View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Pittsburgh Journal of Technology Law and Policy (University of Pittsburgh)

Journal of Technology Law & Policy

Volume XIV – Fall 2013

ISSN 2164-800X (online)

DOI 10.5195/tlp.2013.132

http://tlp.law.pitt.edu

Give Me Your Password Because Congress Can Say So: An Analysis of Fifth Amendment Protection Afforded Individuals Regarding Compelled Production of Encrypted Data and Possible Solutions to the Problem of Getting Data from Someone's Mind

Michael Wachtel

(cc) BY-NC-ND

This work is licensed under a Creative Commons Attribution-Noncommercial-No Derivative Works 3.0 United States License.

This site is published by the University Library System of the University of Pittsburgh as part of its D-Scribe Digital Publishing Program and is cosponsored by the University of Pittsburgh Press.

Give Me Your Password Because Congress Can Say So: An Analysis of Fifth Amendment Protection Afforded Individuals Regarding Compelled Production of Encrypted Data and Possible Solutions to the Problem of Getting Data from Someone's Mind

Michael Wachtel*

INTRODUCTION

In the summer of 2009, Federal Bureau of Investigation (FBI) agents compelled Google Inc. to disclose a wealth of incriminating documents from a suspect's Google Docs account.[1] The suspects, "Levi Beers and Chris de Diego, [were] the alleged operators of a firm called Pulse Marketing."[2] They were suspected of launching a deceptive email marketing campaign, "spamming" millions of users with information regarding a diet supplement.[3] The suspects were shocked to find out that their documents were not secured or protected, because they thought Google, the company providing electronic document storage services, had a duty to maintain its customers' privacy.[4] The FBI was not only able to compel Google to release information; it did so without having to show probable cause.[5] Instead the FBI needed to establish the lower "reasonable ground" standard to obtain the information.[6] The government is able to obtain documents from a third-party storage, or email provider, under the 1986 Stored Communications Act

* J.D. Candidate, Rutgers University School of Law, Class of 2014. This note is dedicated to my mom, dad, and the Aharon family, for without their love, support, and guidance I would not have been able to get through the rigors of law school.

[1] Kevin Poulsen, *Spam Suspect Uses Google Docs: FBI Happy*, WIRED (Apr. 16, 2010 3:20 PM), http://www.wired.com/threatlevel/2010/04/cloud-warrant/.

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] *Id.*

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

(SCA).[7] The SCA enables the government to access a customer's data whenever there are "reasonable grounds" to believe that the information would be relevant in a criminal investigation.[8] In addition to Google, other third-party storage providers have admitted that government compulsion of a customer's data would be possible even if the data is encrypted by the third-party provider.[9] A spokesperson for Dropbox Inc., a corporation that provides the extremely popular online storage system, explained that "like most online services, we have a small number of employees who must be able to access user data for the reasons stated in our privacy policy (e.g., when legally required to do so)."[10] Thus, companies like Google and Dropbox Inc. will not protect their customers' files against government intrusion.[11] However, what about individuals who encrypt and store their files in personal storage systems, such as a computer?

---

[7] Poulsen, *supra* note 1; *see also* Stored Wire and Electronic Communications and Transactional Records Access Act of 1986, 18 U.S.C. § 2703 (2012).

[8] *See* 18 U.S.C. § 2703 (2012), stating in relevant parts:

> **(a) Contents of wire or electronic communications in electronic storage.** A governmental entity *may require the disclosure* by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. (emphasis added).
>
> **(d) Requirements for court order.** A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are *reasonable grounds* to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider. (emphasis added).

[9] *See, e.g.*, Ryan Singel, *Dropbox Lied to Users About Data Security, Complaint to FTC Alleges*, WIRED (May 13, 2011 4:54 PM), http://www.wired.com/threatlevel/2011/05/dropbox-ftc/.

[10] *Id.*

[11] The Government's action compelling Google to give them Levi Beers' and Chris de Diego's files on Google Docs was based in the Western District of New York where the CSA is still judicially

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

Today, personal computers are in many respects akin to a safe: they are used to protect documents and files that the owner wishes to remain private. Why else would a person utilize password based encryption tools on their computer if they were not trying to keep it private? Although the Fourth Amendment ensures that citizens are protected against unlawful searches and seizures, it also permits the government to seize a person's computer if they have "probable cause" to do so.[12] In light of this, an interesting issue arises when the hard drive of a lawfully seized computer is protected by software or an operating system, which cannot be cracked by the respective law enforcement's forensic unit. This issue was addressed in *In re Grand Jury Subpoena Tecum Dated March 25, 2011 (United States v. Doe) (Doe IV)*, where the forensic detective was unable to decrypt a suspect's seized laptop.[13] The Court of Appeals for the Eleventh Circuit declared that compelling the defendant to relinquish his password in order for the state to decrypt his files was unconstitutional, and violated his Fifth Amendment right against self-incrimination.[14]

This Note addresses how courts currently view the government's attempted compulsion of a defendant's password and encryption keys, and whether the government's use of this information to decrypt the defendant's device triggers the defendant's Fifth Amendment right against self-incrimination. Additionally, this Note analyzes the suggested solutions for how to deal with password-encrypted data in a trial setting, and recommends a legislative solution. Part I provides background information regarding encryption technology, and how the technology creates *an evidence collection* problem for the state's case in chief. Part II addresses whether password compulsion is violative of the Fifth Amendment under *stare decisis*, and how the forgone conclusion doctrine relates to evidence that might be protected by a defendant's Fifth Amendment privilege. Part III analyzes the pros and cons of current and suggested ways of overcoming Fifth Amendment protection that were granted based on the privilege clause against self-incrimination. Finally, this Note addresses the following issue: whether legislation

---

adhered by that circuit. *See* Poulsen, *supra* note 1. *But see* United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) (holding that Internet Service Provider customers deserve a reasonable expectation of privacy and the SCA is unconstitutional to the extent that it allows the government to obtain emails without a warrant). However, other circuits, like the second circuit in Google's case are not forced to follow the sixth circuit's precedent, until the Supreme Court makes a final determination regarding the CSA.

[12] *See* U.S. CONST. amend. IV (stating that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized").

[13] United States v. Doe, 670 F.3d 1335, 1340 (11th Cir. 2012) [hereinafter *Doe IV*].

[14] *Id.* at 1352–53.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

dealing with the encryption problem would pass constitutional muster and, if so, whether it could offer a viable solution to the Fifth Amendment privilege against self-incrimination that passwords create.

I. ENCRYPTION: HISTORY AND ITS EFFICACY

The study and practice of encryption is referred to as cryptography.[15] Originally cryptography meant the science of secret writing.[16] Today cryptography is the study of how parties safeguard important information on personal devices, such as computers, by using passwords as a form of encryption.[17] Cryptography is not a recent innovation and humans have been using forms of data protection for nearly 4,000 years.[18] Encryption places a password on or blocks access to certain data, making it undecipherable to third parties.[19] That data can only become accessible to a third party if it is decrypted-turning the undecipherable data into regular text.[20] Depending on if the data is encrypted or decrypted, it is either "plaintext" or "ciphertext."[21] The "plaintext" is the data that a person wishes to encrypt, while the "ciphertext" is the undecipherable product resulting from the encryption.[22] "Anyone wishing to uncover the secret message, including the government acting in their criminal investigatory capacities, will be after the underlying data, i.e., the plaintext."[23]

An example of this practice during Greek times, "involved the tattooing of a secret message on the scalp of a slave, allowing the slave's hair to grow back, and then sending the slave to the recipient of the message so that his head could be shaved and the secret message revealed."[24] Julius Caesar used cryptography to prevent his military communications from being intercepted. Caesar "employed the simple cryptographic process of shifting every letter in the alphabet up three steps,

[15] Andrew J. Ungberg, Note, *Protecting Privacy Through a Responsible Decryption Policy*, 22 HARV. J.L. & TECH. 537, 540 (2009).

[16] Brendan M. Palfreyman, *Lessons from the British and American Approaches to Compelled Decryption*, 75 BROOK. L. REV. 345, 348 (2009).

[17] Ungberg, *supra* note 15, at 540.

[18] *Id.*

[19] Palfreyman, *supra* note 16, at 348–49.

[20] *Id.* at 348–49.

[21] *Id.* at 349.

[22] *Id.*

[23] *Id.*

[24] *Id.*

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

such that a 'B' would become a 'E,' and a 'P' would become an 'S'."[25] Today, cryptography has become significantly more complex then when it was employed by the early Greeks and Caesar.[26] Today, freely available software can render data virtually undecipherable without the proper password or encryption key.[27]

Unlike the old days of ciphers being decoded by tattooing or the use of letter keys, today's digital world requires complex methods for encryption and decryption.[28] When a message is encrypted using current technology an "encryption key" is required to decrypt the message.[29] An encryption key is basically a very long string of numbers that is stored in the encryption software's memory.[30] The software users do not have to remember this long number; "instead [they] can enter a more easily remembered password or passphrase, which in turn activates the encryption key."[31] When the government "seeks to compel an ordinary citizen to turn over the means by which he can decrypt the data, the disclosure order will typically compel him to turn over his password rather than the encryption key."[32]

The two primary encryption methods are public key encryption and or private key encryption.[33] Most past encryption has been accomplished using the private key method.[34] This method involves one key that is used for both encrypting and

[25] Palfreyman, *supra* note 16, at 349.

[26] *Id.*

[27] A powerful software encryption program named TrueCrypt can be downloaded free of charge at its website, http://www.truecrypt.org/ (last visited Nov. 29, 2012).

[28] Palfreyman, *supra* note 16, at 350.

