No Computer Exception to the Constitution:[1] The Fifth Amendment Protects Against Compelled Production of an Encrypted Document or Private Key

By Aaron M. Clemens[2]

Computer Crime Seminar
Georgetown University Law Center
Professors Richard Salgado[3] & Christian Genetski[4]

[1] *Cf.*, Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 641 (1989) (Marshall, J., dissenting) ("There is no drug exception to the Constitution, any more than there is a commu nism exception or an exception for other real or imagined sources of domestic unrest."); Hartness v. Bush, 919 F.2d 170, 174 (D.C. Cir. 1970) (Edwards, J., dissenting) ("Faced regularly with the grim results of the illegal drug trade, the judiciary may well be tempted to offer aid to the Government in its War on Drugs. But no matter how pressing the perceived need, the judiciary is simply without authority to trim back the Fourth Amendment. There is, and can be, no 'drug exception' to the Fourth Amendment.").

[2] B.A. 2001, University of Nevada, Las Vegas; J.D. candidate, Spring 2004, Georgetown University Law Center. Special thanks to the staff of the UCLA Journal of Law and Technology as well as GULC Adjunct Professors Richard Salgado and Christian Genetski for their encouragement and supervision of this article. The views expressed herein are my own, as are any errors or omissions.

[3] Richard Salgado, Adjunct Professor of Law, Georgetown University Law Center; Senior Counsel, Computer Crime & Intellectual Property Section, U.S. Department of Justice.

[4] Christian Genetski, Adjunct Professor of Law, Georgetown University Law Center; Partner, Sonnenschein, Nath & Rosenthal L.L.P.

The U.S. Constitution's Fifth Amendment privilege against self-incrimination prevents the government from compelling a person to decrypt or reveal the private key to decrypt her electronic documents absent two circumstances.[5] The government must either prove, by clear and convincing evidence, that the three-prong test in *Fisher v. United States*[6] has been met, or provide use and derivative-use immunity for such production.

I. The Need For Computer Security

Unauthorized access to computer files has been a problem since the computer's advent.[7] Unauthorized access allows identity theft, fraud, and the revelation of intimate secrets.[8] These

[5] Joe Baladi, Comment, *Building Castles Made of Glass-Security on the Internet*, 21 U. Ark. Little Rock L. Rev. 251, 275-76 (1999) ("The Fifth Amendment protections are implicated in that, absent mandated key recovery, the government would have to compel disclosure of the encryption key. If the encrypted communication is incriminating, then the disclosure of the key triggers the protection of the Fifth because the government is compelling access to the incriminating testimonial communication.") (*Citing* Privacy in the Digital Age: Encryption and Mandatory Access, 1998: Hearings before the Subcommittee on the Constitution of the Senate Committee on the Judiciary, 105th Congress (1998) (statement of Kathleen M. Sullivan, Professor, Stanford Law School)); *See* Greg S. Sergienko, *Self Incrimination and Cryptographic Keys*, 2 Rich. J.L. & Tech. 1, 72 (1996):

> Cryptography may provide a technical fix for Supreme Court decisions allowing the invasion of one's private papers. However, the effectiveness of that fix will depend on whether the Court holds that use immunity from the compulsory production of a cryptographic key extends to the incriminating documents decrypted with the key. Logic suggests that the Court should so hold.

See also Richard A. Nagareda, *Compulsion "To be a Witness" and the Resurrection of Boyd*, 74 N.Y.U. L. Rev. 1575, 1580 (1999):

> The application of the Fifth Amendment turns upon the meaning of the phrase "to be a witness." It is the compulsion of a person to assume "witness" status that violates the Fifth Amendment. The phrase "to be a witness" in the Fifth Amendment is best understood as synonymous with the phrase "to give evidence" used in the proposals for a bill of rights formulated by state ratifying conventions upon consideration of the original Constitution. The compulsion of a person to produce self-incriminatory documents is literally the compulsion of that person "to give evidence" against himself--that is, to turn over documents for possible use as incriminatory evidence in a subsequent criminal trial.

[6] 425 U.S. 391 (1976).

[7] Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U.L. Rev. 1596, 1597 (2003) ("In the last quarter century, the federal government, all fifty states, and over forty foreign countries have enacted computer crime laws that prohibit 'unauthorized access' to computers."(citations omitted)); *see also, e.g.,* United States v. Kelly, 507 F. Supp. 495 (E.D. Pa. 1981) (Finding private company employees' use of a company's computer for personal benefit defrauded their employer of their honest and faithful performance of their duties as employees and violated the mail fraud statute). *See generally,* Alois Valerian Gross, *Criminal Liability for Theft of, Interference with, or Unauthorized Use of, Computer Programs, Files, or Systems*, 51 A.L.R.4th 971 (2003).

[8] *See, e.g.,* Andres Rueda, *The Implications of Strong Encryption Technology on Money Laundering*, 12 Alb. L.J. Sci. & Tech. 1, 32-33 (2001) ("[F]or technologically savvy criminals, online credit card fraud can be remarkably effective. … For example, the numbers of over 100,000 credit cards issued by 1,214 different banks were stolen by a single cyberthief using 'packet sniffers,' or 'virus-like programs that surreptitiously hunt through networks' in search of specific types of information, such as credit card numbers.").

potential problems are exacerbated for lawyers, who have an ethical duty to protect their clients' privileged information.[9] Without updated security to match snooping possibilities, the use of computers for client matters may soon, in effect, waive the attorney-client privilege.[10] Despite this emerging insecurity, the computer, like the telephone, has evolved into a personal and professional necessity for many people.[11] Ubiquitous portable high-speed wireless Internet is now a reality for many in America. Increasingly, actual face-to-face conversations are replaced by virtual face-to-face conversations, even between parents and children within voice range of each other.[12] As computers are increasingly used for communication, privacy concerns are heightened.[13] Just as telephone use does not forfeit a person's expectation of privacy,[14] computer

[9] Lawyers have a duty to maintain client confidentiality and many lawyers have integrated the convenience of e-mail and cell phone communication into their business routine. Without improvements in security, using computers to send e-mail or voice mail for confidential attorney-client communications may constitute waiver of privilege because these messages are so easily intercepted. *See* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. Pa. L. Rev. 709, 724 (1995):

> [T]he ease with which intruders can gain access to unprotected computers that can be accessed via the Internet means that unencrypted data on such machines is at risk … [t]he ease with which these [messages] can be overheard or intercepted, combined with the growing simplicity of encryption software, make it conceivable that failure to use encryption may be considered a waiver of privilege at some point in the future (at least for insecure media such as electronic mail and cellular telephones).

See also Sherry L. Talton, Note, *Mapping the Information Superhighway: Electronic Mail and the Inadvertent Disclosure of Confidential Information*, 20 Rev. Litig. 271, 279 (2000) ("Electronic mail is an insecure medium."); Robert A. Pikowsky, Article, *Privilege and Confidentiality of Attorney-Client Communication Via E-mail,* 51 Baylor L. Rev. 483, 578 (1999) ("There seems to be little or no debate as to the degree of privacy that one can reasonably expect in unencrypted e-mail."); R. Scott Simon, Note, *Searching for Confidentiality in Cyberspace: Responsible Use of E-mail for Attorney-Client Communications*, 20 U. Haw. L. Rev. 527, 545 (1998) ("[E]ncryption seems to be a viable answer to the concern about insecurity on the Internet.").

[10] Froomkin, *id*. (Footnotes Omitted) ("Every lawyer knows that she should never discuss client confidences in a crowded restaurant … Unfortunately, the ease with which electronic mail messages can be intercepted by third parties means that communicating by public electronic mail systems, like the Internet, is becoming almost as insecure as talking in a crowded restaurant.").

[11] *See, c.f.*, Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting) (Finding that telephone usage has "for many has become a personal or professional necessity" and thus there is no choice for people to accept the risk of surveillance or give up this medium of communications to preserve their privacy because "as a practical matter, individuals have no realistic alternative.")

[12] John Schwartz, *That Parent-Child Conversation Is Becoming Instant, and Online*, N.Y. Times, Jan. 3, 2004, A1 ("Almost three-quarters of all teenagers with online access use instant messaging and about half of all adults have tried the services, surveys show. . . [Instant messaging is] an old idea that's been made practical . . . Instead of yelling downstairs, `Hey, is there any fried chicken left?' You can I.M. downstairs.").

