Harvard Journal of Law & Technology
Volume 22, Number 2 Spring 2009

PROTECTING PRIVACY THROUGH A RESPONSIBLE DECRYPTION POLICY

Andrew J. Ungberg[*]

TABLE OF CONTENTS

I. INTRODUCTION

In late December 2006, Sebastien Boucher crossed into Vermont from Canada.[1] At the border, customs officials inspected Boucher's car and found a laptop in the back seat.[2] A customs agent accessed the computer without entering a password and initiated a search for media files; the query returned tens of thousands of images.[3] Later, a special agent continuing the investigation found "thousands of images of adult pornography and animation depicting adult and child pornography."[4]

∗ Harvard Law School, Candidate for J.D., 2010; B.S., University of Connecticut, School of Business, 2007. Special thanks to Doug Kochelek for his encouragement, Joshua Gruenspecht for his technical expertise, the Student Writing Committee of the *Harvard Journal of Law & Technology* for their insightful comments, and Jessica Nachman and the members of the Article team for their hard work, without whom this Note could not have been published.

1. *In re* Boucher (*Boucher I*), No. 2:06-mj-91, 2007 WL 4246473, at *1 (D. Vt. Nov. 29, 2007).
2. *Id.*
3. *Id.*
4. *Id.*

At this point, Boucher was detained, read his Miranda rights, and questioned by the agents.[5] At their request, Boucher showed the investigators where his downloaded files were located on the laptop.[6] The agents did not see Boucher enter any password in order to access the files, which were maintained on a hard drive designated as drive Z.[7] After the agents found several pornographic images and videos of children, they seized the laptop and arrested Boucher.[8]

Several days later, officers accessed the laptop and created a mirror image of the hard drive, yet they were unable to access drive Z because it was protected by an encryption algorithm.[9] An agent versed in computer forensics examined the drive and later testified that it would be virtually impossible to access the files,[10] as it would take years to unlock the drive without a password.[11] The grand jury subpoenaed Boucher, demanding that he "provide all documents, whether in electronic or paper form, reflecting any passwords used or associated with the [computer in question]."[12]

Boucher resisted the subpoena, stating that it violated his Fifth Amendment right against self-incrimination.[13] Initially, Magistrate Judge Niedermeier found that forcing Boucher to disclose the password would effectively compel him to testify against himself[14] and quashed the subpoena.[15] Although Chief Judge Sessions later overturned that decision,[16] the original order would have left law enforcement agents unable to catalogue or present as evidence the illegal pornography they knew Boucher possessed.[17]

Boucher is hardly the first time the government has grappled with the seemingly modern issue of data encryption. In 1776, then General George Washington discovered his Chief of Hospitals was sending coded letters to the British concerning the colonial army's supply levels and troop movements.[18] During Aaron Burr's trial for treason in the early 1800s, prosecutors requested that his secretary decipher Burr's personal correspondence, only to have the secretary refuse on

---

5. *Id.*
6. *Id.*
7. *Id.*
8. *Id.* at *2.
9. *Id.*
10. *Id.*
11. *Id.*
12. *Id.*
13. *Id.*
14. *Id.* at *3.
15. *Id.* at *6.
16. *In re* Boucher (*Boucher II*), No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009). Chief Judge Sessions overturned Magistrate Judge Niedermeier's ruling based on the fact that Boucher had voluntarily permitted law enforcement agents to access his computer at the United States border. *Id.* at *4–5.
17. *Boucher I*, 2007 WL 4246473, at *5.
18. DAVID KAHN, THE CODEBREAKERS 175–76 (1967).

Fifth Amendment grounds.[19] However, in each of these cases the government was able to recover the sought-after information simply by breaking the encryption code.[20] Today, the widespread availability of powerful encryption software guarantees that law enforcement will increasingly confront this problem without the ability to break the code in a reasonable amount of time.

Although Chief Judge Sessions permitted law enforcement access to the encrypted files, his ruling depended largely on the fact that Boucher had already voluntarily provided agents with access.[21] Absent this fact, law enforcement would be left facing practically unbreakable encryption with no reasonable recourse to secure important evidence.[22] This Note argues that the magistrate judge's analysis in *Boucher I* mischaracterizes the encryption issue. Consequently, the analysis leads to judgments like the court's initial order in *Boucher I*. Such rulings create incentives for the government to press the boundaries of its police power and to develop law enforcement methods that rely on invasive covert surveillance, which ultimately represents a greater threat to individual privacy than the government's attempt to compel computer decryption.

This Note suggests that a wiser approach would involve creating a procedure by which the government could gain access to encrypted information under judicial oversight and with reasonable protections for individual privacy. Part II briefly discusses encryption and the capabilities of modern encryption software, as well as the practical limitations faced by law enforcement when confronting encrypted data. Part III examines the act of production doctrine, the system of analysis used by the magistrate judge in *Boucher I*, and ultimately suggests that it proves an inadequate tool for resolving the encryption issue. Part IV reviews both the Fifth Amendment's animating purposes and the compromises struck between the needs of law enforcement and the protection of individual privacy. It then suggests desirable features of a new decryption policy and proposes a modified search warrant requirement and statutory civil remedy for abuse of the process. Part V concludes.

---

19. United States v. Burr (*In re* Willie), 25 F. Cas. 38, 39 (C.C.D. Va. 1807) (No. 14,692e).

20. *E.g.*, KAHN, *supra* note 18, at 175–76 (detailing Washington's successful efforts to have the code broken).

21. *Boucher II*, 2009 WL 424718, at *4–5. *See infra* Part III.B.

22. *Boucher I*, 2007 WL 4246473, at *5.

II. ENCRYPTION

Cryptography, the study and practice of encryption, has existed in some form for nearly 4000 years.[23] Encryption is the process of concealing information, and all such systems have several similar characteristics. At its most basic level, encryption involves transforming information or data, called "plaintext," into a coded form that cannot be understood by outsiders.[24] The process is performed according to the encryption algorithm, a set of rules that governs how the plaintext is transformed.[25] While this can be as simple as substituting each letter in a message with a corresponding number,[26] modern encryption algorithms often consist of a complex series of mathematical functions.[27] Regardless of the manner of encryption, the result is that the plaintext is made unintelligible to outsiders.[28] The ability to conceal information from outsiders makes encryption an attractive tool for criminals, especially when their schemes involve recordkeeping or sending secured communication between coconspirators.