[29] Anoop MS, *Public Key Cryptography: Application Algorithms and Mathematical Explanations* (2007), *available at* http://www.infosecwriters.com/text_resources/pdf/Public_Key_Cryptography_AMS.pdf ("The public key algorithms operate sufficiently large numbers to make [deriving the private key from the public key] practically impossible and thus make the system secure. For example, RSA algorithm operates on large numbers of thousands of bits long.").

[30] *Id.*

[31] Palfreyman, *supra* note 16, at 350.

[32] *Id.* at 350–51.

[33] *See* D. Forest Wolfe, *The Government's Right to Read: Maintaining State Access to Digital Data in the Age of Impenetrable Encryption*, 49 EMORY L.J. 711, 715 (2000).

[34] *Id.*

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

decrypting the encoded message.[35] The sender uses a certain key to encrypt the message, and the receiver uses that same key to decrypt it.[36]

In 1976, cryptologists Whitfield Diffie and Martin Hellman proposed a new method called public key encryption.[37] In this system, there are two keys: a public key used for encryption and a private key used for decryption.[38] The public key may be available to multiple persons or the public at large, but only the person using the encryption knows the private key.[39] For example, if one wishes to send a secure message using this type of encryption, he would encrypt the message using a public key, send it, and then the recipient would decrypt the message using her private key.[40] One hoping to intercept and decrypt this message would be unable to do so using only the public key, because it is a "computationally infeasible" task to derive the private key from the public key.[41] This is known as a "one-way function" because the key is only easily solvable in one direction.[42] The only way to ascertain the private key in such circumstances is to use a specialized computer

[35] *Id.*

[36] *Id.*

[37] Whitfield Diffe & Martin E. Hellman, *New Directions in Cryptography*, 12 IEEE TRANSACTIONS ON INFO. THEORY 644 (1976), http://www4.ncsu.edu/~singer/437/proj38.pdf. Public key encryption was actually invented earlier than 1976 by members of the British Government Communications Headquarters, but their findings were not disclosed. *See* Martin Campbell-Kelly, *Not All Bad: An Historical Perspective on Software Patents*, 11 MICH. TELECOMM. & TECH. L. REV. 191, 230 (2005).

[38] Anoop MS, *supra* note 29, at 3.

[39] *Id.*

[40] *Id.*

[41] Diffie & Hellman, *supra* note 37, at 644. *See also* Anoop MS, *supra* note 29, at 1–2. It is an infeasible task to try to derive the key computationally because:

> The private and public key of a device is related by mathematical function called the one-way function. One-way functions are mathematical functions in which the forward operation can be done easily but the reverse operation is so difficult that it is practically impossible. In public key cryptography the public key is calculated using private key on the forward operation of the one-way function. Obtaining of private key from public key is a reverse operation. If the reverse operation can be done easily, that is if private key is obtained from the public key and other public data, then the public key algorithm for the particular key is cracked. The reverse operation gets difficult as the key size increases.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

program that guesses, one at a time, the correct number.[43] This process can take an exceptionally long time.[44] Thus, breaking strong public key encryption is virtually impossible without compelling, or otherwise obtaining, access to the private key.[45]

There are many software companies that offer key encryption technologies.[46] Microsoft Corporation's Windows product has provided its BitLocker Drive Encryption utility free with the operating system since Windows Vista Ultimate[47] was generally released in January of 2007.[48] Unlike some other encryption methods,[49] BitLocker encrypts the entire hard drive and not just particular files.[50] BitLocker can "help block hackers from accessing the system files they rely on to discover your password, or from accessing your drive by removing it from your computer and installing it in a different computer."[51] When forensic detectives seize a suspect's computer during an investigation, they have to remove the hard drive and make a copy of it in order to avoid tainting the evidence for trial purposes.[52] BitLocker prevents the detective who is following proper evidence guidelines from being able to gain access the suspect's hard drive. Furthermore, BitLocker encrypts files automatically and the files remain encrypted until they are

---

[42] Anoop MS, *supra* note 29, at 3.

[43] *See In re* Grand Jury Subpoena to Boucher, No. 2:06-mj-91, 2007 U.S. Dist. WL 4246473, at *2 (D. Vt. Nov. 29, 2007) ("The only way to get access without the password is to use an automated system which repeatedly guesses passwords. According to the government, the process . . . could take years. . . .").

[44] *Id.*

[45] *Id.*

[46] *See* Paul Rubens, *Buyer's Guide to Full Disk Encryption*, ESECURITY PLANET (May 9, 2012), http://www.esecurityplanet.com/mobile-security/buyers-guide-to-full-disk-encryption.html (naming Microsoft's BitLocker, TrueCrypt (for Windows or Macintosh), and McAfee Endpoint Protection as a few of the encryption products available).

[47] *See Chapter 2: BitLocker Drive Encryption*, MICROSOFT TECHNET (Apr. 4, 2007), http://technet.microsoft.com/en-us/library/cc162804(d=printer).aspx.

[48] *See* Tim Fisher, *Windows Vista: Important Facts About Microsoft Windows Vista*, ABOUT.COM (Dec. 24, 2012), http://pcsupport.about.com/od/windowsvista/a/windows-vista.htm.

[49] Encrypting File System (EFS) enables you to encrypt specific files on you operating system's hard drive, but does not allow you to encrypt your whole hard drive. *See Help protect your files using BitLocker Drive Encryption*, MICROSOFT.COM, http://windows.microsoft.com/en-us/windows7/help-protect-your-files-using-bitlocker-drive-encryption (last visited Oct. 16, 2013) [hereinafter BitLocker Info].

[50] *Id.*

[51] *Id.*

[52] *See Doe IV*, 670 F.3d at 1340 (stating the forensic examiner McCrohan testified for the state that he had to clone "5 TB of data from the digital media devices—an 'enormous amount of data,'" further detailing what steps they followed in investigating the defendant's computer).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

decrypted, which is accomplished by entering the password recovery key.[53] Additionally, Microsoft's operating system does not include a "backdoor," which would enable one to "[bypass] normal authentication to gain access to a computer without the computer user knowing."[54] Therefore, in an investigation the state could not compel Microsoft to disclose the "master key" because Microsoft did not create one.[55]

Strong encryption programs like BitLocker are available for other operating systems as well. Apple Inc. (Apple) provides a similar type of encryption utility called FireVault for its Macintosh computer users.[56] The encryption program works with Apple's operating system OS X Mountain Lion, the most common operating system.[57] The disk encryption that it uses is a government approved, advanced encryption standard.[58] In order to access FileVault, the user must enter a login password, Apple ID, and the program's recovery key.[59] This makes any Apple hard drive that is FireVault-enabled nearly impossible to access by forensic investigators during a criminal investigation. Like Microsoft, Apple has refused to program "backdoor" access for its users.[60]

Finally, there are many popular publicly available encryption utilities if a user does not want to use Microsoft's or Apple's encryption programs.[61] TrueCrypt is a free open-source disk encryption utility, available for both the Windows and Macintosh platforms.[62] Unlike BitLocker and FileVault, TrueCrypt enables the user

---

[53] *See* BitLocker Info, *supra* note 49.

[54] Joris Evers, *Microsoft: Vista Won't Get Backdoor*, CNET.COM (Mar. 3, 2006, 6:00 PM), http://news.cnet.com/Microsoft-Vista-wont-get-a-backdoor/2100-1016_3-6046016.html (reporting Microsoft has stated that it will not provide "backdoors" in its Windows Vista Ultimate that the government could use to access encrypted files).

[55] *Id. See also* BitLocker Info, *supra* note 49 (stating further on Microsoft's website that a BitLocker user should "create [a] recovery key when you turn on BitLocker for the first time; otherwise, you could permanently lose access to your files.").

[56] *OS X Mountain Lion: About FileVault Disk Encryption*, APPLE.COM, http://support.apple.com/kb/PH10578 (last visited Nov. 30, 2012).

[57] *Id.*

[58] *Id.* (stating that Apple's encryption is 128-bit AES key encryption, one of the strongest encryption platforms).

[59] *Id.*

[60] *Id.* (stating "Warning: Don't forget your administrator password. If you turn on disk encryption and then forget your log in password, your Apple ID, and your recovery key, you won't be able to log in, and your files and settings are lost forever").

[61] *See* Rubens, *supra* note 46.

[62] TRUECRYPT.ORG, http://www.truecrypt.org/ (last visited Nov. 30, 2012).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

to create multiple passwords within the encrypted date and, in a sense, create hidden files or volumes that are encrypted within the encryption.[63] This means that even if a user is compelled to provide her first password, the second password that was created for hidden files will not be discovered.[64] Additionally, when an unauthorized user attempts to access the non-hidden password and fails, the hidden section is automatically filled with random data and held there until the right password is entered.[65] The hidden data will remain filled and blocked with random data, appearing as random digits to a person attempting to view the data, until the first password is entered correctly.[66]

The defendant in *Doe IV* used TrueCrypt to encrypt his hard drive.[67] The detective testified that he "accessed parts of the drive only to find 'a blank area of the hard drive, and there was no data, you know, physically, that we were able to see.'"[68] Based on the foregoing, the government will probably not be able to access a suspect's computer that is encrypted with one of the aforementioned utilities without the encryption password.

---

[63] *See Hidden Volume*, TRUECRYPT.ORG, http://www.truecrypt.org/docs/hidden-volume (last visited Nov. 30, 2012).

[64] *Id.*

[65] *See id.*

[66] *See id.* The TrueCrypt organization states:

> TrueCrypt first attempts to decrypt the standard volume header [data] using the entered password. If it fails, it loads the area of the volume where a hidden volume header can be stored . . . to RAM [memory] and attempts to decrypt it using the entered password. Note that the hidden [data] cannot be identified, as they appear to consist entirely of random data. If the header is successfully decrypted . . . the information about the size of the hidden volume is retrieved from the decrypted header . . . and the hidden [data] is [revealed].

[67] *See Doe IV*, 670 F.3d at 1340.