[13] David Kahn, *The Codebreakers: The Story of Secret Writing*, at 983 (1996) ("The need to protect the ever-growing number of files as communications expands at its present lighting rate in e-mail, the World Wide Web and other functions of the Internet, internal business networks, and cellular telephones explains why more than a

use must not forfeit a person's expectation of privacy. Therefore, for computers to reach their full potential, unauthorized access to computers must be reduced.[15]

Efforts are underway to alleviate computer security concerns. Secret passwords have long protected access to computer resources and computer files.[16] But, due to advances in cyber-snooping, basic alpha-numeric passwords alone can no longer assure security.[17] Cryptography is one answer to the security problem. Cryptography is the ancient art of preventing unauthorized access to messages by improving the use of basis passwords.[18] Modern cryptology,[19] such as the public and private key system, can ensure computer security.[20]

Public/private key cryptography allows the exchange of secure messages. The process begins when a sender encrypts a message using the public key of the intended recipient. Both the

thousand firms now offer cryptological systems for data, voice, and fax, why manufacturers are now building them into the software packages they sell.")

[14] *See, e.g.,* Katz v. United States, 389 U.S. 347 (1967).

[15] Kahn, *id*. (Footnotes Omitted); *see also* Rueda, *supra* note 8, at 4 ("[S]trong encryption and related technologies are a crucial aspect of the future development of electronic commerce."); Joel C. Mandelman, Article, *Lest We Walk Into the Well: Guarding the Keys-- Encrypting the Constitution: To Speak, Search & Seize in Cyberspace*, 8 Alb. L.J. Sci. & Tech. 227, 236-37 (1998) ("[I]t is essential for certain transactions to be encoded to prevent their interception or fraudulent alteration. This issue is of critical importance to the computer and banking industries, as well as the overall American economy.").

[16] C. Ryan Reetz, Note, *Warrant Requirement for Searches of Computerized Information*, 67 B.U.L. Rev. 179, 206 (1987) ("In most cases, the risk of unauthorized access to computer files by third parties is minimized by access control systems requiring passwords or restricting use to certain users.").

[17] Kevin R. Pinkney, *Putting Blame Where Blame is Due: Software Manufacturer and Customer Liability for Security-Related Software Failure*, 13 Alb. L.J. Sci. & Tech. 43, 52 (2002) ("[A] determined intruder might attempt to crack the password by trying every word in the dictionary. Such 'brute-force' attacks regularly succeed.") (*Citing* Michael Lee et al., Comment, *Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal*, 14 Berkeley Tech. L.J. 839, 851 (1999)).

[18] Kahn, *supra* note 13, at 80, 82, 93 (Explaining that Daniel, of the Christian Bible and the Jewish Torah, was "the first known cryptanalyst," a renown he gained by interpreting the writing on a wall for the Babylonian Emperor Belshazzar; that as early as the fifth century B.C. the Spartans "established the first system of military cryptography;" and that "Cryptology was born among the Arabs" and that the word "cipher" comes from the Arabs.); Rueda, *supra* note 8, at 15 ("Cryptography 'is an ancient science, and was used by Roman emperors to send secret messages.'").

[19] Kahn, *id*. at xv (Cryptological methods "do not conceal the presence of a secret message but render it unintelligible to outsiders."); *see also* Rueda, *id*. at 17 ("Cryptography is a technology that disguises messages using codes, ciphers, and algorithms, so that only the intended recipient can access its meaning.").

[20] Kahn, *id*. at 983 ("Cryptology plays a role in [improving computer security] because it is the only technology that, if good enough, can block access to files in storage or in transit. Passwords can be encrypted so that they cannot be read even if the file in which they are stored is accessed. Files can be encrypted so that their contents can remain secret.").

public and private keys consist of an arrangement of letters, numbers, and symbols. A public key[21] can be made public without fear of undermining the security of a message encrypted with it.[22] Only a viewer of the message with the right private key can decrypt the message.[23] Without this private key, the encrypted information is incomprehensible. To illustrate, I may encrypt this article using my brother's public key,[24] and send it to him.[25] In turn, he could use my public key to encrypt his replying comments. If our private keys remain private, we are assured of security.[26] Modern technology briefly took away privacy,[27] but subsequently recreated it.[28]

[21] *See* Rueda, *id*. at 20-21 (Footnotes Omitted):

> Asymmetric encryption, otherwise known as public-key cryptography, exploits the mathematical characteristics of so-called one-way trapdoor functions. A one-way function is a mathematical operation easy to conduct in one direction, but almost impossible to conduct in the reverse. A trapdoor one-way function means that there is a trick (i.e., a secret algorithm) that allows the otherwise one-way function to be conducted in the reverse. An example of a one-way function involves multiplying two large prime numbers. Although this operation is relatively simple, conducting the operation in the reverse (i.e., factoring to derive the two large prime numbers given their product) is exceedingly difficult.

[22] *Cited* in Rueda, *id*. at 24 ("Unless frequency analysis or other cryptoanalytical methods detect a flaw in the encryption algorithm, it would take a computer processing a million keys per second about 1 x 10[to the 25th power] years to finish the task, or 1 x 10[to the 15th power] 'times greater than the estimated age of the universe.'").

[23] Rueda, *id*. at 17 (With modern cryptology: "Mathematical algorithms are used to scramble information for future recovery. Specifically, the unscrambled 'plaintext' is converted into a 'ciphertext,' or a series of apparently random characters. With the use of a 'key' known only to the intended recipient of the message, the 'ciphertext' is converted back into 'plaintext.'").

[24] Using a retail program from http://www.pgp.com and his public key located at http://www.jclemens.org/pgp.txt [January 18, 2004].

[25] This may be a wise move because he is a Senior Information Security Analyst for Intel Corporation.

[26] *See* Kahn, *supra* note 13, at 984 ("The only way properly encrypted messages can be read nowadays is by theft or betrayal – that is, noncryptological means. It had already begun with the German naval Enigma."). One way for the government to secure a private key would be through informants. A person cannot rely on another person to keep a private key secret. Hoffa v. United States, 385 U.S. 293, 302 (1966) (Stewart, J., for a plurality) ("[T]he Fourth Amendment [does not protect] a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."); *see, e.g.*, Illinois v. Perkins, 496 U.S. 292, 298 (1990) (Kennedy, J., announcing the opinion of the Court) (Holding that *Miranda* does not require suppression of an inmate confession given an agent posing as a fellow prisoner); White v. United States, 401 U.S. 745, 752 (1971) (White, J., for a plurality) ("Inescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police."). The government may also use a search warrant to gain access to a private key via surreptitious surveillance. *See, e.g.,* United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001), described by Rachel S. Martin, Note, *Watch What You Type: As the FBI Records Your Keystrokes, the Fourth Amendment Develops Carpal Tunnel Syndrome*, 40 Am. Crim. L. Rev. 1271, 1287 (2003) ("The warrant issued in *Scarfo* authorized the FBI (1) to lie in wait for Scarfo to leave his password in law enforcement's plain view and (2) to surreptitiously enter Scarfo's residence as many times as necessary to maintain the device. Thus, during this sixty-day period, the FBI essentially maintained a technological 'hover' over Scarfo.").

[27] *See infra* Part III.

[28] Rueda, *supra* note 8, at 25 ("With the emergence of the Internet, the value of encryption technology for civilian applications has greatly expanded. As the Internet economy matures, encryption applications will become

II. Privacy for All Would AllowPrivacy for those Suspected of Crime

Encryption provides secure transmission of confidential legal documents, business transactions, and any other information. But criminals can and do use it,[29] including terrorists,[30] members of drug cartels,[31] organized criminals,[32] and child pornographers.[33] Strong encryption through cryptography will likely remain both readily available and lawful.[34] To combat crimes involving encrypted messages, prosecutors may seek compelled message decryption. For example, the government can subpoena a person to testify before a grand jury and bring the private key and/or a decrypted version of a seized message. The government can thereby compel decryption or the production of the private keys that will decrypt an encrypted message,[35] unless

increasingly routine. Windows 2000, for example, uses 128-bit encryption."). *See also infra*, text accompanying note 46.

[29] Froomkin, *supra* note 9, at 728 ("Undoubtedly, criminals and conspirators will find a use for encryption").

[30] Mandelman, *supra* note 15, at 232-33 ("Terrorists hiding their plans in encrypted format are no longer merely a prospective fear; it is already happening. When the FBI broke the World Trade Center bombing case, the FBI discovered laptop computers containing encrypted materials.").

[31] *Id.* at 233 ("[T]he Cali Colombian drug cartel is now believed to be using encryption technology to conceal its voice and telephone communications.").

[32] *Id*. ("The Italian State Police's crime and technology center believes that the Mafia is also using encryption technology to conceal its massive organized crime activities in Italy.").

[33] *Id.* at 234 ("The Federal Bureau of Investigation's Computer Response Analysis Team has estimated that between five and six per cent of the 1,500 cases that it handles annually involve the use of encryption. These cases involve primarily child pornography and computer crimes, amounting to between seventy-five and ninety cases a year.").