Encryption must be reversible in order to be useful as a method of storing or sending secured information. Most modern encryption systems employ a key that must be applied to the chosen encryption algorithm to recover the plaintext.[29] Today's keys consist of a lengthy string of numbers because of their foundation in complex mathematics.[30] The keys can consist of hundreds of numbers, but for ease of administration some modern encryption programs tie a key to a chosen password, such that entering a password into the system is functionally identical to entering the long key.[31]

Law enforcement agents seeking to recover coded information employ "cryptanalysis," the study of breaking and bypassing encryption.[32] Encryption systems generally have three main areas of vulnerability.[33] First, an outsider might try entering every possible key for the system — this is known as a "brute-force" attack and, depending on the complexity of the system, can require an extraordinary amount

---

23. *See generally* KAHN, *supra* note 18, at 71–105 (describing the earliest forms of cryptography that arose in ancient civilizations).

24. *Id.* at xiii.

25. RICK LEHTINEN ET AL., COMPUTER SECURITY BASICS 141 (2d ed. 2006).

26. *See, e.g.*, KAHN, *supra* note 18, at 113.

27. *See* LEHTINEN, *supra* note 25, at 141–42.

28. KAHN, *supra* note 18, at xiii.

29. LEHTINEN, *supra* note 25, at 141–42.

30. *Id.*

31. *See* PGP Whole Disk Encryption FAQ, http://www.pgp.com/products/wholediskencryption/#faq4 (follow "FAQ" hyperlink; then follow "What is the end-user experience?" hyperlink) (last visited May 15, 2009) (noting that the encryption system can seamlessly integrate with the standard Windows log-in screen).

32. *See* KAHN, *supra* note 18, at xv–xvi.

33. A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 887 (1995).

of time and resources.[34] Broadly speaking, the longer the key, the more time is needed to break the encryption.[35] Second, an outsider might analyze the underlying algorithm, looking for weaknesses or patterns in the mathematics that allow him to make educated guesses about the process.[36] In this way, the outsider can partially "solve" the algorithm and reduce the amount of time required to break the encryption by trying only those keys that his analysis suggests might be successful. This method is faster than a brute-force attack, but such analysis of modern encryption software would require an advanced understanding of theoretical mathematics and computer science.[37] Third, an outsider might steal the key to yield the plaintext; the encryption is only as secure as the secrecy of its key.[38]

The primary problem for law enforcement is the fact that modern encryption software is extremely difficult to break. For example, a brute-force attack on the widely available PGP encryption suite could take billions of years.[39] Furthermore, the underlying algorithms are incredibly complex, and "solving" them is far beyond realistic capabilities of law enforcement.[40] Practically speaking, encryption today is impenetrable insofar as it cannot be bypassed by available means within a reasonable amount of time. In the face of such encryption, often the government's only recourse is to obtain the password from the suspect himself. As in the *Boucher* case, this option almost certainly invites a Fifth Amendment challenge, as courts have conceived of compelled computer decryption as falling under the act of production doctrine.

---

34. *Id*. at 887–88.

35. *Id.*

36. *Id.* at 887. For example, in the letter-number replacement system mentioned above, an attacker might analyze the encrypted text, noting how often each number appears. With this information, the attacker then assumes the most frequently appearing number is used to represent the most frequently used letter in the given language. Thus, the attacker begins cracking the encryption by trying letter-number substitutions that are more likely to yield the plaintext based on his analysis of the encrypted text.

37. The actual math behind modern encryption is complicated and beyond the scope of this article. Encryption algorithms use prime numbers to scramble the plaintext. *See* Paul Horowitz et al., *The Law of Prime Numbers*, 68 N.Y.U. L. REV. 185, 186–89 (1993).

38. Froomkin, *supra* note 33, at 887.

39. *Id.* at 887–88 (discussing 128-bit encryption); *see* PGP Whole Disk Encryption Technical Specifications, http://www.pgp.com/products/wholediskencryption/ (follow "Technical Specifications" hyperlink) (last visited May 15, 2009) (featuring 256-bit encryption keys).

40. *See supra* note 37 and accompanying text. Analyzing an encryption algorithm involves complex prime-composite factoring, which is the realm of theoretical mathematics and far beyond the ability of law enforcement. *See, e.g.*, Dan Boneh, *Twenty Years of Attacks on the RSA Cryptosystem*, 46 NOTICES AM. MATHEMATICAL SOC'Y 203 (1999), *available at* http://www.ams.org/notices/199902/boneh.pdf (discussing unsuccessful attacks on the RSA encryption system and the methods and mathematics upon which they have relied). "Although factoring algorithms have been steadily improving, the current state of the art is still far from posing a threat to the security of RSA . . . . Factoring large integers is one of the most beautiful problems of computational mathematics . . . ." *Id.* at 204.

III. DOCUMENT PROTECTION AND THE ACT OF PRODUCTION DOCTRINE

In relevant part, the Fifth Amendment reads, "[n]o person . . . shall be compelled in any criminal case to be a witness against himself."[41] The act of production doctrine is an offshoot of this privilege that protects the accused from having to hand over incriminating personal writings to investigators. Judges have handled compelled data decryption under the umbrella of this doctrine largely because they have analogized an encrypted hard drive to a virtual wall safe from which the accused is asked to remove incriminating papers.[42]

The basis for the doctrine was first introduced in *Boyd v. United States*, in which the Supreme Court extended Fifth Amendment protection to incriminating writings made by the defendant's hand.[43] In *Boyd*, the government issued subpoenas for the defendant's business invoices during a smuggling investigation and later used the invoices to convict him at trial.[44] The Court reversed and read the Fifth Amendment broadly, holding that "compulsory production of the private books and papers of [the defendant] . . . is compelling him to be a witness against himself."[45] Additionally, the Court foreclosed the government's ability to simply take the evidence by force, as "the seizure of a man's private books and papers to be used in evidence against him is [not] substantially different from compelling him to be a witness against himself."[46]

However, during the early twentieth century, the government's increased attention to white-collar crimes necessitated increased access to documents.[47] In turn, the Court became more willing to interpret the Fifth Amendment to accommodate the needs of law enforcement.[48] Although the holding in *Boyd* remained good law well into the twentieth century, it made for strange bedfellows with some of the Court's decisions in more recent Fifth Amendment cases. In these cases, the Court began to draw a sharp distinction between compelling "testimony" on the one hand and using the accused as a source

---

41. U.S. CONST. amend. V. Throughout this Note, the Author will use "the privilege" or "Self-Incrimination Clause" as shorthand for this particular clause of the Fifth Amendment.

42. *E.g.*, *In re* Boucher (*Boucher I*), No. 2:06-mj-91, 2007 WL 4246473, at *3–4 (D. Vt. Nov. 29, 2007).