[68] *Id.* at 1340 n.10.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

II. FIFTH AMENDMENT: THE SELF-INCRIMINATION PRIVILEGE

The Fifth Amendment's assurance that no person "shall be compelled in any criminal case to be a witness against himself"[69] is "one of the great landmarks in man's struggle to be free of tyranny, to be decent and civilized."[70] But one question that the U.S. Supreme Court has yet to address regarding the Fifth Amendment is whether the state's compulsion of an arrestee's computer password is a per se violation of that arrestee's Fifth Amendment right against self-incrimination. In other words, whether the right not to supply the state with a password is akin to the right not to respond to a criminal inquiry when being questioned by the state, or the right to remain silent. One of the Supreme Court's main motivations in securing the right of silence was to avoid the "cruel trilemma"[71] thereby preserving individual autonomy.[72] The cruel trilemma is the decision a defendant would face if forced to choose between maintaining her silence (not providing the password) and being held in contempt of court, or speaking (providing the password) and either perjuring or incriminating herself.[73] The Fifth Amendment provides individuals a way out of this cruel choice—remain silent without fear of contempt.[74] But other than the scenario of arrestee silence, the Court has analyzed what types of individual compulsions, e.g., forced blood tests, alcohol tests, and compelling a defendant's combination to a safe, may or may not be covered by the Fifth Amendment. This has resulted in various approaches and tests that courts now adopt.

A. The Nature and Scope of the Self-Incrimination Privilege

The U.S. Court of Appeals for the Fifth Circuit in *United States v. Authement* established that in order for an individual to fall within the protection of the Fifth Amendment they must establish the following three elements: (1) compulsion, (2) a testimonial communication or act, and (3) incrimination.[75] The first element,

---

[69] U.S. CONST. amend. V.

[70] WILLIAM O. DOUGLAS, AN ALMANAC OF LIBERTY 238 (1954).

[71] *See, e.g.*, Henry J. Friendly, *The Fifth Amendment Tomorrow: The Case for Constitutional Change*, 37 U. CIN. L. REV. 671, 694–95 (1968); *see also* Murphy v. Waterfront Comm'n, 378 U.S. 52, 55 (1964) (describing how the Court is unwilling "to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt").

[72] *See* John Lilburne, *The Just Defense of John Lilburne*, *reprinted in* THE LEVELLER TRACTS, 1647–1653, at 450, 454, (William Haller & Godfrey eds., Columbia Univ. Press 1944, 1653).

[73] *See* Friendly, *supra* note 71, at 695.

[74] *Id.*

[75] United States v. Authement, 607 F.2d 1129, 1131 (5th Cir. 1979).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

compulsion, has been defined by courts in many ways,[76] and compelling a password to be disclosed may be construed as a unique act of compulsion which will be discussed later in section B. The second and third elements deal with protecting oneself from being a witness against him or herself. This part of the Fifth Amendment's privilege against self-incrimination is satisfied if the evidence or act being sought from the defendant by the state is *testimonial* in nature and therefore self-incriminating.[77] Whether an act or piece of evidence qualifies as testimonial may depend on the court's adherence to *stare decisis*.

In *Schmerber v. California*, the Court ruled that the Fifth Amendment "protects an accused only from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature."[78] In *Schmerber* the defendant was forced to submit a blood sample after he was pulled over in his automobile in order to determine his blood-alcohol content.[79] The Court held that the drawing of blood in those circumstances did not violate the Fifth Amendment.[80] The Court explained, "[the] distinction which has emerged, often expressed in different ways, is that the privilege [against self-incrimination] is a bar against compelling communications or testimony, but that compulsion which makes a suspect accused of real or physical evidence does not violate it."[81]

Schmerber's holding has not been easily understood. Some scholars note that *Schmerber* leaves serious Fifth Amendment questions unanswered.[82] The Court's distinction between physical and non-physical evidence can be seen in the following situation: if a suspect who is hooked up to a polygraph machine is forced to submit to questioning but not compelled to answer, the Fifth Amendment would not be implicated because the suspect has not provided any communication or testimony.[83] The scientific evidence that could be collected in this situation, such as heart rate and blood pressure, is permissible because it constitutes physical

---

[76] *See, e.g.*, Lefkowitz v. Turley, 414 U.S. 70, 79, 84–85 (1973) (analyzing different ways that compulsion has been defined under the Fifth Amendment).

[77] *See* Fisher v. United States, 425 U.S. 391, 409 (1976).

[78] *Schmerber*, 384 U.S. at 761 (1966).

[79] *Id.* at 758–59.

[80] *Id.*

[81] *Id.* at 764.

[82] *See, e.g.*, Ronald J. Allen & M. Kristie Mace, *The Self-Incrimination Clause Explained and its Future Predicted*, 94 J. CRIM. L. & CRIMINOLOGY 243, 259–60 (2004).

[83] *Id.* at 248–49, 261.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

evidence.[84] Importantly, this evidence, though not testimonial under *Schmerber*, could serve as self-incriminating evidence against the accused. For this reason, the Court seems to be drawing an unexplained divergence between certain violations of the Fifth Amendment. The Court further recognizes this concern regarding physical evidence which could serve as self-incriminating evidence by stating, "[t]here will be many cases in which such a distinction is not readily drawn. Some test seemingly directed to obtain 'physical evidence' for example lie detector tests measuring changes in body function during interrogation, may actually be directed to eliciting responses that are testimonial."[85] The Court then concludes to "compel a person to submit to testing in which an effort will be made to determine his guilt or innocence on the basis of physiological responses, whether willed or not, is to evoke the spirit and history of the Fifth Amendment."[86]

After *Schmerber*, the Court shifted its focus away from the notion of physical versus non-physical evidence in determining whether an action or statement is testimonial. Instead, the Court focused on whether the defendant confronted the cruel trilemma.[87] In *Pennsylvania v. Muniz*, the defendant was pulled over on suspicion of drunk driving.[88] Muniz was arrested due to his intoxication, and at trial the officers testified that Muniz appeared intoxicated during their questioning of him because he had incorrectly answered a question about the date of his sixth birthday.[89] Muniz objected to the admission of the substance of his statements as well as inferences that could be drawn from them, since he contended they violated his Fifth Amendment privilege against self-incrimination.[90]

Regarding the officer's testimony that Muniz responded to questions with slurred speech, the Court held that "any slurring of speech and other evidence of lack of muscular coordination revealed by Muniz's responses to Officer Hosterman's direct questions constitute nontestimonial components of those responses."[91] Consequently, evidence of Muniz's physical condition while answering the questions was not protected by the Fifth Amendment. However, Muniz's assertion that his failure to recall the date of his sixth birthday was deemed

[84] *Id.* at 261.

[85] Schmerber v. California, 384 U.S. 757, 764 (1966).

[86] *Id.*

[87] Pennsylvania v. Muniz, 496 U.S. 582, 596–99 (1990).

[88] *Id.* at 585.

[89] *Id.* at 586–87.

[90] *Id.* at 587.

[91] *Id.* at 592.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

inadmissible on grounds that it was testimonial.[92] The Court ruled "when a suspect is asked for a response requiring him to communicate an express or implied assertion of fact or belief, the suspect confronts the 'trilemma' of truth, falsity, or silence, and hence the response contains a testimonial component."[93]

Writing for the Court, Justice Brennan held that the Fifth Amendment protects individual suspects and defendants when they face a cruel trilemma.[94] For Muniz, the trilemma was the choice to either not answer the police officers questions and appear to be hiding something, or answer the questions incorrectly and face incriminating himself. Thus Muniz should be protected from having to decide between whether to answer the officer's complex questions and relinquish his Fifth Amendment privilege, or to not answer these questions and appear guilty.

Unfortunately, like in *Schmerber*, the broad language of *Muniz* has been difficult to define and apply. This is due in part to the diverse opinions amongst the Justices in concluding whether the question relating to the date of Muniz's sixth birthday was truly testimonial.[95] Five Justices found that Muniz's response to the question should be excluded. However Justice Marshall cast the deciding vote, and wrote separately stating the response was inadmissible because Muniz was not given adequate Miranda warnings prior to questioning.[96] Although it is clear that the birthday question in Justice Marshall's mind was testimonial, he never had to reach this conclusion since he determined that Muniz was not given his Miranda warnings.

Writing for the four dissenting Justices, Justice Rehnquist argued that because "it was permissible for the police to extract and examine a sample of Schmerber's blood to determine how much that part of his system had been affected by alcohol," it should be equally permissible to evaluate Muniz's speech in order to evaluate his level of intoxication.[97] *Muniz* is still good law, though it rests on a shaky foundation due to the Justices' varying opinions.

In *Doe v. United States* (*Doe II*), the Supreme Court attempted to define the limits of the Fifth Amendment's protections regarding a defendant who is compelled to provide allegedly self-incriminating evidence in order to assist the

[92] *Id.* at 599.

[93] *Muniz*, 496 U.S. at 597.

[94] *Id.* at 597–98.

[95] Allen & Mace, *supra* note 82, at 274–75.

[96] *Muniz*, 496 U.S. at 608.