[34] Froomkin, *supra* note 9, at 748 ("The United States has several long-standing laws and policies designed to prevent strong cryptography from spreading abroad, and even from being widely used at home. Although these may have served to slow the spread of strong cryptography, ultimately they have failed to stop it."). *But see*, *id.* at 810 ("Imagine a terrorist attack on a major public building in which the conspirators protected their telephone conversations with unbreakable encryption. [Then] Congress might well pass a law requiring that anyone using a strong cryptosystem to communicate by any electronic means acquire a license from the government."); D. Forest Wolfe, Comment, *The Government's Right to Read: Maintaining State Access to Digital Data in the Age of Impenetrable Encryption*, 49 Emory L.J. 711, 713 (2000) ("[T]he use of impenetrable encryption, and the absolute privacy it ensures, is not guaranteed by the Constitution, but is instead a political issue best decided by Congress, not the judiciary.").

[35] Phillip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. Chi. Legal F. 171, 176 (1996) ("That I physically lock that document in a safe is not material; so long as the document is in my custody, I must produce it in response to a legally authorized demand. The result should not differ if, instead of locking the document in a safe, I lock the contents through encryption ... even if I store the document on a computer that requires a password for access, I must produce the document when faced with an authorized demand. Similarly, if I encrypt the document, I should be required to produce the unencrypted version if I receive an authorized demand for the same."); *id*. at 195-96 ("The government should be able to require the production of keys under the same

the person exercises a valid privilege.[36] If a person, without a valid privilege, refuses to comply with a lawful subpoena, punishment can include criminal contempt[37] or an indeterminate fine and jail sentence.[38] Lying to the court in response to a subpoena would expose a person to criminal perjury charges[39] along with a possible contempt charge.[40] Therefore, the history of the Fifth Amendment privilege against self-incrimination must be examined to determine whether a person, without immunity, can resist compelled decryption where such testimony could potentially be used to incriminate her at trial.

III. Applying the Fifth Amendment to Compelled Document Decryption

The Fifth Amendment provides that "no person . . . shall be compelled in any criminal case to be a witness against himself."[41] This privilege against self-incrimination has historically functioned to protect a "'natural individual from compulsory incrimination through his own

conditions as if it were seeking to compel the production of plaintext, because production of keys is, for the most part, equivalent to the act of producing the decrypted document.").

[36] Id. at 178 ("[I]f law enforcement subpoenas information that I have encrypted, I must produce the information in plaintext if it remains available to me in that form, assuming I have no other proper objection, such as my privilege against self-incrimination.").

[37] Diana Lowndes, Note, *Thirty-First Annual Review of Criminal Procedure: III. Trial: Authority of the Trial Judge*, 90 Geo. L.J. 1659, 1675-76 (2002) ("Criminal contempt sanctions are imposed to vindicate the authority of the court and may be imposed even after the action in which the contempt arose is terminated."); Paula F. Wolff, *Federal District Court's Power to Impose Sanctions on Non-Parties for Abusing Discovery Process*, 149 A.L.R. Fed. 589, §2a:

> The federal district court may find the power to compel a non-party to produce documents and things under Federal Rule of Civil Procedure 34(c). Under Rule 45(e), which provides that any person's failure to obey a subpoena without an adequate excuse may be deemed a contempt of the court from which the subpoena issued, the federal district court can find any person, including a non-party, in contempt of court for failure to comply with a subpoena, without objecting to the subpoena.

[38] Michael J. Yaworsky, *Contempt: State Court's Power to Order Indefinite Coercive Fine or Imprisonment to Exact Promise of Future Compliance with Court's Order--Anticipatory Contempt*, 81 A.L.R.4th 1008, §2a (2003) ("[C]ontempt consisting of present, ongoing behavior may be dealt with by an indeterminate fine or term of imprisonment which continues in effect until the violative behavior ceases; this is a coercive sanction.").

[39] 18 U.S.C. 1621 (Perjury generally); 18 U.S.C. 1623 (False declarations before grand jury or court).

[40] J. A. Bock, *Perjury or False Swearing as Contempt*, 89 A.L.R.2d 1258, §12 (2003) ("The commission of perjury or false swearing while testifying before a grand jury has frequently been held or recognized as constituting a contempt of court."). *But see Re Persico*, 491 F.2d 1156 (2d Cir. 1974) (Where purpose of holding person in contempt was to coerce him to answer grand jury's question and was not to punish him for reprehensible conduct, he was only recalcitrant witness and his contempt was manifestly civil in character, to which summary procedure set forth in 28 U.S.C.S. § 1826 was applicable, rather than procedure for criminal contempt set out in Rule 42 of Federal Rules of Criminal Procedure.).

[41] U.S. Const., amend. V.

testimony or personal records.'"[42] The Fifth Amendment, in conjunction with the exclusionary rule,[43] prevents the government from gathering evidence in violation of the Fifth Amendment or using that evidence at trial.[44]

The type of privacy provided by strong encryption has precedent in America. During the time our Constitution developed, government officials regularly lacked direct access to secret communications.[45] At the adoption of the Bill of Rights, "private communications were far more secure than they are today [because] one could have a secure conversation by going for a quiet walk in an open field."[46] At the end of the 18th century, government agents had no long distance microphones, body wires, or hidden tape recorders. Also, people would "encrypt letters in ciphers that no government could break."[47] One encryption system created by Thomas Jefferson[48] near the end of the 18th century remained unbreakable for more than a century.[49] In fact, "[m]odern encryption seems poised to re-create the functional equivalent of the privacy available in the late 1790s and to apply it to devices like telephones and modems, which are increasingly replacing face-to-face contact and letter writing."[50]

[42] Andresen v. Maryland, 427 U.S. 463, 470-71 (1976) (Blackmun, J., announcing the opinion of the Court) (holding that business records are outside the Fifth Amendment privilege) (quoting United States v. White, 322 U.S. 694, 701 (1944)).

[43] Wong Sun v. United States, 371 U.S. 471, 484 (1963) (Brennan, J., announcing the opinion of the Court) (The exclusionary rule "extends as well to the indirect as the direct products" of unconstitutional conduct.).

[44] United States v. Verdugo-Urquidez, 494 U.S. 259, 264 (1990) (Rehnquist, C.J., announcing the opinion of the Court) ("Although conduct by law enforcement officials prior to tria l may ultimately impair that right, a constitutional violation occurs only at trial.") (citations omitted).

[45] Even back then the government likely used informants, a practice dating back "as far as the first records of governing institutions." ROBERT M. BLOOM, RATTING: THE USE AND ABUSE OF INFORMANTS IN THE AMERICAN JUSTICE SYSTEM 1 (Praeger 2002).

[46] Froomkin, *supra* note 9, at 798.

[47] *Id* at 798 (footnote omitted); *see also* Kahn, *supra* note 13, at 191 (Noting that in 1863, when the military's traditionally re lied upon cryptography was forever broken, the military "found many good ideas in the writings of the dilettante cryptographers who had proposed ciphers for the protection of private messages. Soon some of these systems were serving in the various armies of Europe and the Americas.").

[48] Jefferson was known as the Father of American Cryptography. Kahn, *supra* note 13, at 195.

[49] *Id*. at 195. (The system, which was not widely known, is so secure that "[t]o this day the Navy uses it."); *see also* Froomkin, *supra* note 9, at 798.

[50] Froomkin, *supra* note 9, at 799-800 (footnote omitted).

While secrecy shrouded many communications, the framers of our Constitution most assuredly knew that crime existed and that criminals communicated in secret.[51] Yet, half the Bill of Rights limits the government's power to prosecute criminals.[52] With privacy and crime existing simultaneously, the Fifth Amendment was ratified with full knowledge that criminals could and would take advantage of any limitation on government's ability compel them to become witnesses against themselves. The privilege against self-incrimination was created in reaction to abuses of power by King George III,[53] and sought to limit prosecutorial abuse. Nothing of constitutional magnitude has altered this state of affairs since the Bill of Rights' ratification.[54]

Further, despite its potential for abuse by criminals, the privacy protected by the Fifth Amendment's privilege against self-incrimination has many benefits.[55] The United States Supreme Court outlined these benefits in interpreting the scope of the privilege in *Murphy v. Waterfront Comm'n of New York Harbor.*[56] In *Murphy*, union officials refused to testify, even with a state grant of immunity, because federal prosecution remained possible. The Court reversed the New Jersey Supreme Court in holding that, "the constitutional privilege against self-incrimination protects a state witness against incrimination under federal as well as state law and a federal witness against incrimination under state as well as federal law."[57] The *Murphy* Court recognized that the privilege may sometimes be "a shelter to the guilty" but that it is "often a

[51] Many framers themselves had been criminals while they secretly schemed against the Crown.