43. 116 U.S. 616, 634–35 (1886).

44. *Id.* at 617–18.

45. *Id.* at 634–35.

46. *Id.* at 633.

47. *See* William J. Stuntz, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 859–60 (2001) (analogizing the significance of "damning documents" in a white-collar investigation to the body in a murder investigation).

48. *See* Hale v. Henkel, 201 U.S. 43, 70 (1906) (addressing the necessary limits of the Fifth Amendment and failing to find that its protection extends to an agent who refuses to testify against the corporation).

of real evidence such as hair samples or blood-alcohol content on the other. Under its decision in *Schmerber v. California*, the Court held that the Fifth Amendment only protected individuals against compelled testimony.[49] Justice Black wrote in dissent, "[i]t is a strange hierarchy of values that allows the State to extract a human being's blood to convict him of a crime because of the blood's content but proscribes compelled production of his lifeless papers."[50]

The Supreme Court finally overruled *Boyd* and established the foundation of the modern act of production doctrine in *Fisher v. United States*.[51] In that case, the IRS subpoenaed tax documents that were in the possession of the defendant's attorneys.[52] In line with the holdings of *Schmerber* and its progeny, the Court stated "[i]t is . . . clear that 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."[53] While a writing can be testimonial, the Court in *Fisher* found that the tax documents had not been compelled because the defendants prepared them voluntarily.[54] The Court then held that the Fifth Amendment did not apply because the subpoena did not force the taxpayers to testify regarding the documents, but rather it required them simply to hand the documents over to investigators.[55] Several years later, Justice O'Connor tersely noted in a concurring opinion that "the Fifth Amendment provides absolutely no protection for the contents of private papers of any kind."[56]

Although the Court foreclosed any claim to the privilege for voluntarily prepared documents, *Fisher* did not completely strip away the privilege's protection for an individual facing a subpoena duces tecum. The Court recognized that while the content of the incriminating documents was not privileged, the act of producing the documents itself might communicate facts.[57] Producing documents in response to

---

49. 384 U.S. 757, 764–65 (1966).

50. *Id.* at 775 (Black, J., dissenting).

51. 425 U.S. 391 (1976).

52. *Id.* at 394. The Court's analysis is somewhat circuitous. The defendants invoked the attorney-client privilege, claiming they gave the documents to their attorneys in order to obtain legal advice. *Id.* at 402. The Court reasoned that the attorney-client privilege would shield the documents only if the defendants themselves could have resisted production under the Fifth Amendment. *Id.* at 404. Accordingly, Justice White's opinion analyzed whether the privilege applied to the documents when in the hands of the defendants themselves. *See id.* 405–14.

53. *Id.* at 408.

54. *Id.* at 409–10.

55. *Id.* at 409 ("[The subpoena] does not compel oral testimony; nor would it ordinarily compel the taxpayer to restate, repeat, or affirm the truth of the contents of the documents sought.").

56. United States v. Doe (*Doe I*), 465 U.S. 605, 618 (1984) (O'Connor, J., concurring) (writing to explicitly "sound [] the death knell for *Boyd*").

57. *Fisher*, 425 U.S. at 410–11.

a subpoena implicitly cedes the existence of the documents, the defendant's control over them, and the defendant's belief that the documents are in fact the ones the government seeks.[58] The privilege applies when the act of production communicates information, and as a result, an individual may resist the subpoena.[59] This is the facet of document production that ensnares the analysis of compelled decryption. While the documents on Boucher's computer are not protected under *Fisher*, Magistrate Judge Niedermeier noted that "[e]ntering a password into the computer implicitly communicates facts. By entering the password Boucher would be disclosing the fact that he knows the password and has control over the files on drive Z."[60]

The defendants in *Fisher* were in a similar situation to Boucher, but the Court upheld the document production order in *Fisher* under an implicit exception to the act of production rule — namely, the facts communicated by the act proved to be irrelevant to the government's case.[61] The information was a "foregone conclusion," as the investigators already knew the tax documents existed and that they were within the defendant's control; as such, the information was not incriminating and therefore did not trigger the protections of the Fifth Amendment.[62] On review, Chief Judge Sessions seized upon this rationale to overturn Judge Niedermeier's initial order. To him, the fact that Boucher had permitted investigators to see at least some of the child pornography on his hard drive sufficed to render the existence of all the illegal files a "foregone conclusion."[63]

A. The Doctrine Today

Courts have analyzed whether document production implicates Fifth Amendment protection along a spectrum of cases, with the *Fisher* decision standing at one end, and a later Supreme Court decision, *United States v. Doe* (*Doe I*),[64] at the other. Production is nontestimonial when the government has specific knowledge of the files

58. Richard A. Nagareda, *Compulsion "To Be a Witness" and the Resurrection of* Boyd, 74 N.Y.U. L. REV. 1575, 1595 (1999).

59. *Doe I*, 465 U.S. at 612–14.

60. *In re* Boucher (*Boucher I*), No. 2:06-mj-91, 2007 WL 4246473, at *3 (D. Vt. Nov. 29, 2007).

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

62. *Id.* ("[T]he taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers . . . . '[T]he question is not of testimony but of surrender.'").

63. *In re* Boucher (*Boucher II*), No. 2:06-mj-91, 2009 WL 424718, at *4 (D. Vt. Feb. 19, 2009). Initially, Judge Niedermeier had rejected the government's foregone conclusion argument on the grounds that although investigators had seen *some* of the child pornography on Boucher's hard drive, they would gain access to *all* documents on the computer if given the password. *Boucher I*, 2007 WL 4246473, at *5–6.

64. 465 U.S. at 605.

it has subpoenaed,[65] but where the government is fishing for new information, the Fifth Amendment shields the content by preventing production.[66] This spectrum was later refined in *United States v. Hubbell*.[67]

In *Doe I*, the Court upheld the privilege as asserted by a business owner, holding that the privilege could be asserted when the government sought document production with a subpoena that was overly broad.[68] Because the existence and control of the documents were not foregone conclusions as they were in *Fisher*, the defendant successfully moved to quash the subpoena.[69] The Court affirmed that the government was merely fishing for documents it suspected an average business owner might possess, rather than seeking documents of which the government had particularized prior knowledge.[70] The Court in *Hubbell* reinforced *Doe I* on this point and clarified *Fisher* by flatly rejecting the government's argument that the existence of the subpoenaed documents was a foregone conclusion simply because "a businessman such as [Hubbell] will always possess general business and tax records."[71]

Hubbell also dealt with the government's attempts to obtain the contents of documents through the creative use of an immunity agreement.[72] Jailed at the time pursuant to a plea agreement, Hubbell was served with a subpoena duces tecum by investigators seeking to uncover whether he had proffered false testimony earlier in the investigation.[73] After initially resisting the subpoena on Fifth Amendment grounds, Hubbell produced more than 13,000 pages of records upon securing an immunity agreement.[74] Despite the agreement, federal prosecutors used the content of Hubbell's disclosed documents to charge him with a variety of tax crimes and wire fraud.[75] The district court dismissed the case, finding that the government violated the immunity agreement.[76] On appeal, the appellate court remanded the

65. *Fisher*, 425 U.S. at 411 (noting that production would "add[] little or nothing to the sum total of the Government's information").