[97] *Id.* at 607.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

government with their investigation.[98] In *Doe*, several Cayman Islands and Bermuda banks refused to comply with the U.S. government's subpoenas to turn over any accounts or records associated with Doe because their governments prohibited such disclosure without customer consent.[99] Consequently, the U.S. government filed a motion to have Doe sign a consent form, which did not identify or acknowledge the existence of any accounts, authorizing the banks to disclose any records so that the banks would comply with the U.S. government's subpoenas.[100] The lower court ordered the defendant to sign the consent form.[101]

The Supreme Court found that although "the executed form allows the Government access to a potential source of evidence, the directive itself does not point the Government toward hidden accounts or otherwise provide information that will assist the prosecution in uncovering evidence."[102] The Court concluded that the consent form was not testimonial in nature because in "signing the form, Doe [made] no statement, explicit or implicit, regarding the existence of a foreign bank account or his control over any such account."[103] Additionally, his signing the form did not "admit the authenticity of any records produced by the bank."[104]

Following *Doe II* and *Muniz*, the Court in *United States v. Hubbell* held that evidence may be excluded if the suspect was forced to utilize mental capacities in producing it.[105] In *Hubbell* the defendant was being investigated for a series of federal offenses regarding his corporation.[106] During a previous prosecution on unrelated charges, the defendant agreed to provide information related to the subsequent investigation of his corporation.[107] Pursuant to that agreement, the prosecutor in the second case subpoenaed the same defendant to provide any and all documents relating to his corporation.[108] The defendant initially claimed that the use of the agreement to compel information relating to the second investigation

[98] *Doe II*, 487 U.S. 201 (1988).

[99] *Id.* at 205–06.

[100] *Id.*

[101] *Id.* at 205.

[102] *Id.* at 215.

[103] *Id.* at 215–16.

[104] *Doe II*, 487 U.S. 216.

[105] United States v. Hubbell, 530 U.S. 27 (2000).

[106] *Id.* at 30.

[107] *Id.*

[108] *Id.* at 31.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

violated his Fifth Amendment rights; however, he later complied after being granted immunity. Despite the grant of immunity, the government still indicted Hubbell on tax evasion and fraud charges.[109]

With regards to Hubbell's act of producing the documents, the Supreme Court held that forcing a defendant to provide a prosecutor with information that would lead to potentially incriminating evidence contravenes the defendant's rights against compelled self-incrimination.[110] The Court reasoned that "[i]t was unquestionably necessary for respondent to make extensive use of *contents of his own mind* in identifying the hundreds of documents responsive to the requests in the subpoena."[111] Moreover, the Court emphasized 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."[112]

Following *Hubbell*, commentators were quick to recognize that the Court was apparently changing the focus of its Fifth Amendment analysis.[113] The Court seemed to change its test from a physical versus non-physical distinction to a test that prevents the government from compelling a suspect's mental powers to assemble its case.[114] This dramatic shift could have serious implications for future applications of both *Schmerber* and *Muniz* to the extent that the blanket categorical rules presented in those cases may be displaced by the cognitive standard set out in *Hubbell*. However, some scholars point out that *Hubbell* does not explicitly adopt a cognitive requirement, but instead can only be read to imply such a test.[115]

It is unclear whether *Schmerber*, *Muniz*, *Doe II*, or *Hubbell* will be the controlling case for what constitutes testimonial acts protected by the Fifth Amendment's privilege against self-incrimination. However, it is completely plausible that the Supreme Court will not adopt a particular standard, and instead proceed on a case-by-case basis in analyzing whether the compulsion is testimonial and deserving of Fifth Amendment protection. Notwithstanding further speculation regarding what the Supreme Court will do, when it comes to the state forcing a defendant to give up their computer password, as the next section points out, the

---

[109] *Id.* at 27–28.

[110] *See id.* at 43.

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

[112] *Id.*

[113] *See, e.g.*, Jody C. Barillare, Comment, *As its Next Witness, The State Calls . . . The Defendant: Brain Fingerprinting as "Testimonial" Under the Fifth Amendment*, 79 TEMP. L. REV. 971, 991 (2006).

[114] *Id.*

[115] *See id.*

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

lower courts have generally followed the *Hubbell* line of thinking, except for a limited number of exceptions.[116]

B. Compelled Passwords are Testimonial and Incriminating Since They Reveal the Contents of One's Mind

After *Hubbell*, *Muniz*, and *Schmerber*, the Supreme Court still did not face the issue of computer passwords, and whether they were testimonial, and therefore protected under the Fifth Amendment. But in *United States v. Fisher* the Court established that the reach of the Fifth Amendment's privilege against self-incrimination might extend to a defendant who is compelled to produce incriminating evidence.[117] Furthermore, in *United States v. Doe* (*Doe I*), the Court held that even the act of producing unprotected and unprivileged evidence by a defendant for the state could have communicative aspects that may be "testimonial" and thereby entitled to Fifth Amendment protection.[118] The Court stated that "the contents of a document may not be privileged, [however] the act of producing the document may be."[119]

The lower courts faced tough questions when dealing with the circumstances of a defendant having to disclose a password to the prosecution to allow them to gain access to the defendant's property. Can the state compel the disclosure of the contents of one's mind without leading to a *Hubbell* violation? More fundamentally, does the compelled use of a password that decrypts a defendant's encryption software become an act of production and thus a violation of the defendant's Fifth Amendment rights under *Doe I*? The Sixth Circuit addressed the *Hubbell* question in the following cases.

In 2010, the U.S. District Court for the Eastern District of Michigan in *United States v. Kirschner* addressed whether a defendant's Fifth Amendment privilege against self-incrimination extended to the defendant's computer password.[120] The government had issued a subpoena compelling the defendant to provide all passwords associated with his computer or any files on the computer.[121] With the

---

[116] *See Doe IV*, 670 F.3d at 1346 (concluding what the government sought to compel demanded the contents of one's mind their password key, and therefore it was testimonial and covered under *Hubbell*. Additionally, since the foregone conclusion doctrine was not applicable in this instance it could not be viewed as an exception to *Hubbell*'s use of mind test.).

[117] *See* Fisher v. United States, 425 U.S. 391, 408 (1976).

[118] United States v. Doe, 465 U.S. 605, 612 (1984) [*Doe I*].

[119] *Id.*

[120] United States v. Kirschner, 823 F. Supp. 2d 665, 668 (E.D. Mich. 2010).

[121] *Id.* at 666.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

subpoena, the government sought evidence of child pornography allegedly contained in encrypted files on the defendant's computer.[122] The defendant filed a motion to quash the subpoena based on his Fifth Amendment privilege against self-incrimination.[123]

The court answered the defendant's motion by analyzing relevant Supreme Court precedent.[124] Referencing *Hubbell*, the court stated that it "agree[d] with [the] Defendant because . . . [the precedent was] set forth in *United States v. Hubbell*."[125] The court analogized a computer password to a wall safe combination that only resides in someone's mind, which, as *Hubbell* resolved, is testimonial, and therefore protected.[126] By stating that this "case is not about producing specific documents—it is about specific testimony asserting a fact," the Court concluded that the self-incrimination clause protected the defendant from revealing his computer password procured through mental processes to assert an incriminating fact.[127]

In February 2012, the Eleventh Circuit in *Doe IV* addressed the *Doe I* act of production issue regarding when a compelled act is testimonial.[128] It also addressed whether the act of decryption itself, based on passwords given by a defendant, would be protected by the Fifth Amendment privilege against self-incrimination.[129] The government was investigating Doe, a Youtube.com account holder suspected of sharing child pornography.[130] By tracing several Internet protocol addresses, government officials tracked Doe to several hotels.[131] They subsequently secured and executed a warrant for Doe's hotel room; officers seized seven pieces of digital

---

[122] *Id.*

[123] *Id.*

[124] *Id.* at 668.

[125] *Id.*

[126] *Kirchner*, 823 F. Supp. 2d. at 669 (quoting *Hubbell*, 530 U.S. at 43). For further support, the court cited Justice Steven's majority opinion in *Hubbell*, and analogizes the compulsion of a computer password to that of privileged information that was recalled in an individual's mind. The court stated, "[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." *Id. See also* Part II B *supra* discussing *Hubbell*.

[127] *Kirchner*, 823 F. Supp. 2d at 669.

[128] *See* Part II A *supra* discussing *Doe I*.

[129] *Doe IV*, 670 F.3d at 1341.

[130] *Id.* at 1339.

[131] *Id.*

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

media, including two laptops and five external hard drives.[132] While analyzing the digital media, the forensic examiners could not gain access to the hard drives because they were encrypted with the TrueCrypt software.[133] The government tried to avoid triggering Doe's Fifth Amendment right against self-incrimination by offering him a limited act-of-production immunity in exchange for his password.[134] Doe refused; he reasoned that the immunity would not extend to the government's derivative use of the hard drives after they obtained his password.[135] He was held in civil contempt because he refused to decrypt the hard drives for the grand jury subpoena.[136] He appealed his contempt judgment, and challenged the order given by the prosecutor to decrypt the drives as a violation of his Fifth Amendment right against self-incrimination.[137]

The Eleventh Circuit reversed the district court and held that the "decryption and production of the hard drives' contents would trigger Fifth Amendment protection because it would be testimonial, and that such protection would extend to the Government's use of the drives' contents."[138] Echoing *Hubbell*, the court stated that, "[t]he touchstone of whether an act of production is testimonial is whether the government compels the individual to use the 'contents of his own mind' to explicitly or implicitly communicate some statement of fact."[139] The court stressed that the act of decryption and production would require Doe to reveal the contents of his mind.[140] The court further reasoned that "[r]equiring Doe to use a decryption password is most certainly more akin to requiring the production of a combination because both demand the use of the contents of the mind, and the production is accompanied by [] implied factual statements [] that could prove to be incriminatory."[141]

Thus, in criminal cases where the government compels a defendant to provide a computer password, or to provide the computer or it's drives in an already

---

[132] *Id.*

[133] *Id.* at 1340. *See* Part I *supra* discussing TrueCrypt software.

[134] *Id.* at 1339.

[135] *Doe IV*, 670 F.3d at 1339.

[136] *Id.* at 1340.

[137] *Id.* at 1341.

[138] *Id.*

[139] *Id.* at 1345.

[140] *Doe IV*, 670 F.3d at 1346.

[141] *Id.*

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

decrypted state (with the password already entered), circuit courts have agreed that this type of request violates the Fifth Amendment's right against self-incrimination. The reason being that entering a password to decrypt one's computer requires an individual to use the contents of one's mind in order to communicate a potentially incriminating fact.