[52] E.g., U.S. CONST. amend. IV, U.S. CONST. amend V, U.S. CONST. amend. VI, U.S. CONST. amend. VII, U.S. CONST. amend. VIII.

[53] THE DECLARATION OF INDEPENDENCE para. 2 (U.S.1776).

[54] That is, unless the murderous terrorists of Sept. 11th, 2001 were more widely successful than they imagined and somehow proved themselves more threatening to the United States than agents and sympathizers of the Soviet Union during the Cold War, enemy agents during World Wars I and II, and confederate agents and sympathizers during the Civil War.

[55] Froomkin, *supra* note 9, at 799 ("[T]he possibility that more criminals will avoid detection if the privacy available to individuals were to be increased [does not] necessarily mean that choosing to increase privacy is unwise.").

protection to the innocent."[58] Some criticize the privilege for preventing compulsory process and thus preventing innocent defendants from exonerating themselves by grilling the guilty.[59] However, the *Murphy* Court, with no dissent, found the privilege justified the privilege for numerous reasons,[60] including its "unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt."[61]

IV. Compelled Decryption or Production of Private Keys Implicates the Fifth Amendment

An assertion of the privilege against self-incrimination is nullified where the government provides use and derivative-use immunity.[62] This immunity removes any danger of prosecution due to the person's compelled testimony. Therefore, such a grant of immunity is "coextensive with the scope of the privilege against self-incrimination."[63] Some scholars, most prominently

[56] Murphy, 378 U.S. 52 (1964).

[57] *Id.* at 77-78 (Goldberg, J., announcing the opinion of the court).

[58] *Id.* at 55. With this decision the Court at least implicitly responded to the criticism enumerated by Professor Sergienko, *supra* note 5, ¶ 39:

> [O]nly those who claim to be criminally incriminated by the key or the decrypted document can claim the protection of the Fifth Amendment. . .[T]his result seems unsatisfactory. Why should criminals have a right to privacy in their documents when non-criminals do not? The obvious answer is that the Fifth Amendment protects against self-incrimination, not against invasions of privacy.

[59] Akhil Reed Amar and Renee B. Lettow, *Fifth Amendment First Principles: The Self-Incrimination Clause*, 93 Mich. L. Rev. 857, 889, n.148 (1995).

[60] *Murphy*, 378 U.S. at 55:

> 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 dictates "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." (citations omitted).

[61] *Id*.

[62] Kastigar v. United States, 406 U.S. 441, 459-60 (1972) (Powell, J., announcing the opinion of the Court):

> [A]n analysis of prior decisions and the purpose of the Fifth Amendment privilege indicates that use and derivative-use immunity is coextensive with the privilege. . .The statute provides a sweeping proscription of any use, direct or indirect, of the compelled testimony and any information derived therefrom (citing and quoting 18 U.S.C. § 6002 "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…").

[63] *Murphy*, 378 U.S. at 54.

Phillip R. Reitinger,[64] have argued that compelled decryption of documents can occur without a grant of use and derivative-use immunity because providing immunity for the act of producing the decrypted document or private key will satisfy the privilege against self-incrimination.[65] Mr. Reitinger warned that because cryptology "restricts the ability of law enforcement to protect the public from the depredations of criminals," compelled production "is a minimal accommodation to the need for public security."[66]

[64] Formerly a Trial Lawyer, Computer Crime and Intellectual Property Section, U.S. Department of Justice, Reitinger is now a Senior Security Strategist for Microsoft Corporation.

[65] *See also* Susan W. Brenner, *The Privacy Privilege: Law Enforcement, Technology, and the Constitution*, 7 J. Tech. L. & Pol'y 123 (2002):

> When the encryption password was recorded, it assumed tangible form and became an artifact like the key to a strongbox … [compelling production of the password] would not, however, violate the Fifth Amendment if the statute gave the password holder immunity for the act of producing the password. Even absent a grant of immunity, enforcing the statute would not violate the Fifth Amendment if the government knew that the person possessed a password that had been reduced to tangible recorded form.

[66] Reitinger, *supra* note 35, at 205-6.

Despite contrary assertions,[67] the Fifth Amendment's privilege against self-incrimination prevents the government from compelling either decryption of encrypted documents or production of a private key unless use and derivative-use immunity is granted or the government has met, by clear and convincing evidence, the three-prong test from *Fisher v. United States*.[68] Mr. Reitinger concluded that immunity need not be granted by using the *Fisher* test in determining whether compelled production will violate the privilege against self-incrimination. Aside from one error,[69] Mr. Reitinger correctly enumerated how the *Fisher* Court held that compelled production of documents may implicitly communicate incriminating facts where the

[67] *Id.* at 196 ("[I]n most cases, the key should be producible by granting the same degree of immunity required to obtain production of the plaintext document associated with the key."); *see also* Raymond Shih Ray Ku, Article, *Modern Studies in Privacy Law: Searching for the Meaning of Fourth Amendment Privacy After Kyllo v. United States: The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 Minn. L. Rev. 1325, 1354 (2002):

> Relying upon the concepts of public exposure and assumption of risk, Orin Kerr has argued that government efforts to decrypt messages should not be considered searches under the Fourth Amendment. According to Kerr, once the government obtains an encrypted message, the message itself is effectively "in plain view." Encryption, therefore, merely affects the government's ability to understand the message, not to access it. As such, he argues that when "the government obtains communications in a form that it does not understand, the Fourth Amendment does not require law enforcement to obtain a warrant before translating the documents into understandable English." In other words, government decryption of a message is no different than the government's translation of Spanish into English, which is not considered a search under the Constitution. (citations omitted).

Mr. Kerr provided no support for the argument that the Fifth Amendment's privilege against self-incrimination remains protected where a suspect who has not been given use and derivative-use immunity is compelled to provide the means to decode encrypted documents that may implicate her. It is quite correct that the government can permissibly translate a seized document from Spanish to English. Since the government has access to the Spanish language, the government may freely attempt to translate the document. At trial or any hearing, different experts can debate the actual meaning of the intercepted message using this common language, as well as any potentially hidden messages, without the need for any assistance from the suspect. But the situation is different for encrypted messages. Mr. Kerr's translation analysis is only accurate where the government already possesses the means to decrypt this message, not where they seek to compel production of the means of translation. The government's freedom to try and translate an encrypted document cannot provide a right to compel decryption or private key production against the Fifth Amendment's privilege against self-incrimination. Mr. Kerr's analysis begs the question as to whether the government can compel the following "trilemma," *Murphy*, 378 U.S. at 55, to a suspect: I must choose between risking perjury, contempt, or provide a document which "would furnish a link in the chain of evidence needed to prosecute the claimant." Ohio v. Reiner, 532 U.S. 17, 20 (2001) (per curiam).

[68] *Fisher*, 425 U.S. 391.

[69] Mr. Reitinger, through insertion of the word 'and' in his list of three criteria from *Fisher*, implied that an act of production communicates incriminating facts only where all three are present. In fact, as Mr. Reitinger notes, the privilege against self-incrimination applies "when the accused is compelled to make a testimonial communication that is incriminating." Reitinger, *supra* note 35, at 178, n.30 (*citing Fisher*, 425 U.S. at 408). Therefore, if the government cannot meet any one of the three prongs of the *Fisher* test, the privilege against self-incrimination will apply.

act will: "(1) concede the existence of a document; (2) concede possession, location, or control of a document; [or][70] (3) assist in authentication of a document."[71] Compelled decryption or production of private keys may infringe on all of the three above concerns, thereby causing such compelled testimony to implicitly communicate incriminating facts and thus violate the Fifth Amendment's privilege against self-incrimination. In sum, under *Fisher*, the government can compel message decryption or private key production only where it proves that the requested document or private key: (1) exists; (2) was possessed, located or controlled by the person it is requested from; and (3) will not have its authentication assisted by this decryption or production.[72]

(A) Standard of Proof

(1) The Burden of Proving Compelled Production of Message Decryption or Private Key Production Must Rest With the Government

The government must bear the burden of proving each of the three prongs from *Fisher*. This burden is necessary to enforce the right to be free from self-incrimination and the presumption of innocence.[73] This burden is also important because the proliferation of encrypted documents means that many innocent people use them[74] and encrypted documents may soon bear great similarity to plaintext documents. The government must meet its burden before

[70] *See supra* note 69.

[71] Reitinger, *supra* note 35,. at 181. (*citing Fisher*, 425 U.S. at 410-413).