66. *Doe I*, 465 U.S. at 613 & n.12 (quoting the Third Circuit below, which noted that the government provided no evidence of knowledge that defendant actually possessed or controlled the documents referenced in the subpoena at issue).

67. 530 U.S. 27 (2000).

68. *Doe I*, 465 U.S. at 613 & n.12, 614 (upholding the appellate court's analysis of the government's subpoena).

69. *Id.* at 617.

70. *Id.* at 613 & n.12, 614.

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

72. *Id.* at 30. The government can overcome a Fifth Amendment challenge and compel an individual to answer questions by granting immunity, which renders a statement not incriminating. *See* Kastigar v. United States, 406 U.S. 441, 442 (1972).

73. *Hubbell*, 530 U.S. at 30–31.

74. *Id*. at 31; *see* 18 U.S.C. § 6002 (2006).

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

76. *Id.* at 31–32.

case and instructed the lower court to determine the degree to which investigators were aware of Hubbell's incriminating finances *prior* to his production of the subpoenaed documents.[77] The court reasoned that if investigators could demonstrate knowledge of the wrongdoing independent of information gained from the content of Hubbell's production, then the immunity agreement would not have been violated.[78]

The Supreme Court upheld the appellate decision, highlighting the extraordinary testimonial significance of Hubbell's production.[79] Writing for the majority, Justice Stevens noted that the effort required of Hubbell to produce thousands of documents "[was] the functional equivalent of the preparation of an answer to either a detailed written interrogatory or a series of oral questions at a discovery deposition."[80] This language is hard to square with *Fisher*, which suggested that the Fifth Amendment protected only the act of production itself. Conversely, *Hubbell* seems to take into account the number and type of documents to be produced and the difficulty in preparing them for production. Scholarly debate continues over how to reconcile the holdings of these two cases, and their implications for the act of production doctrine going forward.[81] Regardless, it is enough that *Hubbell* stands for the proposition that the government cannot simply immunize the act of production to gain access to the document's contents.

Working encryption into the *Fisher-Doe I* document production spectrum would be difficult but for the Court's decision in *Doe v. United States* (*Doe II*).[82] In *Doe II*, federal agents subpoenaed several banks in the Cayman Islands for the defendant's bank records while investigating a white-collar crime.[83] The banks resisted, citing local law that prohibited disclosure of personal financial information without the customer's consent.[84] The government then subpoenaed the

77. *Id.* at 32–33.

78. *Id.* The "derivative use" immunity provided by 18 U.S.C. § 6002 does not prevent the government from prosecuting a crime using incriminating evidence that was discovered — or would have been discovered — without using any of the content of the immunized testimonial production. *See* Kastigar v. United States, 406 U.S. 441, 453 (1972).

79. *See Hubbell*, 530 U.S. at 41–42, 46.

80. *Id.* at 41–42.

81. *See, e.g.*, 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, 190–92 (2002) (praising the practical effects of *Hubbell*: overturning *Fisher* and restoring "meaningful" Fifth Amendment protections); Stuntz, *supra* note 47, at 865 (downplaying *Hubbell*'s importance by noting that the government can still simply obtain a search warrant to seize the evidence that it wants); H. Richard Uviller, *Foreword:* Fisher *Goes on the Quintessential Fishing Expedition and* Hubbell *Is Off the Hook*, 91 J. CRIM. L. & CRIMINOLOGY 311, 312 (2001) (expressing bewilderment at the *Hubbell* decision, which rejected author's "clear understanding" of *Fisher*).

82. 487 U.S. 201 (1988).

83. *Id.* at 202–03.

84. *Id.* at 203.

defendant for his signature on a consent form,[85] which the defendant refused to provide on the grounds that signing would constitute self-incrimination.[86] The Court held that signing the form did not have testimonial significance because it did not express the accused's belief as to whether the accounts existed.[87] The Court instead noted that the form instructed the bank to "do something," but that it did not assert any facts, and as such the Fifth Amendment was of no avail.[88] Justice Stevens, the lone dissenter in *Doe II*, disagreed with the analysis, stating that while the accused may "be forced to surrender a key to a strongbox . . . he [cannot] be compelled to reveal the combination to his wall safe."[89] Still, commentators struggle to square the *Doe II* decision with *Doe I* and *Fisher*,[90] leaving unanswered the question of how different a computer password is from a bank authorization order. In *Boucher*, as in *Doe II*, a significant source of real evidence is shielded by a comparatively insignificant testimonial communication. It is not clear why a computer password should be held sacrosanct when a signature is not.

B. Encryption Does Not Fit Neatly into the Act of Production Doctrine

While certain facts of *Boucher* suggest analogues to the act of production doctrine, the present doctrine may not be best suited to resolve the questions presented here. Entering a password into a computer seems analogous to the bank authorization of *Doe II*, but a computer cannot independently "do something" regarding Boucher's right to access in the same way a bank manager can. When Boucher is forced to proffer the password, the production will tacitly admit that he controls *all* the files on his computer, despite agents only knowing of *some* files with certainty. Yet, two seasoned federal judges contemplated this inevitability and still disagreed on whether the existence and control of the files constituted a "foregone conclusion" under *Fisher*.[91] The document production analysis presents broader

85. *Id.* at 204 n.2.
86. *Id.* at 203–04.
87. *Id.* at 215–16.
88. *Id.* at 216–17.
89. *Id.* at 219 (Stevens, J., dissenting).
90. *See, e.g.*, Cole, *supra* note 81, at 147–49 (noting that the Supreme Court's lack of detail in *Fisher* and *Doe I* created difficulties for lower courts in administering the "basic discovery device for federal criminal investigations"); Arthur B. Laby, Note, *Fishing for Documents Overseas: The Supreme Court Upholds Broad Consent Directives Against the Claim of Self-Incrimination*, 70 B.U. L. REV. 311, 320–22, 329–34 (1990) (critiquing *Doe II* as inconsistent with both *Fisher* and *Doe I*, and disputing the Court's implicit analogies to *Schmerber*).
91. Chief Judge Session's order specifically refused to decide the issue regarding files that agents had not viewed, leaving open the question whether decrypting the computer opens the door to every file contained therein, including documents and contraband of

problems for encryption. For example, under *Schmerber*, law enforcement is presumably free to take biometrics, such as fingerprints and retinal scans, which some encryption programs use instead of passwords.[92] It makes little sense to allow the government's ability to decrypt computers to turn arbitrarily on the authentication method of an encryption program.

