 13, 2001, § Southern California Living, at 2, *available at* http://articles.latimes.com/2001/jun/13/news/cl-9673.

216. Osama Bin Laden has been known to avoid electronic communications and, instead, rely on human couriers to transmit messages. Craig Whitlock, *In Hunt for Bin Laden, a New Approach*, WASH. POST, Sept. 10, 2008, at A01, *available at* http://www.washingtonpost.com/wp-dyn/content/story/2008/09/09/ST2008090903480.html.

217. Thomas Frank, *Most Fake Bombs Missed by Screeners*, USA TODAY, Oct. 18, 2007, at 1A, *available at* http://www.usatoday.com/news/nation/2007-10-17-airport-security_N.htm; Lisa Myers et al., *Airline Screeners Fail Government Bomb Tests*, MSNBC.COM, Mar. 17, 2006, http://www.msnbc.msn.com/id/11863165/.

tion technology in electronic devices denies the government this rightful power to search for things it wants to keep out.

Yet the Fifth Amendment prohibits the compulsion of a person to give self-incriminating evidence. Despite the Supreme Court's narrowing of the Fifth Amendment privilege in the years after *Boyd*, the Court's decision in *Hubbell* has reinvigorated the Fifth Amendment to give us the protections that are enshrined in the Constitution. In fact, the *Hubbell* decision can be viewed as encouraging full encryption of electronic devices for two reasons. The first is that disclosing an encryption passphrase will always be a testimonial act because it reveals the contents of one's mind and is therefore protected under the Fifth Amendment. Second, the more of the device that is encrypted, the more difficult it would be for the government to search for incriminating evidence that can be used to nullify any claim of the Fifth Amendment privilege under the *Fisher* foregone conclusion doctrine. Therefore, the Fifth Amendment provides an independent basis for the protection of encrypted private data at the border.

It is true that current court cases involving border searches of electronic devices have uncovered repugnant child pornography, and perhaps future cases may see the seizure of smoking gun terrorist materials. The possibility that criminals and terrorists may thwart law enforcement by gaining constitutional protection for encrypted devices may be untenable to some, in light of present concerns over national security. The remedy, though, must be addressed through Congress and not the courts.[218]

These cases, however, may just be the harbingers of what lies ahead. To help guide us, it would be wise to heed the words of Justice Frankfurter many years ago: "It is a fair summary of history to say that the safeguards of liberty have frequently been forged in controversies involving not very

218. The United Kingdom has taken steps to curtail the domestic use of encryption. The Regulation of Investigatory Powers Act 2000 (RIPA) was passed by Parliament to meet the challenges faced by law enforcement of new technology. A "Section 49" notice requires that the person produce the encryption key or produce the data in decrypted form. Regulation of Investigatory Powers Act, 2000, c. 23, § 49 (U.K.), *available at* http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1. For a discussion of the first case under RIPA requiring production of encryption keys, see Mark Ward, *Campaigners Hit by Decryption Law*, BBC NEWS, Nov. 20, 2007, http://news.bbc.co.uk/1/hi/technology/7102180.stm.

nice people."[219] Those words are just as relevant today as they were then.

219. United States v. Montoya de Hernandez, 473 U.S. 531, 548 (1985) (Brennan, J., dissenting) (quoting United States v. Rabinowitz, 339 U.S. 56, 69 (1950) (Frankfurter, J., dissenting)).