[72] *See also, e.g.,* Lance Cole, Article, *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, 166 (2002). ("If the government can show that existence, possession, and authenticity are a foregone conclusion, then the witness's assertion of the Fifth Amendment privilege against self-incrimination can be overridden and the production can be compelled without a grant of immunity.").

[73] Medina v. California, 505 U.S. 437, 455 (1992) (O'Connor, J., concurring) ("In determining whether the placement of the burden of proof is fundamentally unfair, relevant considerations include:. . .whether placing the burden of proof on the government is necessary to help enforce a further right, such as the right to be presumed innocent, the right to be free from self-incrimination...").

[74] See Froomkin, *supra* note 9, at 800 ("If everyone makes a habit of using strong cryptography, the presence of an encrypted message will never be probative of a guilty conscience or a need for secrecy."); *see also* Rueda, *supra* note 8.

compelling a person to decrypt a message.[75] If such a rule is not adopted, the government could point to any encrypted document it discovers and compel the purported author, under the penalty of perjury or contempt, to decrypt the document or provide the private key for such decryption. Such prosecutorial power could facilitate oppressive intrusion into every American's life. Despite the good intentions of those involved today,[76] and even though such intrusion could sometimes ensnare the guilty,[77] any such action must be struck down as unconstitutional.

(2) The Standard of Proof Must Be Clear and Convincing Evidence

Taking up a challenge offered by Professor Lance Cole,[78] I eschew the D.C. Circuit's "reasonable particularity" test[79] to posit that the government's burden here must demand that the government establish proof by clear and convincing evidence on each prong.[80] The D.C. Circuit's use of the standard given when a police officer decides to commit a pat down for

[75] The Fifth Amendment involves the right to remain silent. Miranda v. Arizona, 384 U.S. 436 (1966). The Fifth Amendment protects the innocent and guilty alike. *Reiner*, 532 U.S. at 18 ("The Supreme Court of Ohio here held that a witness who denies all culpability does not have a valid Fifth Amendment privilege against self-incrimination. Because our precedents dictate that the privilege protects the innocent as well as the guilty. . .[we] reverse.").

[76] Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting) ("The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.").

[77] Bostick v. State, 554 So. 2d 1153, 1158-1159 (Fla. 1989), rev'd, 501 U.S. 429 (1991):

> Roving patrols, random sweeps, and arbitrary searches or seizures would go far to eliminate such crime in this state. Nazi Germany, Soviet Russia, and Communist Cuba have demonstrated all too tellingly the effectiveness of such methods. Yet we are not a state that subscribes to the notion that [the] ends justify [the] means. History demonstrates that the adoption of repressive measures, even to eliminate a clear evil, usually results only in repression more mindless and terrifying than the evil that prompted them.

[78] Cole supra note 72, at 184-85:

> The only significant question left unanswered by the Supreme Court in Hubbell is how the courts should decide a close case in which the government has some prior knowledge but the witness asserts an act of production privilege and declines to produce the subpoenaed documents. Future development of the case law should answer this question, the lower courts decide whether to adopt the D.C. Circuit's "reasonable particularity" test - and nothing in the Supreme Court's Hubbell opinion suggests they should not do so - or develop alternative tests.

[79] United States v. Hubbell, 167 F.3d 552, 580-81 (D.C. Cir. 1999):

> [T]he 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. *See In re Grand Jury Subpoena Duces Tecum*, 1 F.3d 87, 93 (2d Cir. 1993). In making this assessment, though, the focus must remain upon the degree to which a subpoena "invades the dignity of the human mind," *Doe II*, 487 U.S. at 219-20 n.1 (Stevens, J., dissenting) and on the quantum of information as to the existence, possession, or authenticity of the documents conveyed via the act of production.

(footnote omitted).

weapons during a *Terry* stop[81] is widely inapposite to this situation. In *Terry*, the Court considered a situation where an officer justifiably "believ[ed] that the individual whose suspicious behavior he is investigating at close range is armed and presently dangerous to the officer or to others,"[82] when the Court held that "it would appear to be clearly unreasonable to deny the officer the power to take necessary measures to determine whether the person is in fact carrying a weapon and to neutralize the threat of physical harm."[83] Conversely, in compelled production situations, the police will be investigating at long range, not at close range. Also, the persons targeted by these subpoenas may not even be engaged in any suspicious behavior. Finally, a litigant who has gone to court to quash a subpoena cannot be automatically considered an armed and dangerous threat. There will be no exigency in these cases comparable to the dangers faced by police during a *Terry* stop situation. Yet, even if there was some exigency, it would only be proper for the court to approve of a "limited search of the outer clothing for weapons."[84] This pat down "constitutes a severe, though brief, intrusion upon cherished personal security, and it must surely be an annoying, frightening, and perhaps humiliating experience,"[85] but it would not be as broad as the intrusion that would occur if the government, upon meeting the mere "reasonable particularity test" could force any person to produce a broad range of documents, heretofore unknown of by the government, without a grant of immunity and then prosecute the person based upon any potential law violations uncovered through these disclosures.

[80] The government must be able to overcome the privilege without bootstrapping its proof by forcing a person to become a witness against herself, an action which would circumvent the privilege.

[81] *Id*. at 579 n.34 ("A search for weapons incident to a *Terry* stop is also assessed for whether the officer had a reasonable, particularized suspicion that the individual was armed." (citing Alabama v. White, 496 U.S. 325, 330 (1990)).

[82] Terry v. Ohio, 392 U.S. 1, 24 (1968).

[83] *Id*.

[84] *Id*. at 24-25.

[85] *Id*.

While any subjective ranking of immutable constitutional rights could be questioned, a person's interest in avoiding compelled self-incrimination must be at least as important as the right to avoid pretrial detention. Thus, the clear and convincing standard is appropriate because the Fifth Amendment interest against self incrimination at stake is comparable to that in pre-trial detention cases where the government, to overcome the Fifth Amendment due process liberty interest, must demonstrate a sufficiently compelling governmental need by clear and convincing evidence.[86] Similarly, the Fifth Amendment privilege against compelled self-incrimination can be compared to the Sixth Amendment right to counsel.[87] If the standard of proof here was less demanding than clear and convincing, the presumption of innocence and privilege against self-incrimination could be overridden by a governmental fishing expedition.[88]

(B) Applying the *Fisher* Test

(1) Proving that a Documents Exists

The first prong of the *Fisher* test is whether the compelled testimony will concede that a potentially incriminating document exists. A prosecutor's bare assertion that a document exists cannot establish a document's existence as a matter of law. Mr. Reitinger's claim that whenever law enforcement has seized a potentially encrypted document, the existence of this document is "a foregone conclusion" undoubtedly "misreads *Fisher* and ignores [the Court's] subsequent decision in *United States v. Doe*."[89] The *Fisher* Court forced a taxpayer's lawyer to produce the workpapers of the client's accountant. The Court held that the existence of the tax documents was "a foregone conclusion" because "the Government already knew that the documents were in

[86] Demore v. Hyung Joon Kim, 123 S. Ct. 1708, 1731, 538 U.S. 510 (2003) (Souter, J., dissenting).

[87] United States v. Wade, 388 U.S. 218, 239-40 (1967) (holding that where line-up identification occurred outside of the presence of counsel, the government must prove by a clear and convincing standard that the in-court identifications were based upon identifications of the accused outside those impermissible lineup identifications.).

[88] A lesser standard would unfavorably contrast the "sharply focused scheme" approved in the pretrial detention context. Foucha v. Louisiana, 504 U.S. 71, 81 (1992) (citing United States v. Salerno, 481 U.S. 739, 747-51 (1987)).

the attorneys' possession and could independently confirm their existence and authenticity through the accountants who created them."[90] The *Fisher* Court did not comp el decryption of documents the government could not otherwise use against her in a criminal trial. Notably, the *Fisher* Court focused on a narrow subpoena of business records that did not involve the production of any personal documents.[91] The point in *Fisher*, reiterated in *Doe* and *Hubbell*, is that the government must "independently confirm the existence and authenticity" of targeted documents before it can compel production.[92]

Undoubtedly, the government will sometimes independently prove the existence of encrypted documents. For example, the government often obtains, via a search warrant or otherwise, a defendant's hard drive either encrypted in its entirety or containing certain encrypted folders or documents. A court may be convinced that encrypted documents exist that can be accessed only with a private key. But there is one important corollary to the principle requiring proof of the existence of the documents the government seeks to access: unless the government had the defendant under intrusive surveillance,[93] it cannot prove that it has seized every single document that can be decrypted with this private key.