Even a return to the broader protections of *Boyd* would do nothing to answer the question of whether the protection afforded to papers and effects extends to contraband like child pornography. Some commentators argue that the government could potentially compel passwords with an appropriate grant of immunity,[93] and others maintain that the government can never compel disclosure absent the strenuous requirements of *Fisher*.[94] Rather than elucidate the problem, these arguments and questions underscore the folly of attempting to force compelled decryption into the act of production doctrine.

A hard drive is not simply a locked box full of documents.[95] Encryption is neither a bank nor a safe. Importantly, either of these is ultimately subject to the superior force of the State, as the government can subpoena a bank or obtain a search warrant and break into a safe if necessary. Because the government can resort to force to get the information it needs, defendants rarely invoke the Self-Incrimination Clause in situations involving these items. Conversely, encryption creates a universe where the government *cannot* go, where arguably no amount of force will permit unauthorized entry. In this respect, encryption holds the promise of absolute privacy. Privacy advocates are quick to praise encryption,[96] and as a result have largely failed to consider the broader implications of a "victory" on compelled encryption.

The government knew Boucher possessed child pornography. Even if the original order had been upheld and Boucher was not convicted, several police officers had seen his computer files and might

---

which the police were formerly unaware. *See In re* Boucher (*Boucher II*), No. 2:06-mj91, 2009 WL 424718, at *4 n.2 (D. Vt. Feb 19, 2009); *see also* Aaron M. Clemens, *No Computer Exception to the Constitution: The Fifth Amendment Protects Against Compelled Production of an Encrypted Document or Private Key*, 2004 UCLA J.L. & TECH. 2, 16–17, http://www.lawtechjournal.com/articles/2004/02_040413_clemens.pdf (arguing the "foregone conclusion" rationale is insufficient precisely because the government will likely not have actual knowledge of every document that would be decrypted).

92. *E.g.*, M2SYS, Fingerprint PC Security Software, http://www.m2sys.com/DBS.htm (last visited May 15, 2009) (marketing encryption software featuring a fingerprint reader).

93. Phillip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171, 189–91.

94. *See* Clemens, *supra* note 91, at 19–20.

95. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 554–57 (2005) (discussing the merits of two alternative conceptions of a hard drive: either a virtual container full of documents or a physical storage device that is viewable by anyone with the right equipment).

96. *See* Paul Ohm, *Good Enough Privacy*, 2008 U. CHI. LEGAL F. 1, 13–14.

suspect that he would attempt to possess more child pornography in the future. If the courts prohibit access to evidence by compelled decryption, the government would most likely continue to investigate Boucher in the shadow of the new rule. As discussed in Part II, when the encryption cannot be broken, the only alternative is to steal the key. Without the ability to compel production of passwords, the government will be forced to resort to increasingly invasive measures to steal passwords in order to enforce the law. These measures will likely result in more harm to the cause of privacy than if courts permitted password compulsion.

C. The Future of Encryption Analyzed Under Document Production: Government "Hover" Orders[97]

United States v. Scarfo[98] demonstrates the lengths to which law enforcement agents are motivated to go in order to obtain encrypted electronic evidence. In 1999, federal agents entered Scarfo's business with a search warrant, seeking evidence relating to an ongoing illegal gambling and loan sharking operation.[99] The investigators discovered Scarfo's personal computer but could not access portions that were encrypted with PGP software.[100] Investigators believed that the encrypted files contained incriminating evidence and subsequently secured two additional search warrants.[101] The agents returned and surreptitiously installed keylogging software[102] on the computer in the hope of capturing the PGP password as Scarfo entered it on his keyboard.[103]

These secondary warrants permitted an invasion of privacy far beyond a typical search order. In addition to the initial entry, the warrants authorized agents to search, physically and electronically, the premises and computer as many times as necessary in a thirty-day period in order to obtain access.[104] Thus, the order essentially permitted government agents to "hover" in Scarfo's residence until they got the information they wanted.[105] The district court dismissed the de-

---

97. *See generally* Rachel S. Martin, Note, *Watch What You Type: As the FBI Records Your Keystokes, the Fourth Amendment Develops Carpal Tunnel Syndrome*, 40 AM. CRIM. L. REV. 1271 (2003) (discussing warrants designed primarily to uncover computer passwords).

98. 180 F. Supp. 2d 572 (D.N.J. 2001).

99. *Id.* at 574.

100. *Id.*

101. *Id.*

102. *See* Amitai Etzioni, *Implications of Select New Technologies for Individual Rights and Public Safety*, 15 HARV. J.L. & TECH. 257, 275–76 (2002) (describing KLS, the keylogger used on Scarfo's computer).

103. *Scarfo*, 180 F. Supp. 2d at 574.

104. Martin, *supra* note 97, at 1286–87. The order was eventually extended to cover an additional thirty days. *Id.*

105. *Id.*

fendant's challenge to the scope of the search: "That the [keylogger] certainly recorded keystrokes typed into Scarfo's keyboard *other* than the searched-for passphrase is of no consequence."[106]

While the investigators in *Scarfo* used only keyloggers, the court stated "[w]here proof of wrongdoing depends upon documents or computer passphrases whose precise nature cannot be known in advance, law enforcement officers must be afforded the leeway to wade through a potential morass of information in the target location to find the particular evidence."[107] This seems to suggest that even more invasive methods of data gathering, such as video surveillance, wiretaps, and audio bugging, might be within the necessary "leeway" allotted to investigators. Furthermore, any incriminating evidence investigators come across under such a warrant is in "plain view,"[108] whether or not it is related to the present investigation. For example, while investigating business crimes, the government might uncover evidence of narcotics possession, or other crimes about which agents had no prior knowledge. Given sixty days of virtually unlimited searching, little in the target's home would remain unknown to investigators. It seems unlikely that privacy advocates who have expressed a preference for disallowing compelled encryption would prefer this outcome.