C. The Foregone Conclusion Doctrine: A Limited Exception

While the precedent that *Hubbell* sets—that compulsion of the contents of one's mind by the government is testimonial and therefore protected by the Fifth Amendment—is still good law, courts have carved out an exception to this rule. The foregone conclusion doctrine holds that if the state in an investigation is able to prove that the contents they are trying to compel have been reasonably seen and verified, then it is a foregone conclusion that the evidence sought is known and therefore will not be protected under the ambit of the Fifth Amendment.[142] In *In re Grand Jury Subpoena Duces Tecum Dated October 29, 1992* (*United States v. Doe*) (*Doe III*), the Second Circuit said that the existence and location of a calendar, that the state compelled the defendant to produce, was a foregone conclusion.[143] This was because it was known, through production of a photocopy, that the suspect had possession of the calendar and therefore compulsion of the original added little or nothing to the sum total of the government's information.[144] This exception has become known as the "foregone conclusion" doctrine.[145]

In 2006, Sebastien Boucher was crossing the Canadian border into Vermont when he was stopped by U.S. Customs officials.[146] After a secondary inspection, a customs agent found a laptop in the back seat of his car.[147] The agents were able to gain access to approximately 40,000 images without the use of a password.[148] A special agent with experience in recognizing child pornography discovered

---

[142] *See In re* Grand Jury Subpoena to Sebastien Boucher (*Boucher II*), No. 2:06-mj-91, 2009 WL 424718, at *3 (D. Vt. Feb. 19, 2009).

[143] *See In re* Grand Jury Subpoena Duces Tecum Dated October 29, 1992, 1 F.3d 87, 93 (2d. Cir. 1993) [hereinafter *Doe III*]; *see also* United States v. Fisher, 425 U.S. 391, 411 (1976).

[144] *Fisher*, 425 U.S. at 411.

[145] *See id.* (stating the original foundation of the foregone conclusion doctrine was established in *Fisher v. United State* where the Court stressed where the existence and location of evidence is known to the government, "no constitutional rights are touched because the matters are a foregone conclusion"); *see also Doe III*, 1 F.3d at 93.

[146] *In re* Grand Jury Subpoena to Sebastien Boucher (*Boucher I*), No. 2:06-mj-91, 2007 WL 4246473, at *1 (D. Vt. Nov. 29, 2007).

[147] *Id.*

[148] *Id.*

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

thousands of images depicting adult and child pornography.[149] After Boucher was read his Miranda rights, the agent asked Boucher if he could view the contents of a hard drive labeled drive Z.[150] The agent asked Boucher to leave the room, and as he examined drive Z he found several additional images and videos of child pornography.[151] The agent was able to view the images on the hard drive before it was shutdown, however, as soon as it was turned off, the encryption was activated and the computer was inaccessible for trial. Boucher was charged with the crime of transporting child pornography.[152]

Like in *Doe IV*, the forensic detectives in *Boucher I* were unable to create a mirror of Boucher's laptop contents because the videos on the Z drive were encrypted, and inaccessible without the password.[153] In order to gain access to drive Z, the state sought a subpoena requiring Boucher to provide all passwords associated with the seized computer.[154] Boucher moved to quash the subpoena asserting that the compulsion of his password was a violation of his Fifth Amendment right against self-incrimination.[155] The court agreed with Boucher and found that entering a computer password is testimonial because it implicitly communicates facts, and that if Boucher "[did] know the password, he would be faced with the forbidden trilemma: incriminate himself, lie under oath, or find himself in contempt of court."[156]

The state further argued that even if the compulsion of Boucher's password was covered under the Fifth Amendment, the foregone conclusion doctrine permits the government's access to the Z drive because a law enforcement agent already viewed some of the incriminating evidence before the computer was shut down.[157] The court in *Boucher I* held that even if the "government [had] seen some of the

---

[149] *Id.*

[150] *Id.* at *2.

[151] *Id.*

[152] *In re* Grand Jury Subpoena to Sebastien Boucher (*Boucher I*), 2007 WL at *2.

[153] *See Boucher I*, 2007 WL 4246473, at *2 (the state who brought in Secret Service Agent Mathew Fasvlo, who had experience in computer forensics and testified that "it [was] nearly impossible to access [the] encrypted files without knowing the password. There are no 'back doors' or secret entrances to access the files.").

[154] *Id.*

[155] *Id.*

[156] *Id.* at *3.

[157] *Id.* at *6.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

files on drive Z, it [had] not viewed all or even most of them" and therefore the foregone conclusion was not an applicable exception.[158] The state appealed.

Chief Judge William Sessions overturned the magistrate judge, stating that "Second Circuit precedent . . . [did] not require that the government be aware of [all of] the incriminatory contents of the file; it requires the government to demonstrate with reasonable particularity that it knows of the existence and location of subsequent documents."[159] Judge Sessions declared that the state did have particular knowledge of the existence of child pornography on Boucher's Z drive; consequently, the foregone conclusion doctrine applied.[160] The court denied Boucher's motion to quash the subpoena, and directed him to provide an unencrypted version of the Z drive.[161]

In *United States v. Fricosu*, the U.S. District Court for the District of Colorado was asked to decide whether the foregone conclusion doctrine applied to Ms. Ramona Fricosu.[162] The FBI executed a search warrant at her residence during which agents seized six computers.[163] Of the six computers, three were laptops, one of which had an encryption program that required a password to access its contents.[164] The next day Fricosu spoke with her incarcerated husband Scott Whatcott, and through a recorded conversation Fricosu admitted that the encrypted laptop was hers.[165] Based on the fact that the laptop was labeled "RS.WORKGROUP.Ramona"[166] and pursuant to the All Writs Act,[167] the state sought to require Fricosu to produce the unencrypted contents of the laptop.[168] Fricosu refused, and claimed the compelled disclosure of the password to decrypt the laptop violated her Fifth Amendment right against self-incrimination.[169]

---

[158] *Id.*

[159] *Boucher II*, 2009 WL at *3.

[160] *Id.*

[161] *Id.* at *4.

[162] *See* United States v. Fricosu, 841 F. Supp. 2d 1232, 1237 (D. Col. 2012).

[163] *Id.* at 1234.

[164] *Id.*

[165] *Id.* at 1235.

[166] *Id.* at 1234.

[167] 28 U.S.C. § 1651 (2006) (enabling the Supreme Court and all courts established by Congress to issue orders that aid in the usage and principles of law).

[168] *Fricosu*, 841 F. Supp. 2d at 1235.

[169] *Id.*

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

The court held that Fricosu was like the defendant in *Boucher II*, and said that there is "little question here but that the government knows of the existence and location of the computer's files. The fact that it does not know the specific content of any specific document[] is not a barrier to production."[170] The court determined that the fact that she admitted to her husband during their phone conversation that the contents were accessible by only her and that the computer was identified as "RS.WORKGROUP.Ramona," was sufficient for authorities to conclude that the contents belonged to her.[171] Therefore, her motion to quash was denied, and the Fifth Amendment protection did not cover the production of the unencrypted contents of the requested laptop."[172]

In *Doe IV*, however, the defendant was able to quash the state's motion compelling him to provide a password for his encrypted hard drive on *Hubbell* grounds.[173] The court concluded that password disclosure meant disclosing the thoughts of the person's mind.[174] Despite this holding, the government had argued that even if password compulsion violated the Fifth Amendment, the foregone conclusion doctrine would still allow them to compel Doe to provide an unencrypted version of the drive.[175]

The Eleventh Circuit denied the government's claim and held that "[n]othing in the record [revealed] that the government knew whether any files exist or [where] the location of those files [was] on the hard drive."[176] Additionally, there was nothing to illustrate that the "Government knew with reasonable particularity that Doe was even capable of accessing the encrypted portions of the drives."[177] Unlike the special agent in *Boucher* or the telephone conversation in *Fricosu*, the record in *Doe IV* failed to support the conclusion that the government "knew to any degree of particularity what, if anything, was hidden behind the encrypted wall."[178]

---

[170] *Id.* at 1237.

[171] *Id.*

[172] *Id.*

[173] *Doe IV*, 670 F.3d at 1349.

[174] *Id.*

[175] *Id.* at 1346–47.

[176] *Id.* at 1346.

[177] *Id.*

[178] *Id.* at 1349.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

Thus, because the government did not know what was on the drive or whether he was capable of accessing it, the foregone conclusion doctrine did not apply.[179]

Therefore, even though compulsion to reveal a password is protected because it reveals the contents of one's mind,[180] cases that involve passwords almost always relate to physical evidence such as computers and/or hard drives. The government cannot compel a defendant to disclose a password to decrypt the physical device. However, if the government can prove that it either has reason to know what is on the device, like in *Boucher*, or that the defendant is the only person capable of decrypting it, like in *Fricosu*, then the foregone conclusion doctrine will apply. In those cases, even though the government is not accessing one's mind, they are forcing the person to provide a decrypted device. Therefore the distinction between the two is a distinction without a difference. If a defendant will not produce the decrypted device, the court is well within its rights to hold the defendant in contempt.[181] Thus, the foregone conclusion doctrine is a limited solution for the government regarding compulsion of encrypted devices because it will only apply if the aforementioned conditions are met.

III. POSSIBLE ALTERNATIVES TO DEAL WITH PROTECTED PASSWORDS

As noted above, in situations where the government has a reason to know what the contents of a decrypted device contain or it can prove that a particular defendant is the only person that can decrypt the device, then the defendant will not be able to invoke his or her Fifth Amendment privilege against self-incrimination. The government will simply bypass the password request and use the foregone conclusion doctrine to enforce production of a decrypted version of the password protected drive. As a result, when analyzing different alternatives that deal with the protected password dilemma, this Note generally assumes that the government is not able to use the foregone conclusion doctrine as an exception to the Fifth Amendment privilege against self-incrimination.