While claiming that production can be compelled from someone with access to an encrypted document, Mr. Reitinger argued that "production of keys is, for the most part, equivalent to the act of producing the decrypted document."[94] Mr. Reitinger later explained that

[89] United States v. Hubbell, 530 U.S. 27, 44 (2000) (citing Doe v. United States, 465 U.S. 605 (1984)).

[90] *Id.* at 44-45.

[91] *Fisher*, 425 U.S. at 401, n.7 (The government had narrowly sought documents of unquestionable relevance to their tax investigation.).

[92] *Hubbell*, 530 U.S. at 44-45.

[93] The government should have no need for compelled decryption since it should already have gleaned the private key through this surveillance.

[94] Reitinger, *supra* note 35, at 195-96. *But see* Wolfe, *supra* note 34, at 738 (applying *Andresen*, 427 U.S. 463) ("While it is possible that a court could disregard the distinction between the properties of the key itself and the use of the key, a reasonable understanding of the Fifth Amendment would require that a key not be deemed testimonial.").

while “a key has no substantive meaning at all,” he conceded that “act-of-production immunity should be necessary . . . only because possession of the key tends to demonstrate a connection between the possessor of the key and the underlying document.”[95] It is for this implied connection between the possessor and the underlying document that production of private keys cannot be compelled. Because existence must be proven before testimony can be compelled, the privilege can only be overcome regarding documents whose existence has been proven. But compelling production of a private key would facilitate decryption of any and all communications encrypted with this private key, even those documents whose existence has not been proven. A person will likely often use one public/private key set to encrypt all her communications.[96] Therefore, compelling private key disclosure can never be equivalent to compelled document decryption.[97] Compelling private key production will always be a greater intrusion than compelled document decryption.[98] Private key production would give the government access both to documents whose existence were proven[99] and provide access (while authenticating) documents the government did not know about.[100]

(2) Proving Possession, Location or Control: Rejecting the “Manna from Heaven” Approach[101]

The second prong of the *Fisher* test is whether the compelled testimony concedes possession, location, or control of a potentially incriminating encrypted document or private key

[95] Reitinger, *supra* note 35, at 196-97, n.108 (Noting that “[t]he inference would be that because the subpoenaed party possesses the key, the document came from and was possessed, in plaintext form, by that party.”).

[96] Memorization of a private key may be a difficult task and one private key should be enough since the encryption is impossible to break.

[97] *See supra* notes 35-36.

[98] One quandary is that the only way for the government to verify that a document was properly decrypted would be when someone qualified observed the decryption process. To prevent private key disclosure to the government, a neutral party sworn to secrecy by the Court should oversee the process to ensure that documents are decrypted properly while preserving the privacy of all private key.

[99] As well as provide a means of authenticating these documents. *See infra* Part IV(B)(3).

[100] Either because the documents had not been created or discovered by the government by the time of the hearing.

to decode the document. The government must bear the burden of independently proving this prong. If it does not, in the absence of use and derivative-use immunity, compelled testimony would infringe on the privilege against self-incrimination. In *Fisher*, the Court approved compelled production of tax records because possession, location, or control over these documents was proven because it was not disputed that the accountants who created the records were available to testify.[102]

It does not logically follow that a person with possession or control of certain encrypted documents, even where access to these documents has been proven, is the only one with the private key to decrypt these documents.[103] It will be difficult for the government to prove that each document it seeks has been possessed, located, or controlled by the person from whom decryption is demanded. Besides surveillance or independent testimony, for example from an informant, the only way the government could meet this prong would be to force a person to answer whether she has accessed the documents or whether she alone has the private key to decrypt these documents,[104] two questions that implicate the Fifth Amendment by forcing a person to authenticate possible evidence against her.

Fisher is also distinguishable from this compelled decryption case for other important reasons. The *Fisher* Court explained that the applicability of the privilege against self-incrimination will "depend on the facts and circumstances of particular cases or classes

[101] Robert P. Mosteller, *Cowboy Prosecutors and Subpoenas for Incriminating Evidence: The Consequences and Correction of Excess*, 58 WASH. & LEE L. REV. 487, 514 (2001).

[102] Fisher v. United States, 425 U.S. 391,410-11 (1976) (The Court held that "[i]n light of the records now before us, we are confident that however incriminating the contents of the accountant's workpapers might be, the act of producing them - the only thing which the taxpayer is comp elled to do - would not itself involve testimonial self-incrimination.").

[103] A private key has greatest worth if it is known only to one person, but that does not mean that any given private key is known by only one person.

[104] Naturally, proving access plus proving that only one person has the means of access meets this prong.

thereof."[105] First, *Fisher* involved the disclosure of tax papers which had been prepared by someone else, not private papers.[106] The special nature of private papers has been long recognized by the Court,[107] a recognition that must not be diminished simply because these private papers are stored in a computer. Second, and most importantly for this article, it is uncontested that decrypting a document and bringing it in under compulsion will communicate incriminating facts by conceding "possession, location, or control of a document."[108] Mr. Reitinger agreed that the potential for government exploitation of compelled self-incrimination was so explicitly present that there may be no option other than providing act-of-production immunity for these disclosures.[109]

Where act-of-production immunity is provided, it was believed that a person's Fifth Amendment rights could be protected by treating this evidence produced under compulsion as if it had "magically appeared in grand jury room."[110] This is the "manna from heaven" treatment of compelled disclosure.[111] This "long advocated government position"[112] was soundly rejected in

[105] *Fisher*, 425 U.S. at 410-11.

[106] *Id.* at 414 ("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.'").

[107] Froomkin, *supra* note 9, at 833 ("[T]he Court has never questioned the special nature of some private noncommercial personal papers, such as diaries, and has held that these retain their Fifth as well as Fourth Amendment protection."); *see, e.g.,* Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 459 n.22 (1977) (Brennan, J.) (noting that the most personal of documents are entitled to special protection). The protection is from subpoenas only, not search warrants. But, search warrants cannot be useful for compelling access to encrypted documents.

[108] Reitinger, *supra* note 35, at 181.

[109] *Id.* at 202:

> Although the existence of a key may be a foregone conclusion, who possesses the key is not known. The government cannot establish that it is a foregone conclusion that the suspect possesses the key, and it may need to use the act of production to introduce and demonstrate access to the encrypted document. In short, the act of production adds to the government's knowledge. Accordingly, act-of-production immunity for the suspect is probably required.…

[110] Mosteller, *supra* note 94, at 513 n.119 (citing Samuel A. Alito, Jr., *Documents and the Privilege Against Self-Incrimination*, 48 U. PITT L. REV. 27, 59-60 n.27 (1986)).

[111] *Id.* at 514.

[112] *Id.* at 513.

Hubbell.[113] The Court told the prosecution that the Fifth Amendment's privilege against self-incrimination meant that the government could not compel Mr. Hubbell to produce documents, under a grant of immunity, and then prosecute him based upon these disclosures.[114] The Court criticized the government's "anemic view of respondent's act of production as a mere physical act that is principally non-testimonial in character and can be entirely divorced from its 'implicit' testimonial aspect."[115] In sum, the *Hubbell* Court held the "manna from heaven" approach inappropriate.[116]

The *Hubbell* Court cited a part of *Doe* which Mr. Reitinger dismissed as dicta,[117] when holding that "[t]he 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."[118] *Hubbell* held where a person asserts the privilege but is compelled after a grant of use and derivative-use immunity, no indictment derived from this information can survive.[119] Analogous to *Hubbell*, compelled decryption may occur only after a grant of use and derivative-use immunity, such as provided for

[113] United States v. Hubbell, 530 U.S. 27, 31 (2000) (Webster Hubbell objected to the government's use of information from documents he turned over after being granted immunity "to the extent allowed by law.").

[114] Mosteller, *supra* note 102,at 514-15 (Citing *Hubbell*, 530 U.S. at 44-45) (Stevens, J.) (The Court "rejected the government's attempt to limit use immunity to direct uses by the prosecution of the communicative aspects of the act of production and never to the contents.")

[115] *Hubbell*, 530 U.S. at 44-45.

[116] *Id.* at 42-43 ("It was only through respondent's truthful reply to the subpoena that the Government received the incriminating documents of which it made 'substantial use ... in the investigation that led to the indictment.'").

[117] Reitinger, *supra* note 35, at 203 ("[T]he Supreme Court has indicated in dicta that being compelled to testify about the combination of a safe implicates the Fifth Amendment.") (*Citing* Doe v. United States, 487 U.S. 201, 219 (1988)).