While the free access provided by the "hover" order is disturbing, the access is only a means to an end: installing the government's keylogger. This is not the only tool the government has in its virtual lock pick set,[109] and an expansion of protections for encryption passwords will likely lead to an expansion of the use and development of these tools. The covert technologies employed by the government are as varied and innovative as the technologies they are designed to intercept. Whereas traditional wiretaps might intercept phone calls at the central office of a telephone company, a technology known as "triggerfish" allows agents to intercept cellular signals, enabling eavesdropping on calls made by targets within a given distance.[110]

---

106. *Scarfo*, 180 F. Supp. 2d at 578.

107. *Id.* The Ninth Circuit has reviewed and upheld the use of keyloggers and other forms of Internet surveillance by law enforcement stymied by PGP encryption. *See* United States v. Forrester, 512 F.3d 500 (9th Cir. 2008).

108. *See* Arizona v. Hicks, 480 U.S. 321, 325–27 (1987) (detailing the "plain view" doctrine and explaining that "the practical justification for [the doctrine] is the desirability of sparing police . . . the inconvenience and the risk — to themselves or to preservation of the evidence — of going to obtain a warrant").

109. *See generally* Etzioni, *supra* note 102, at 274–80 (describing many of the surveillance software available to law enforcement agencies); Mark G. Young, Note, *What Big Eyes and Ears You Have!: A New Regime for Covert Governmental Surveillance*, 70 FORDHAM L. REV. 1017 (2001) (detailing examples of government spyware in use today); Posting of Declan McCullagh to CNET News Blog, Feds Use Keylogger to Thwart PGP, Hushmail, http://news.cnet.com/8301-10784_3-9741357-7.html (July 10, 2007) (discussing "Magic Lantern").

110. Young, *supra* note 109, at 1028.

The FBI has developed "Carnivore," a network sniffing system capable of gathering, among other things, the routing information and content of an email.[111] Similarly, "trap and trace" devices and their counterparts, "pen registers," allow law enforcement to monitor the numbers dialing into, and the numbers dialed from, a land-line phone.[112] There have been reports that the FBI is developing an improved version of the keylogger used in *Scarfo*, code-named "Magic Lantern," that can be delivered to a target computer without physical intrusion, much like a virus.[113] Further government innovation in this field is hardly desirable, and over-protecting encryption passwords will only spur the development of even more invasive technology as law enforcement seeks to steal such passwords.[114]

Analyzing encryption under document production will lead to rulings, as in the *Boucher I* opinion, that create an incentive for the government to press the boundaries of its police power to conduct covert surveillance. Ironically, the incentive is caused by a shortsighted insistence on the inviolability of computer passwords. From broad "hover" orders and search warrants to increasingly advanced signal intercept devices, these developments are uniformly adverse to individual privacy rights and information security. A wiser approach would involve limiting Fifth Amendment safeguards and fashioning a procedure protected by judicial oversight by which the government could openly and reasonably gain access to encrypted information. Implementing Fifth Amendment protections in this way would not be unprecedented. Perhaps more so than any other amendment, the doctrine surrounding the Fifth Amendment has been reexamined and adjusted in an effort to maintain the delicate balance between the protection of individual rights and the needs of modern law enforcement.

IV. FINDING THE FIFTH AMENDMENT BALANCE

The proper scope and purpose of the Fifth Amendment's Self-Incrimination Clause is unclear and continually debated among scholars. Professor William Stuntz goes so far as to comment, "[i]t is probably fair to say that most people familiar with the doctrine surrounding the privilege against self-incrimination believe that it cannot

111. Martin, *supra* note 97, at 1283.

112. *See, e.g.*, U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 454 (D.C. Cir. 2000).

113. *See* Bob Sullivan, *FBI Software Cracks Encryption Wall*, MSNBC, Nov. 20, 2001, http://www.msnbc.msn.com/id/3341694/.

114. For example, Swiss researchers claim to have developed a device capable of detecting keystrokes by analyzing the electromagnetic emissions given off by a standard wired keyboard during normal operation. Martin Vuagnoux & Sylvain Pasini, Compromising Electromagnetic Emanations of Wired and Wireless Keyboards, http://lasecwww.epfl.ch/keyboard/ (last visited May 15, 2009).

be squared with any rational theory."[115] Professors Akhil Amar and Renée Lettow have called the Self-Incrimination Clause "a Gordian knot in the middle of our Bill of Rights,"[116] while others have dismissed the task of characterizing its true modern purpose as "a largely futile endeavor."[117] Still, ardent critics would not do away with the privilege entirely.[118] The Supreme Court itself has not been immune from this struggle for meaning. At one point, the Court said:

> [T]he constitutional foundation underlying the privilege is the respect a government — state or federal — must accord to the dignity and integrity of its citizens. To maintain a "fair state-individual balance," to require the government "to shoulder the entire load," . . . to respect the inviolability of the human personality, our accusatory system of criminal justice demands that the government seeking to punish an individual produce the evidence against him by its own independent labors . . . .[119]

Yet just one week later, the Court recognized that:

> [T]he privilege has never been given the full scope which the values it helps to protect suggest. History and a long line of authorities in lower courts have consistently limited its protection to situations in which the State seeks to submerge those values by obtaining the evidence against an accused through "the cruel, simple expedient of compelling it from his own mouth."[120]

These two statements highlight the internal conflict within Self-Incrimination Clause jurisprudence. On the one hand the jurisprudence expresses an idealistic concern for the dignity and rights of the accused.[121] On the other, it recognizes the needs of law enforcement

115. William J. Stuntz, *Self-Incrimination and Excuse*, 88 COLUM. L. REV. 1227, 1228 (1988).

116. *See* Akhil Reed Amar & Renée B. Lettow, *Fifth Amendment First Principles: The Self-Incrimination Clause*, 93 MICH. L. REV. 857, 857 (1995).

117. *See* Ronald J. Allen & M. Kristin Mace, *The Self-Incrimination Clause Explained and Its Future Predicted*, 94 J. CRIM. L. & CRIMINOLOGY 243, 243 (2004).

118. *See, e.g.*, David Dolinko, *Is There a Rationale for the Privilege Against Self-Incrimination?*, 33 UCLA L. REV. 1063, 1064 (1986) (stating that even without "principled justification," the privilege may still "come to serve important functions in the legal system as a whole, so that its repeal would do violence to the entire system").