The following section analyzes different solutions to the password problem, including: (A) how allowing production immunity may be a viable solution in certain situations; (B) how issuing a contempt order on a defendant for life until they reveal their password is an impractical and unrealistic solution; (C) creating a

[179] *Id.*

[180] *See* United States v. Hubbell, 530 U.S. 27, 31 (2000).

[181] *See* 18 U.S.C. § 401 (2012) ("A court of the United States shall have power to punish by fine or imprisonment, or both at its discretion, such as contempt of its authority, and none other, as—. . . (3) Disobedience or resistance to its lawful writ, process, order, rule, decree, or commend.").

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

backdoor access point for encryption technologies would prove fruitless; and (D) a legislative solution could prove to be the only viable non-judicial solution.

A. Act-of-Production Immunity: Limited Applicability

Under 18 U.S.C § 6002 Congress provided the government a way to compel the disclosure of evidence from a witness that would otherwise be protected from compelled disclosure under the Fifth Amendment.[182] If a prosecutor grants a defendant production immunity under § 6002 in exchange for the defendant's computer password, will the subsequent evidence uncovered after the decryption of the computer be covered within the "derivative" scope of the immunity granted the defendant?

In *Kastigar v. United States* the Supreme Court dealt with the scope of the production immunity clause.[183] Justice Powell delivered the opinion of the Court, stating, "[i]n a subsequent prosecution, the prosecution has the burden of proving affirmatively that evidence proposed to be used is derived from a legitimate source wholly *independent* of the compelled testimony."[184] Justice Powell reinforced the position that the immunity clause is "consonant with Fifth Amendment standards" and that any information "directly or indirectly derived from such testimony" under such a "grant of immunity must be afforded protection commensurate with that afforded by the privilege, [and] need not be broader."[185] The Court was clear that a prosecutor could not give production immunity to a defendant and subsequently claim that the "derivative" information stemming from the information produced in exchange for immunity was not covered.[186] Additionally, it was the prosecution's burden to prove that the evidence proposed to be used against a defendant did not derive from evidence initially covered by the act-of-production immunity clause.[187]

---

[182] 18 U.S.C. § 6002 (2012) ("Whenever a witness refuses, on the basis of his privilege against self-incrimination, to testify or provide other information in a proceeding . . . no testimony or other information compelled under the order may be used against the witness in any criminal case, except a prosecution for perjury, giving a false statement, or otherwise failing to comply with the order.").

[183] Kastigar v. United States, 406 U.S. 441 (1972).

[184] *Id.* at 441.

[185] *Id.* at 453.

[186] *Id.*

[187] *Id.* at 441.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

A crafty prosecutor in *Doe IV* tested the application and scope of the term "derivative" evidence.[188] The prosecutor tried to avoid the potential Fifth Amendment issues that would arise if the state compelled the defendant to provide his password to his computer drive by offering the defendant limited production immunity in exchange for his password.[189] Doe refused to provide his password because he was afraid that the evidence uncovered by the state after using his password to decrypt his drive would fall outside of the "derivative" scope of the immunity granted.[190] His concern was valid. The prosecution argued that the Doe should have accepted the immunity since it protected him from the use of the password and the decryption; however, Doe feared that it would not extend to the contents underneath the encryption, a distinction the prosecutor was trying to make regarding the scope of "immunity" which he was granting to Doe.[191]

The Eleventh Circuit concluded that the prosecutor was wrong in assuming that the act-of-production label only extended to the password and the decryption.[192] In analyzing whether evidence should be within the scope of the immunity, the court should ask "what conduct was actually immunized and what use would the Government make of the evidence derived from such a conduct in a future prosecution?"[193] In referencing *Kastigar*, the court further reasoned that the government "cannot obtain immunity only for the act of production and then seek to introduce contents of the production, regardless of whether those contents are characterized as nontestimonial evidence, because doing so would allow the use of evidence derived from an original testimonial statement."[194] Consequently, the prosecutor could not compel Doe to disclose his password because the limited act-of-production immunity did not offer Doe proper immunity to justify relinquishing his Fifth Amendment privilege against self-incrimination.[195]

Therefore, assuming that the foregone conclusion doctrine does not apply, a prosecutor could get around Fifth Amendment privilege issues and compel a

---

[188] *See Doe IV*, 670 F.3d at 1338 (stating the U.S. attorney wanted to grant Doe immunity for his password but wanted to limit its use to the password and the decryption, not the contents that were later discovered).

[189] *Id.*

[190] *Id.*

[191] *Id.* at 1350.

[192] *Id.*

[193] *Id.*

[194] *See id.* at 1351.

[195] *Doe IV*, 670 F.3d at 1352.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

defendant to reveal his or her password to an encrypted drive by offering the defendant full act-of-production immunity. One might ask why the prosecutor would do this? Furthermore, why would the prosecutor give the defendant a get out of jail free card, assuming the evidence uncovered from the decrypted drive contains incriminating evidence? The answer is found in the old idiom, "a bird in the hand is worth two in the bush."[196] If the defendant is a small player in a larger criminal conspiracy, and the evidence uncovered by granting password immunity to the defendant is worthwhile, then there may be reason to grant production immunity to the defendant. The alternative could result in losing both the greater criminal enterprise and the defendant, which without the decrypted drives would lead to a dropped case due to lack of evidence. A prosecutor might rather get the bigger player based on the decrypted evidence uncovered, instead of losing both birds in the bush. Therefore, in instances where the state is trying to build a greater case than the case brought against the defendant with the encrypted evidence, the act-of-production immunity available under § 6002 could be a useful prosecutorial tool.

B. Contempt Until You Comply: A Controversial Solution

The authority that a judge has to hold a defendant in contempt of court for failing to follow a decree or command is codified in 18 U.S.C. § 401.[197] This authority includes the power to imprison a defendant for any misbehavior that may "obstruct the administration of justice."[198] In *Gompers v. Buck's Stove & Range Co.*, Justice Lamar for the Supreme Court stated that "the power of the courts to punish for contempt as is necessary and [an] integral part of the independence of the judiciary, and is absolutely essential to the performance of the duties imposed by law."[199] When a defendant violates a court order there are two separate wrongs that he or she is perpetrating.[200] The first violation is the thwarting of the lawful processes of the court, and is addressed punitively under the notion of criminal

---

[196] This idiom originated from ancient sage Ahikar and was articulated in his proverbs 49; *see* Sebastian Brock, *The Proverbs of the Aramean Ahikar (700 B.C.)*, THE ARAMEAN DEMOCRATIC ORGANIZATION (Mar. 10, 2013, 9:20 AM), http://www.aramaic-dem.org/English/History/The%20 proverbs%20of%20the%20Aramean%20Ahikar.pdf ("a sparrow in thy hand is better than a thousand sparrows flying . . . and a living fox is better than a dead lion").

[197] 18 U.S.C. § 401 (2012).

[198] *Id.*

[199] Gompers v. Buck's Stove & Range Co., 221 U.S. 418, 450 (1911). *See also* Mitchell J. Frank, *Modern Odysseus Or Classic Fraud—Fourteen Years In Prison For Civil Contempt Without A Jury Trial, Judicial Power Without Limitation, And An Examination Of The Failure Of Due Process*, 66 U. MIAMI L. REV. 599, 600 (2012).

[200] Robert H. Whorf, *The Boundaries of Contempt: Must the Courts Power Yield to Due Process?*, 46 MAY R.I. B.J. 9, 11 (1998).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

contempt.[201] The second wrong is that the defendant's conduct damages the "party for whose benefit the court order exists."[202] This wrong is referred to as a civil contempt sanction, and it is "intended to provide a remedy for the party whose interests are impaired by the non-compliance."[203]

The main hallmark of civil coercive contempt is that it is designed to force "a reluctant defendant to comply with a court order."[204] The defendant can cure the contempt order by having the ability to "purge" the order, which simply means to do what the judge is asking them to do.[205] However, because the purpose is to assist the plaintiff in obtaining enforcement of a court order, it is considered civil in nature rather than criminal.[206] Since coercive contempt is "imposed as an adjunct to an action in equity" and equitable procedures are followed, no jury trial is available to the defendant.[207] Thus, because the contemnor has the ability to purge the order at any time, a contemnor "facing civil sanction is entitled to far less due process than one facing an ordinary criminal contempt sentence."[208] After all, the defendant is said to have the "keys to their prison in their own pockets."[209]

This lower level of rights afforded to defendants who are thrown in jail for civil contempt, as opposed to criminal, contempt is very troubling. Justice Blackmun in *United Mine Workers of America v. Bagwell* stated that, "[c]ivil contempt proceedings leave the offended judge solely responsible for identifying, prosecuting, adjudicating, and sanctioning the contumacious conduct."[210] And the "contempt power uniquely is 'liable to abuse.'"[211] Justice Blackmun's concern is that defendants will not be afforded due process when they are held in civil contempt, and that only judges will be the sole arbiter of their rights instead of

[201] *Id.* at 10.

[202] *Id.*

[203] *Id.*

[204] Margit Livingston, *Disobedience and Contempt*, 75 WASH. L. REV. 345, 352 (2000).

[205] *See* Whorf, *supra* note 200, at 11.

[206] *See* Livingston, *supra* note 204, at 353.

[207] *Id.*

[208] *See* Whorf, *supra* note 200, at 11.

[209] *In re* Nevitt, 117 F. 448, 461 (8th Cir. 1902).

[210] United Mine Workers of America v. Bagwell, 512 U.S. 821, 831 (1994).