[118] *Hubbell*, 530 U.S. at 42-43:

> It was unquestionably necessary for respondent to make extensive use of "the contents of his own mind" in identifying the hundreds of documents responsive to the requests in the subpoena. … 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. *Doe*, 487 U.S. 210 n.9 (Blackmun, J.) ("We do not disagree with the dissent … [w]e simply disagree with the dissent's conclusion that the execution of the consent directive at issue here forced petitioner to express the contents of his mind."); *see also Doe*, 487 U.S. at 219 (Stevens, J., dissenting) ("A defendant … may in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe -- by word or deed.").

[119] *Hubbell*, 530 U.S. at 45 ("*Kastigar* requires that [a dismissal be] granted unless the Government proves that the evidence it used in obtaining the indictment and proposed to use at trial was derived from legitimate sources

in 18 U.S.C. §6002.[120] Unless the government makes a narrow request for certain documents,[121] and meets the *Fisher* test, immunity must be granted. Using the *Hubbell* analysis, it appears that compelling a person to decrypt documents whose contents are unknown to the government is like the constitutionally impermissible act of compelling a person to provide "a combination to a wall safe."[122] Compelled disclosure of a private key is like forcing a person to provide combinations to multiple wall safes she has used in the past, even those the government is unaware of, and to future wall safes (namely, those created whenever someone uses her public key). The wall safe analogy is impenetrable when considering compelled production of a memorized private key.[123]

(3) Proving Lack of Authentication: Facing the Cruel Trilemma of Self-accusation, Perjury or Contempt

The third prong of the *Fisher* test is whether compelled testimony will help authenticate a potentially incriminating document or the private key to decrypt this document. Therefore, the government cannot rely on non-immunized compelled decryption of a document to authenticate itself because it bears the burden of independently authenticating a document to avoid infringing on the privilege against self-incrimination. Mr. Reitinger recognized that "the government could use possession of the key to prove the possession or authenticity of the underlying document."[124] But he mistakenly claimed that authentication of a key, and thus authentication of the document it decodes "is a foregone conclusion" and can always be relied upon because proof of

'wholly independent' of the testimonial aspect of respondent's immunized conduct in assembling and producing the documents described in the subpoena.").

[120] *Id.* at 40, n.22.

[121] *See, e.g.,* Fisher v. United States, 425 U.S. 391, 401 n.7 (1976).

[122] *Hubbell*, 530 U.S. at 43. *See also* Adam C. Bonin, Comment, *Protecting Protection: First and Fifth Amendment Challenges to Cryptography Regulation*, 1996 U. CHI. LEGAL. F. 495, 514 (1996) ("The courts likely will find that compelling someone to reveal the steps necessary to decrypt a PGP-encrypted document violates the Fifth Amendment privilege against compulsory self incrimination. Because most users protect their private keys by memorizing passwords to them and not writing them down, access to encrypted documents would almost definitely require an individual to disclose the contents of his mind.").

[123] *See supra* Part IV(B)(4).

[124] Reitinger, *supra* note 35, at 196.

"possession of the key, combined with the fact that the key does decrypt the [encrypted document], establishes that … [this is the] key to the document."[125] Such a position simply eviscerates the privilege against self-incrimination by removing the government's burden to independently verify the authentication of the document.

Compelled testimony cannot be the sole source to verify the authenticity of that same compelled testimony or else the Fifth Amendment would only protect the innocent.[126] The privilege against self-incrimination protects the innocent and guilty alike.[127] The presumption of innocence is a founding principle of the rule of law in the United States.[128] Just as the Fourth Amendment does not exclude illegally gained evidence against only the factually innocent,[129] the Fifth Amendment's privilege must extend to all those accused of crime, [130] especially while the presumption of innocence remains sacrosanct.[131] The privilege against self-incrimination has long prevented the government from asking a person about the "existence of sources of

[125] *Id.* at 199.

[126] This position is akin to making confessions in violation of Miranda legal if a person's confession verified the government's suspicions of guilt. If a person could be compelled, without a grant of use and derivative-use immunity, to turn over her private keys or decrypt any potentially encrypted documents upon government request, without facing the authentication prong, only those whose compelled testimony is not self-authenticating could properly invoke the Fifth Amendment. This analysis makes the Fifth Amendment's privilege against self-incrimination a dead letter by allowing an impermissible bootstrapping authentication in contravention of the privilege against self-incrimination.

[127] *Reiner*, *supra* note 75; *see also Murphy*, 378 U.S. at 55 (While the rule is "sometimes 'a shelter to the guilty,' it is often 'a protection to the innocent.'").

[128] Estelle v. Williams, 425 U.S. 501, 503 (1976) (Burger, C.J., announcing the opinion of the Court) ("The presumption of innocence, although not articulated in the Constitution, is a basic component of a fair trial under our system of criminal justice. Long ago this Court stated: 'The principle that there is a presumption of innocence in favor of the accused is the undoubted law, axiomatic and elementary, and its enforcement lies at the foundation of the administration of our criminal law.'").

[129] Andrew E. Taslitz, Condem*ning the Racist Personality: Why the Critics of Hate Crimes Legislation Are Wrong*, 40 B.C. L. Rev 739, 748 ("[T]he Fourth Amendment seeks to protect both the innocent and the guilty, shielding 'privacy [that] enables the individual to constitute himself as the unique person he is,' an aspect of the 'fully realized life' and a 'condition . . . for the realization of the common good.'") (footnotes omitted).

[130] *See supra* note 120.

[131] United States v. Salerno, 481 U.S. 739, 767 (1987) (Marshall, J., dissenting):

Honoring the presumption of innocence is often difficult; sometimes we pay substantial social costs as a result of our commitment to the values we espouse. But at the end of the day the presumption of innocence protects the innocent; the shortcuts we take with those whom we believe to be guilty injure only those wrongfully accused and, ultimately, ourselves.

potentially incriminating information."[132] The *Kastigar* Court held that the privilege "protects against any disclosures that the witness reasonably believes could be used in a criminal prosecution or could lead to other evidence that might be so used."[133] The *Reiner* Court reiterated that the privilege "extends not only 'to answers that would in themselves support a conviction . . . but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant.'"[134] The Court added that "[i]t need only be evident from the implications of the question, in the setting in which it is asked, that a responsive answer to the question or an explanation of why it cannot be answered might be dangerous because injurious disclosure could result."[135] The questions 'decrypt these documents for us' or 'produce a private key to decrypt these documents' infringes on the privilege unless the third prong has been established by proof that this compelled decryption or private key production will not help authenticate the produced document or private key. The government may counter that authentication is near impossible without access to a decrypted message. Therefore, where the government establishes the first two *Fisher* prongs, it can proffer in camera (possibly ex parte), the independent proof of authentication it has. The court will then review the document in

[132] *Hubbell*, 530 U.S. at 43 ("[W]e have no doubt that the constitutional privilege against self-incrimination protects the target of a grand jury investigation from being compelled to answer questions designed to elicit information about the existence of sources of potentially incriminating evidence."); *Kastigar*, 406 U.S. at 444 (Powell, J.) ("[T]he power to compel testimony is not absolute. There are a number of exemptions from the testimonial duty, the most important of which is the Fifth Amendment privilege against compulsory self-incrimination."); *see also Andresen*, 427 U.S. at 473-74:

> A party is privileged from producing the evidence but not from its production ... thus, although the Fifth Amendment may protect an individual from complying with a subpoena for the production of his personal records in his possession because the very act of production may constitute a compulsory authentication of incriminating information,a seizure of the same materials by law enforcement officers differs in a crucial respect[, as] the individual against whom the search is directed is not required to aid in the discovery, production, or authentication of incriminating evidence. (citations omitted).

[133] *Kastigar*, 406 U.S. at 444-45 (Powell, J.):

> The privilege reflects a complex of our fundamental values and aspirations, and marks an important advance in the development of our liberty. It can be asserted in any proceeding, civil or criminal, administrative or judicial, investigatory or adjudicatory; and it protects against any disclosures that the witness reasonably believes could be used in a criminal prosecution or could lead to other evidence that might be so used. This Court has been zealous to safeguard the values that underlie the privilege.

[134] *Reiner*, 532 U.S. at 20 (*citing* Hoffman v. United States, 341 U.S. 479, 486 (1951)).

question[136] to determine if it has been independently authenticated and thus whether immunity is required for compelled decryption.

(4) Disclosing by Word or Deed

Compelled testimony about a private key or the existence of incriminating evidence such as decrypted documents, even where it has met the three-prong *Fisher* test, must involve act-of-production immunity or else the person questioned would impermissibly face "the cruel trilemma of self-accusation, perjury or contempt."[137] Unless the government provided act-of-production immunity, a person compelled to provide this information would face this trilemma because such a disclosure would allow the government to introduce the evidence that this person produced this document at such and such a time upon a request from the government.