119. Miranda v. Arizona, 384 U.S. 436, 460 (1966) (internal citations omitted).

120. Schmerber v. California, 384 U.S. 757, 762–63 (1966) (citation omitted).

121. *See, e.g.*, Murphy v. Waterfront Comm'n, 378 U.S. 52, 55 (1964) (Goldberg, J.) ("The privilege against self-incrimination . . . registers an important advance in the devel-

and that the privilege often protects the guilty.[122] The facts of *Boucher*, and the existence of computer encryption more broadly, present a situation in which the courts must yet again both address this conflict and fashion a resolution that maintains a careful balance between the two competing interests. The policies that animate the Fifth Amendment and the judiciary's efforts to implement them shed light on the proper way to strike a compromise between an individual's need for privacy and law enforcement's need to access encrypted information.

A. Balancing the Purposes and Practical Realities of the Fifth Amendment Privilege

The Fifth Amendment is sometimes justified as a safeguard of human dignity, a shield against the State's effort to use the accused "as the means of his own destruction."[123] The privilege prevents the accused from having to aid his "enemy" and stands in recognition of the fact that an individual has no "moral duty to bring conviction and imprisonment upon himself."[124] Justice Brennan extolled the privilege: "At its core, the privilege reflects our fierce unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt."[125] The Fifth Amendment forces the government to respect individual autonomy and protects the accused from being coerced into confession.[126] The privilege's protection reflects society's "respect for the inviolability of the human personality

---

opment of our liberty — one of the great landmarks in man's struggle to make himself civilized." (internal citations and quotations omitted)); Stephen J. Schulhofer, *Some Kind Words for the Privilege Against Self-Incrimination*, 26 VAL. U. L. REV. 311, 330–32 (1991) (noting that the privilege is often beneficial to the innocent and criticizing other scholars who predict that the privilege could be abolished without harm to innocent defendants).

122. *See, e.g.*, Palko v. Connecticut, 302 U.S. 319, 326 (1937) ("Justice, however, would not perish if the accused were subject to a duty to respond to orderly inquiry."); Stephanos Bibas, *The Right to Remain Silent Helps Only the Guilty*, 88 IOWA L. REV. 421, 424, 427, 430 (2003) (noting that guilty suspects who confess enjoy psychological benefits as well as reduced sentences, while guilty suspects who lie to investigators will, if successful, go free, or will, if unsuccessful, increase law enforcement's general skepticism of all suspects' statements); Peter W. Tague, *The Fifth Amendment: If an Aid to the Guilty Defendant, an Impediment to the Innocent One*, 78 GEO. L.J. 1, 1–3 (1989) (arguing that the privilege frustrates attempts by innocent defendants to prove their innocence by allowing the actual guilty party to refuse to testify as a witness when called during the trial).

123. Amar & Lettow, *supra* note 116, at 892; *see also* Bram v. United States, 168 U.S. 532, 544 (1897) (noting the privilege embodies "principles of humanity and civil liberty").

124. R. Kent Greenawalt, *Silence as a Moral and Constitutional Right*, 23 WM. & MARY L. REV. 15, 36–37 (1981).

125. Pennsylvania v. Muniz, 496 U.S. 582, 596 (1990) (internal citations omitted) (internal quotations omitted).

126. *See* Robert S. Gerstein, *The Demise of* Boyd*: Self-Incrimination and Private Papers in the Burger Court*, 27 UCLA L. REV. 343, 347 (1979) ("[A]n individual ought to be autonomous in his efforts to come to terms in his own conscience with accusations of wrongdoing against him.").

and of the right of each individual to a private enclave where he may lead a private life."[127] Nevertheless, the Supreme Court has drastically limited the privilege — often in ways that directly contravene these values — in order to accommodate the legitimate needs of law enforcement.

In 1966, the Court held in *Schmerber v. California* that law enforcement could forcibly extract blood from an individual's body.[128] The Court drew a sharp distinction between compelled "testimony" and using the defendant as a source of real evidence, finding the latter constitutional.[129] Thus, the privilege applies only when an individual is acting as a witness.[130] "The word 'witness' in the constitutional text limits the relevant category of compelled incriminating communications to those that are 'testimonial' in character."[131] The Court has held that "in order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information."[132] In so doing, the Court has tailored the Fifth Amendment to allow law enforcement access to physical evidence that often proves vital to criminal investigations. Encryption keys challenge courts in their application of the testimony/real evidence distinction; often a very minimal amount of testimony — sometimes a single password — shields thousands of documents that would otherwise be subject to government seizure with a simple search warrant.

In addition, effective law enforcement requires investigators to obtain information in a timely manner, and Fifth Amendment doctrine has been limited in light of this pragmatic constraint. Courts have granted law enforcement significant leeway in conducting an investigation. The government is free to surreptitiously record conversations,[133] place informants into an individual's confidence,[134] deceive suspects in custody,[135] or attempt to induce statements with unenforceable promises of leniency.[136] Furthermore, the privilege is not absolute, and the government can compel a witness to admit wrongdo-

---

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

128. 384 U.S. 757, 765 (1966).

129. *Id.* at 764.

130. Fisher v. United States, 425 U.S. 391, 408 (1976).

131. United States v. Hubbell, 530 U.S. 27, 34 (2000).

132. Doe v. United States (*Doe II*), 487 U.S. 201, 210 (1988).

133. *See Fisher*, 425 U.S. at 400 (noting that absent compulsion, overheard statements are admissible given "appropriate safeguards"); *see also* Stanley v. Wainwright, 604 F.2d 379, 382 (5th Cir. 1979) (holding that law enforcement's secret recording of defendant's statements did not violate the privilege because police officers were physically absent).

134. Hoffa v. United States, 385 U.S. 293, 304 (1966).

135. *See, e.g.*, United States v. Lux, 905 F.2d 1379, 1382 (10th Cir. 1990) (stating that the fact that detective lied to suspect regarding co-defendant's statements to police did not render subsequent statements involuntary).

136. *See, e.g.*, United States v. Jaswal, 47 F.3d 539, 542 (2d Cir. 1995) ("[P]romises of leniency do not per se render a confession involuntary . . . .").

ing pursuant to an appropriate grant of immunity from prosecution.[137] The very existence of the immunity doctrine demonstrates that the privilege is not meant to keep information from the government. It also shows that the doctrine is not designed to spare an individual from the effects of publicly admitting to wrongdoing.[138] In fact, the Supreme Court has said, "[a] witness has . . . a constitutional right to stand on the privilege against self-incrimination *until* it has been fairly demonstrated to him that an immunity, as broad in scope as the privilege it replaces, is available and applicable to him."[139]

Originally, the Supreme Court insisted on so-called "transactional immunity" that shielded the witness from any prosecution relating to the crimes about which he was questioned.[140] However, this doctrine has been limited over time. In *Kastigar v. United States*, the Court held that a sufficient grant of immunity need only be "coextensive with the scope of the privilege," such that it is "as comprehensive as the protection afforded by the privilege."[141] The federal immunity statute[142] upheld in *Kastigar* affords immunity only from "use and derivative use."[143] this prevents prosecutors from using the testimony or any physical evidence discovered as a direct or indirect result of the testimony. However, if investigators can show they would have come across evidence of the crime as an inevitable discovery, derivative-use immunity, unlike transactional immunity, is of no avail.