[211] *Id.* (citing Bloom v. Illinois, 391 U.S. 194, 202 (1968)).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

juries.[212] The Supreme Court has remained silent regarding how long a judge can keep a defendant in jail solely based on coercive contempt.[213]

The Court has come up with two approaches regarding how long a defendant who is detained due to a civil contempt order may be incarcerated.[214] The first approach was articulated by the Supreme Court in *Maggio v. Zeitz*.[215] The Court articulated that a contemnor's "denial of possession is given credit after demonstrat[ing] that a period in prison does not produce the goods."[216] This created a rationale, although not a rule articulated by the Court specifically, that a defendant should be held in contempt only if keeping him there would have a coercive effect.[217] The second approach was formulated in *Bagwell*, and stated that unless a defendant complied with the civil contempt order he could face indefinite confinement without any jury trial.[218] Furthermore, the burden of proof rested on the defendant to prove impossible compliance with the order.[219] These two different standards have created very different results. When did the order lose its coercive effect, and therefore make the order feel more like a criminal contempt order where defendants are afforded their due process rights?[220] Additionally, how can the defendant ever prove impossible compliance with an order, and thwart off indefinite confinement if their incarceration makes it impossible to prove an inability to comply? This is especially true if the civil contempt order is to reveal a password or produce a decrypted drive to the state, since the detainee might have been in prison for a long period of time and may have genuinely forgotten the password. This would make compliance impossible, and possibly under *Bagwell* lead to indefinite confinement without due process.

---

[212] *Id.*

[213] Frank, *supra* note 199, at 634–35.

[214] *See id.* at 631 (comparing the two Supreme Court standards articulated regarding coercive civil contempt jail durations a defendant might be subject to).

[215] Maggio v. Zeitz, 333 U.S. 56 (1948).

[216] *Id.* at 76.

[217] *See* Marlene DiGiacomo, *Judge Finally Sets Former Lawyer Free After 14 Years*, DELAWARE COUNTY DAILY TIMES (July 11, 2009), http://www.delcotimes.com/articles/2009/07/11/news/doc4a57fea1b39ed606977003.prt (the judge for the defendant's final successful appeal after a fourteen yearlong jailing due to civil contempt, commented that in order to be lawful, the petitioner's confinement for civil contempt of court must have a coercive effect).

[218] United Mine Workers of America v. Bagwell, 512 U.S. 821, 827 (1994).

[219] *See* United States v. Rylander, 460 U.S. 752, 757 (1983).

[220] *See* Whorf, *supra* note 200, at 10 (stating that since "criminal contempt is a crime in the ordinary sense . . . [t]herefore carries with it the full panoply of due process rights to which the criminally accused are normally entitled" (footnote omitted)).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

On April 5, 1995, H. Beatty Chadwick was arrested for civil contempt in connection with his divorce proceedings.[221] Fourteen years later, on July 10, 2009 he was released from prison.[222] He was suspected of embezzling $2.5 million in order to conceal the money from his ex-wife.[223] However, Chadwick contended that the money went toward bad investments.[224] He continued appealing the case, claiming that there should be limits of imprisonment for contempt.[225] He urged the judges to acknowledge that the confinement lost its coercive effect, and therefore he should be released from prison.[226] It ultimately took numerous appeals and fourteen years for his release to occur.[227]

What is so troubling about the lack of due process afforded to "civil" contempt confinements is the comparison Professor Frank makes regarding how long Chadwick was imprisoned, compared to other types of criminal penalties given out for various criminal convictions.[228] Murder in the third degree, is punishable by as little as six years in prison.[229] A defendant convicted of robbery with a serious bodily injury is subject to a recommended sentence of a minimum of six years in prison.[230] Had Chadwick simply stolen the money from Mrs. Chadwick, he would have been guilty of theft, which is punishable by up to seven years in prison.[231] The conclusion is that the lack of due process in coercive contempt cases can subject a defendant to greater punitive harm than if the defendant would have pleaded guilty to the alleged embezzlement.

In criminal cases where the state seeks to compel disclosure of the defendant's computer password, and the foregone conclusion doctrine does not apply, the defendant will not have to worry about the court issuing an order to compel disclosure.[232] As *Doe IV* illustrates, the Eleventh Circuit held that the Fifth

---

[221] Frank, *supra* note 199, at 600.

[222] *Id.*

[223] *Id.* at 603.

[224] *Id.* at 605.

[225] *Id.* at 632.

[226] *Id.* at 630.

[227] DiGiacomo, *supra* note 217.

[228] *See* Frank, *supra* note 199, at 628.

[229] *Id.*

[230] *Id.*

[231] *Id.* at 629.

[232] *Doe IV*, 670 F.3d at 1353.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

Amendment's privilege against self-incrimination protects defendants from revealing the contents of their minds.[233] But what about situations where the judge could grant an order of civil contempt if the defendant does not produce the decrypted information that he or she is compelled to produce? This situation arises when the foregone conclusion doctrine forces the defendant, not to disclose a password, but to produce an already decrypted device.

In *Fricosu*, the defendant received production immunity for her decrypted drive, and therefore provided it to the state.[234] But what if she was not receiving immunity from the prosecutor for the unencrypted drive, and she refused to produce it after the court ordered her to? Would the court then keep her in prison until she complied? The court in every subsequent appeal by Fricosu would have to decide whether to apply the *Bagwell* (indefinite confinement) standard or the *Maggio* (confinement until no coercive effect exists) standard.[235] In the *Chadwick* case, the court did not believe that he sincerely relinquished the money to pay a debt.[236] The court undoubtedly reasoned that he knew where it was hidden. However, unlike Mr. Chadwick, Ms. Fricosu is asked to use a password that is stored in her mind to decrypt her hard drive. Ms. Fricosu could forget the password, as humans are often times forgetful; Mr. Chadwick, however, had assets that were liquidated, and hidden in a place that probably would not fade in Chadwick's memory over time. The longer Ms. Fricosu is in prison under the *Bagwell* line of reasoning the greater the possibility that she will forget the password. Therefore, if she genuinely loses the ability to decrypt the hard drive, how can she still be punished for having to comply with a "civil order" that she will never be able to comply with?

The New Jersey Supreme Court in *Cantena v. Seidl*, stated that it was

> abhorrent to [the court's] concept of personal freedom that the process of civil contempt can be used to jail a person indefinitely, possibly for life, even though he or she refuses to comply with the court's order . . . . The legal justification for commitment for civil contempt is to secure compliance. Once it appears that the commitment has lost its coercive power, the legal

[233] *Id.* at 1346.

[234] *Fricosu*, 841 F. Supp. 2d at 1238.

[235] *See* Part III B *supra* discussing *Bagwell* and *Maggio*.

[236] Chadwick v. Janeka, 312 F.3d 597, 600 (3d Cir. 2002).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

> justification for it ends and further confinement cannot be tolerated."[237]

Thus, issuing coercive contempt orders for cases that involve encrypted evidence that falls under the ambit of the foregone conclusion doctrine is technically a feasible option. However, it is a very controversial practice because there is a possibility for judges to abuse their power like in Chadwick's case. Under this practice, defendants could be imprisoned for an indefinite or excessive period of time without due process.[238] Accordingly, coercive contempt is not the best solution in situations where the defendant fails to follow a judge's directive to produce certain evidence.

A legislative directive, as discussed in section D is a better approach. As Professor Frank articulated the point at issue:

> [W]hether Chadwick was a modern Odysseus of a classic fraud, the judicial system failed him. . . . The substantial likelihood that he was very far from blameless does not change the fact that he was entitled to the benefits of the due process clause. No legal authority need be cited for the proposition that even those who commit the most heinous crimes will be provided such protection.[239]

C. Compelling "Backdoor" Access Would Prove Fruitless

Picture the scenario where a defendant has numerous encrypted hard drives that the prosecutor needs to access in order to make her case. What if the prosecutor did not have to deal with the defendant's Fifth Amendment right to stay silent, or the burden of proving to a judge that the foregone conclusion doctrine would entitle her under a possible contempt order to a decrypted version of the hard drives? This would be ideal because the prosecutor could make her case in a more efficient and less cumbersome manner. Why not just have a "backdoor" entrance to the encryption programs currently used that would not require obtaining the password to the drives from the defendant? This would be ideal, however, there are

---

[237] Cantena v. Seidl, 321 A.2d 225, 228 (N.J. 1974).

[238] *See* U.S. CONST. amend XIV, § 1 (due process of law is afforded every individual under the following section of the Fourteenth Amendment; "nor shall any state deprive any person of life, liberty, or property, without due process of law").

[239] Frank, *supra* note 199, at 646.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

serious problems that arise with this type of conduct. They include incorporating backdoor entrances while obtaining encryption provider consent, possible Fourth Amendment constitutional violations, and alternative encryption technologies that could operate outside the U.S. and contain "unbackdoorable" code.

Microsoft has stated publicly that it does not plan to include any backdoors for BitLocker.[240] TrueCrypt, the encryption software used by the defendant in *Doe IV*, has similarly denied the existence of a "backdoor" to its multi-platform encryption utility.[241] This reluctance by mainstream encryption providers suggests that they will not incorporate "backdoors" into their software without legislative directive.

The next concern with using "backdoors" to avoid the problem raised by the compelled disclosure of a computer password involves privacy concerns. These concerns are likely based on the assumption that the FBI or the National Security Agency (N.S.A.) could create "backdoors" even without the permission or help of current encryption technologies. Thus, the issue becomes whether an encryption user expects their privacy interests to be protected from unreasonable search and seizures that an unauthorized "backdoor" might cause.