The Court, in both *Doe* and *Hubbell*, asserted that a suspect cannot "be compelled to reveal the combination to his wall safe -- by word or deed."[138] The government cannot avoid this prohibition by not requesting entry into the safe but by non-specifically requesting any and all contents of the safe. Nor could the government avoid this prohibition by simply seeking all combinations to any safes in a person's possession.[139] The private key to decode a message is analogous to the combination to a wall safe. Therefore, if the government cannot either secure or break the password required to translate encrypted documents, it cannot simply request all encrypted documents in a person's possession unless it provides use and derivative-use

[135] *Id.* at 20-21 (*citing Hoffman*, 341 U.S. at 486-87).

[136] The person must decrypt the document in question for the Court. *See supra* note 92. This will not imply the privilege because prosecution may only occur if the *Fisher* test is met, which would mean that the privilege does not apply.

[137] *Murphy*, 378 U.S. at 55.

[138] *See supra* note 111.

[139] *See* Reitinger, *supra* note 35, at 198, n.116 ("If the subpoena instead called for all keys in one's possession, however, it would not call for the exercise of testimonial judgment to the same extent.").

immunity.[140] Since the government cannot force a non-immunized[141] suspect to disclose the combination to a wall safe, it cannot compel a person to disclose all of her encrypted messages.

Compelling production of a memorized private key can never be permissible. Such an act is particularly analogous to the forbidden act of compelling production of "the combination to a wall safe."[142] Mr. Reitinger recognized that "memorized passwords might defeat the government's subpoena power," but quickly dismissed this proposition. He believed that private keys small enough to be memorized could now be broken by brute force attacks.[143] He thought that a person could be compelled to turn over their private key or decrypt documents, with the government only providing act-of-production immunity, because keys "too long to be memorized" would be "stored on a computer, in encrypted form for security."[144] Production of the key could be compelled because "the plaintext of a key stored in encrypted form in hardware or software is itself a document subject to subpoena."[145] But, he failed to note that even a stored private key can only be compelled after satisfaction of the three-prong *Fisher* test.[146]

Even where the government can independently confirm "the existence, possession, and authenticity of the subpoenaed documents"[147] by clear and convincing evidence,[148] Mr.

[140] *Kastigar*, 406 U.S. at 459 (such immunity is coextensive with the Fifth Amendment).

[141] Meaning use and derivative-use immunity: Act-of-production immunity is presumed. *See supra* Part IV(B)(2).

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

[143] Reitinger, *supra* note 35, at 205 ("[O]nly truly memorized passwords might defeat the government's subpoena power, and the government is more likely to be able to "break" encryption if people use small, memorized keys."). Mr. Reitinger ignores the possibility that with the growth of biometrics, modern passkeys might be single word or pass phrase, unbreakable because the simple word or phrase could trigger access to an algorithm in combination with a retinal scan, face recognition, and/or a palm print. *See* Michael Richarme, *Biometric Systems, The Next Big Security Opportunity*, *Decision Analyst, Inc*., 2002 http://www.decisionanalyst.com/publ_art/Biometrics.asp [January 18, 2004] ("Biometric security systems, still in their early development stages, have already been successfully employed, giving corporations key insight into ways to affordably and effectively employ the newest of security technologies.").

[144] Reitinger, *supra* note 35, at 204.

[145] *Id.* at 205 (Adding that if documents "reflecting an exchange of keys" exist, these are also "subject to subpoena").

[146] *See supra* at Part IV(B)(1-3).

[147] *Hubbell*, 530 U.S. at 44 (quoting U.S. v. Hubbell, 167 F.3d 552, 580 (D.C. Cir. 1999)).

[148] *See supra* at Part IV(A)(2).

Reitinger's own analysis demonstrates that the government cannot compel disclosure of memorized public keys without providing use and derivative-use immunity. Memorized public keys may proliferate due to a combination of biometric security procedures with memorized passwords. Biometric identifiers may even soon serve as a private key itself. These methods provide security to any person who seeks privacy for private keys and encrypted documents.[149] In either situation, the password created can only be disclosed if a person is compelled to orally state a memorized word while providing her palm print, iris scan, and/or DNA sample. Therefore, to gain access to encrypted information, the government must compel specific oral testimony before a grand or petit jury, along with other actions.[150] A person can be compelled to talk, get fingerprinted, or provide a DNA sample, but not compelled to recite from memory something she has an expectation of privacy in.[151] Compelled production of memorized, private

[149] Access to private keys may be hidden behind spoken passwords, voice analyzed, in conjunction with a palm print, retinal scan, and/or DNA sample. *See, e.g.*, Oscar H. Gandy, Jr., *Exploring Identity and Identification in Cyberspace*, 14 ND J. L. Ethics & Pub. Pol'y 1085, 1091 (2000) ("The routine use of biometric techniques is likely to develop as a way of ensuring that the user has been reliably identified."); *see* http://www.iriscan.com [January 18, 2004]; John D. Woodard, *Biometric Scanning, Law & Policy: Identifying the Concerns - Drafting the Biometric Blueprint*, 59 U. Pitt. L. Rev. 97-98 (1997) ("[B]oth the governmental and private sectors are making extensive use of biometrics to provide better service to the public.").

[150] Braswell v. United States, 487 U.S. 99, 113-15 (1988) (Rehnquist, C.J., announcing the opinion of the Court) (A line has been drawn between "oral testimony and other forms of incrimination," with oral testimony not being subject to compulsion without immunity.). The government can compel someone speak for a witness to hear the tone of her voice, but the government cannot compel her to say something that she has kept private and that she has an interest in keeping private.

[151] *See, e.g.*, United States v. Mara, 410 U.S. 19, 21 (1973) (Stewart, J., announcing the opinion of the Court) ("[T]he Fourth Amendment … is not violated by a grand jury directive compelling production of 'physical characteristics' that are 'constantly exposed to the public.' Handwriting, like speech, is repeatedly shown to the public, and there is no more expectation of privacy in the physical characteristics of a person's script than there is in the tone of his voice."); United States v. Dionisio, 410 U.S. 1, 14 (1973) (Stewart, J., announcing the opinion of the Court) ("[T]he Fourth Amendment provides no protection for what "a person knowingly exposes to the public, even in his own home or office . . . ." 389 U.S. at 351. The physical characteristics of a person's voice, its tone and manner, as opposed to the content of a specific conversation, are constantly exposed to the public. Like a man's facial characteristics, or handwriting, his voice is repeatedly produced for others to hear. No person can have a reasonable expectation that others will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world.").

keys and documents encrypted in such a manner would be impermissible without the granting of use and derivative-use immunity.[152]

V. Conclusion

Why can the government compel a suspect to hand over a physical key to a strongbox,[153] but it cannot compel a suspect to recite, from memory, a private key to gain access to a virtual strongbox?[154] The Fifth Amendment's privilege against self-incrimination guarantees "personal control over the production of cognitive evidence, free of official coercion."[155] Unless this constitutional principle is altered, the government must rely on other methods of crime control. For example, the police have "untrammeled authority to unleash informants on the population."[156] These "human bug[s]"[157] are more likely to put the government in a position to prevent crimes, not just punish them after the fact through compelled testimony. The innocent should not need to live in fear of compelled privacy violations.[158] Removing the privilege against self-incrimination is not and cannot be the government's best solution to deter and punish crime.[159]

[152] *See* Bonin, *supra* note 114, at 497 ("[T]he Fifth Amendment precludes the government's ability to coerce individuals to decrypt their documents. As long as users memorize their passwords and do not commit them to paper, the government will prove unable to force them to decrypt their documents.").

[153] An actual strongbox can be forced open by government officials.

[154] A virtual strongbox cannot otherwise be broken into by government officials.

[155] H. Richard Uviller, *Evidence from the Mind of the Criminal Suspect: A Reconsideration of the Current Rules of Access and Restraint*, 87 Colum. L. Rev. 1137, 1137 (1987).

[156] Tracey Maclin, *Informants and the Fourth Amendment: A Reconsideration*, 74 Wash. U. L. Q. 573, 623 (1996).

[157] *Id.* at 625.

[158] *See also* Greg Sergienko, *United States v. Hubbell: Encryption and the Discovery of Documents*, 7 Rich. J.L. & Tech. 31 (2001) ("Because the determinedly guilty have always had ways to shield themselves, the primary effect of encryption is more to assure individuals that their privacy will be respected.").

[159] Reitinger, *supra* note 35, at 205 (Concluding that smart criminals will destroy their keys before being subpoenaed and that those "[f]aced with the choice of providing a key that will unlock critical evidence or refusing and facing the risk, but not certainty, of contempt, many will run the risk of contempt by claiming a loss of memory or that a written key has been destroyed.").