In light of these and similar decisions, it is reasonable to say that interpretation of the Self-Incrimination Clause has been motivated by what was perceived, at the time, to be desirable public policy.[144] This explanation is instructive: instead of allowing the issue of decryption to devolve into a potentially endless debate over hypothetical keys and combination safes, a wiser approach involves looking forward toward a system that would be most beneficial to society.

---

137. *See* Kastigar v. United States, 406 U.S. 441, 448 (1972) (flatly rejecting petitioner's contention that the privilege "deprives Congress of power to enact laws that compel self-incrimination, even if complete immunity from prosecution is granted prior to the compulsion of the incriminatory testimony").

138. *See* Brown v. Walker, 161 U.S. 591, 605–06 (1896) ("The design of the constitutional privilege is not to aid the witness in vindicating his character . . . .").

139. Stevens v. Marks, 383 U.S. 234, 246 (1966) (emphasis added); *see also* Murphy v. Waterfront Comm'n, 378 U.S. 52, 79 (1964) (holding that immunity must foreclose prosecution by both state and federal governments).

140. *See Brown*, 161 U.S. at 594 (citing Counselman v. Hitchcock, 142 U.S. 547 (1892)).

141. 406 U.S. at 449.

142. 18 U.S.C. § 6002 (2006).

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

144. *See* Stephen A. Saltzburg, *The Required Records Doctrine: Its Lessons for the Privilege Against Self-Incrimination*, 53 U. CHI. L. REV. 6, 7–11 (1986) (discussing the trend toward narrow construction of the Self-Incrimination Clause by courts, due in part to the "impression that [the privilege] is no longer a great protection of civilized people, but a safe harbor for those who break society's rules").

B. A Responsible Decryption Policy

An ideal decryption policy should have several features to ensure both its usefulness to law enforcement and its viability as a safeguard for individual privacy interests. The procedure should be straightforward in its pleading requirements, such that law enforcement could seek decryption orders without the help of the prosecutor's office. It should require few additional resources to administer and avoid creating more bureaucracy or new agencies for oversight. Given the time-sensitive nature of many investigations, law enforcement should be able to obtain decryption orders with reasonable speed. However, expediency should not come at the cost of transparency: the procedure must provide notice and an opportunity for the target of the order to challenge the government's actions and seek redress. Finally, to ensure an impartial referee between suspects and law enforcement, the judiciary should oversee the procedure. All of these goals could be achieved within the current criminal procedure framework by implementing a reasonable warrant requirement, subpoena hearing provision, and sufficient civil remedy for government abuse.

Imagine a situation very similar to the facts of *Scarfo*:[145] after a period of investigation, agents come to suspect one Smith of money laundering and tax crimes. Under the proposed new procedure, the agents would seek a warrant as if they were preparing to seize any other type of evidence. The warrant must spell out with particularity the documents or information sought. For example, it would specify the type of business documents or the specific year of the tax returns to be seized. Moreover, the agents must show probable cause to a neutral magistrate. Once they obtain the warrant, the agents seize Smith's computer and serve him with a subpoena for the encryption password. Now confronted with a subpoena, Smith can move to quash and thereby gain a hearing before the judge to challenge the government's actions. If he loses his motion, Smith then has the choice of handing over his password or being held in contempt of court.

However, the mere communication of his password would not authorize a fishing expedition through all of his documents. Rather, the procedure would restrict the government's ability to prosecute Smith to evidence specified by the particularized statements in the warrant. If the agents discover evidence of a crime about which they had no knowledge, Smith is immunized from prosecution because the agents have no right to use evidence not specified in the warrant. This implied grant of immunity would guard against accidental discoveries made by police acting in good faith.

145. United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001).

One concern with this approach is that law enforcement may be tempted to improperly secure decryption orders. Consequently, there must be a mechanism to ensure that the government does not use the decryption procedure irresponsibly. A statutory civil remedy similar to § 1983[146] would effectively police improper decryption orders. If the law enforcement agents decrypted Smith's computer in bad faith, the statutory remedy would allow Smith to sue the government for damages arising from the improper seizure and decryption.[147] Damage awards may be significant when property is destroyed or when irreplaceable data has been lost. When the damage sustained is minimal or arises solely from the revelation of an individual's private data, the civil remedy should provide for reasonable statutory damages. To be useful as a tool to deter law enforcement, however, the remedy must go beyond § 1983 and provide for awards of costs and attorney's fees. This will ensure that individuals have the means to bring an action to seek redress. Furthermore, the court must require law enforcement to destroy any copies of the defendant's information they might still possess.

This decryption procedure provides several advantages over the approach presented in both *Boucher I* and *Scarfo* for law enforcement and privacy advocates alike. Law enforcement would benefit by gaining access to encrypted evidence without having to spend months listening to wiretaps or sifting through mountains of keystroke data. However, because law enforcement must pursue decryption orders with judicial oversight, individuals would be given notice and, through the subpoena hearing, a venue to challenge the government's case before submitting to decryption. The prospect of a hearing would limit the likelihood that law enforcement would seek speculative or abusive decryption orders and would encourage the government to seek decryption only when there is credible evidence to suggest such action is warranted. Finally, even if the hearing is insufficient to fully discourage speculative decryption proceedings, the implied grant of immunity would limit the ability of law enforcement to go "fishing," and the civil remedy would punish law enforcement for overstepping its authority.

V. CONCLUSION

Cases such as *Boucher* and *Scarfo* show that in its shortsighted effort to protect against every attempt by government to enter an indi-

146. 42 U.S.C. § 1983 (2006) (providing a right of action for individuals who have suffered Constitutional injury at the hands of state authorities).

147. *See* Kimel v. Fla. Bd. of Regents, 528 U.S. 62, 80–81 (2000) (stating the Fourteenth Amendment grants Congress the power "both to remedy and to deter violation of rights guaranteed" by the amendment).

vidual's private sphere, the law may ultimately do more harm than good to the cause of privacy. The decryption procedure suggested in this Note attempts to strike a balance between an individual's right to privacy and the legitimate needs of law enforcement to access that individual's data.