In *Katz v. United States*, Justice Stewart, writing for the Supreme Court, inferred that the Fourth Amendment protects people using public mediums in a private manner.[242] By this he meant that the Constitution protects places where society would expect a person's privacy to be protected.[243] The defendant in *Katz* made a phone call from a phone booth, which the Court deemed to be an area protected by the Fourth Amendment, because although it was a public space, Katz was using the booth in a private manner.[244] Despite this ruling, the test that the Supreme Court has applied since *Katz* to decide Fourth Amendment privacy issues comes from Justice Harlan's concurrence in *Katz*.[245] Justice Harlan declared that an

---

[240] *See* Part III B *supra* discussing encryption software. *See also* Evers, *supra* note 54 (stating that Niels Fergusson, a developer and cryptographer at Microsoft, indicated that the suggestion that Microsoft is working with governments to create a "backdoor" so that they can always access BitLocker encrypted data is simply not true, and would happen "over his dead body").

[241] *See Doe IV*, 670 F.3d at 1340; *see also Frequently Asked Questions*, TRUECRYPT.ORG, http://www.truecrypt.org/faq (last visited Mar. 3, 2013).

[242] Katz v. United States, 389 U.S. 347, 351 (1967).

[243] *See id.* at 352 (explaining that when a medium like a public telephone has become adopted by society for private communication, then the public telephone would become a type of medium that is protected by the Fourth Amendment).

[244] *See id.* at 351.

[245] *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 740 (1979) (stating that "[c]onsistently with Katz, this Court uniformly has held that the application of the Fourth Amendment depends on whether the

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

individual's Fourth Amendment right to privacy is based on a twofold requirement.[246] First, the person must have "exhibited an actual (subjective) expectation of privacy and, second[,] the expectation [must] be one that society is prepared to recognize as 'reasonable.'"[247]

We do not know if accessing data that is purposely encrypted by its users is a place that the Fourth Amendment protects against unlawful searches and seizures, because the Supreme Court has not directly decided that issue. However, is encryption technology that is meant to keep files and data protected an area where a user would have a reasonable expectation of privacy? I would argue that it is considered an area where people expect privacy. The Court in *Katz*, was willing to let a place which is normally a public area with no expectation of privacy fall within the ambit of Fourth Amendment protection solely because it was used by a person in a private manner.[248] Thus, wouldn't a person's use of technology that is meant to protect and keep data private not obviously fall under the *Katz* line of thinking? It is clear that many computer users that use privately-owned computers only purchase and use encryption software to ensure their data remains private. If any place would fall under an area protected from government intrusion, it would be a user's encrypted data. The "backdoor" employed by the FBI or NSA would be analogous to the wiretap left in the phone booth in *Katz*, and therefore should be protected under *Katz*.

In order for the government to challenge *Katz* as being dispositive, it would probably contend that a "backdoor" is not an intrusive invasion of a defendant's privacy. This argument would be based on *Schmerber v. California*, which held that physical intrusions such as blood testing involved minimal intrusions that are widely accepted by society as procedures that do not unreasonably infringe on personal privacy.[249] This argument is not persuasive since society has not accepted computer "backdoors" as a minimally accepted physical intrusion of privacy. Additionally, the blood test as used by police would reveal very limited information as opposed to a "backdoor" entrance of an encrypted computer, which could reveal a tremendous amount of information that the user expects to be private. Thus, the two intrusions are not analogous, and the government would probably lose the society based minimally intrusive argument.

---

person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action").

[246] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[247] *Id.*

[248] *See id.* at 351.

[249] Schmerber v. California, 384 U.S. 757, 757 (1966).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

However, assuming *arguendo*, it was legal for the government to create their own "backdoors" in encryption software, and computer users did not have a reasonable expectation of privacy when using those programs, the question remains: would these government created "backdoors" be effective in collecting incriminating evidence? The answer to that question lies in the fact that in today's globalized world, software and encryption technologies spread quickly across the world via the Internet at an alarming speed.[250]

In 2000, then President Bill Clinton, mainly drawing from a legislative proposal called the Security Freedom Through Encryption Act (SAFE), *inter alia* lifted bans that had precluded American companies from competing in the international market for strong encryption products.[251] The move allowed virtually any data encryption program sold in the U.S. market to be sold overseas, pending a one-time review by the U.S. Department of Commerce.[252] More importantly the government would allow, without a license, the encryption programs' source code to be exported.[253] The technology overwhelmed the government's ability to control a majority of these products, including some that could be downloaded for free off the Internet.[254]

Therein lay the answer to the question of whether "backdoors" created by the government would be an effective tool to get encrypted data from uncooperative defendants. They would not be effective in the long run because encryption technologies are massively shared, openly sold throughout the world, and as soon as it is known that the government had a "backdoor" on an encryption technology, a new encryption technology that was "unbackdoorable" would be created by the encryption software company. And, because U.S. companies have been sharing current and new encryption technologies freely since 2000, the government would not be able to compel a U.S. company to stop creating programs that would not allow for "backdoors." The company could simply say that it did not create the program, and some competing internationally based encryption developer would advertise "unbackdoorable" software products. The "aphorism that national borders

---

[250] Adam C. Bonin, Comment, *Protecting Protection: First and Fifth Amendment Challenges to Cryptography Regulation*, U. CHI. LEGAL F. 495, 502 (1996).

[251] Teddy Kang, *Cryptography*, BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY (last visited Mar. 13, 2013), http://cyber.law.harvard.edu/privacy/Encryption%20Description.html.

[252] David E. Sanger & Jeri Clausing, *U.S. Removes More Limits on Encryption*, N.Y. TIMES (Jan. 13, 2000), http://www.nytimes.com/2000/01/13/business/us-removes-more-limits-on-encryption.html.

[253] *Id.*

[254] *Id.*

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

have been speed bumps on the information superhighway seems true; once in cyberspace, encryption technology spreads uncontrollably."[255] Therefore, even if the hypothetical where the government created its own "backdoors" were true, due to commercial competition and an inability to control companies producing technologies via the Internet, "backdoors" would be an ineffective way for prosecutors to get encrypted data from savvy defendants.

D. Legislative Directive from Congress, a Viable Solution

The final alternative that this Note analyzes is legislative action by Congress. Can Congress enact a law that violates an individual's Fifth Amendment right against self-incrimination? The analysis hinges on the type of right potentially being violated (fundamental or not), and if the Supreme Court agrees with the government's reason for doing so.[256]

1. Privilege Against Self-Incrimination Is a Fundamental Right

By the end of the 17th century, the privilege against self-incrimination was firmly established in the American colonies.[257] Throughout the colonies, the general principle that individuals should not be compelled to produce evidence against themselves emerged as a fundamental right.[258] After the Revolutionary War, colonial leaders drafted constitutions to ensure the protection of fundamental rights, many of which included the privilege against self-incrimination.[259] Later, when the Bill of Rights became necessary to allay the concerns that the new federal government would be too powerful, the colonial leaders said that without a privilege against self-incrimination they could not ensure the protection of individuals from the "evils that lurked in the shadows of a new and untried sovereignty."[260] The privilege against self-incrimination was subsequently adopted in the Bill of Rights within the text of the Fifth Amendment.[261] The Supreme Court has recognized the importance of a defendant's Fifth Amendment right against self-

---

[255] Bonin, *supra* note 250, at 503.

[256] *See* ERWIN CHEMERINSKY ET AL., CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 814–17 (4th ed. 2011).

[257] *See, e.g.*, LEONARD LEVY, ORIGINS OF THE FIFTH AMENDMENT 97 (1968).

[258] *Id.* at 332–404.

[259] O. JOHN ROGGE, THE FIRST & THE FIFTH 184–85 (1960) (stating Virginia, Pennsylvania, Maryland, North Carolina, Vermont, Massachusetts, and New Hampshire included self-incrimination clauses in their state constitutions or bill of rights).

[260] R. Carter Pittman, *The Colonial and Constitutional History of the Privilege Against Self-Incrimination in America*, 21 VA. L. REV. 763 (1935).

[261] U.S. CONST. amend. V ("nor shall be compelled in any criminal case to be witness against himself . . .").

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

incrimination. In 1973, the Court in *Roe v. Wade* found that the rights explicitly found in the Bill of Rights were fundamental constitutional rights.[262] The Court again in *United States v. Verdugo-Urquidez* held the right against self-incrimination to be fundamental.[263]

2. Fundamental Rights Are Afforded Strict-Scrutiny

When Congress creates a law that is challenged as infringing upon a fundamental right, the standard that the judiciary reviews that law under is classified as strict-scrutiny.[264] The notion of different levels of judicial review depending on the rights the Court was analyzing came from a now famous footnote found in *United States v. Carolene Products Co.*[265] The strict scrutiny standard affords the least deference to lawmakers and is the most intensive form of review.[266] Under strict scrutiny, a law will be upheld if it meets the following three conditions: (1) the law is necessary to achieve a compelling government purpose, and it is necessary as a means to accomplishing an end; (2) it is the least restrictive or least discriminatory alternative; and (3) the law must be narrowly tailored to achieve that goal or interest.[267]

3. National Security/Global War on Terror and Child Protection are Compelling Government Interests

Under strict scrutiny analysis, the government has the burden to show that the law is necessary to accomplish a compelling governmental purpose.[268] Although the Supreme Court never articulated explicit criteria for determining whether a claimed purpose is compelling, the government must persuade the Court that a

---

[262] Roe v. Wade, 410 U.S. 113, 155 (1973).

[263] United States v. Verdugo-Urquidez, 494 U.S. 259, 264 (1990).

[264] *See* CHEMERINSKY ET AL., *supra* note 256, at 812.

[265] United States v. Carolene Products Co., 304 U.S. 144 (1938); *see* CHEMERINKSY ET AL., *supra* note 256, at 640 ("In a famous footnote, the Court would defer to the government and uphold laws so long as they were reasonable. . . . In other words, courts generally would presume that laws are constitutional. However, this deference would be replaced by a 'more searching judicial inquiry' when it is a law that interferes with individual rights, or a law that restricts the ability of the political process to repeal undesirable legislation, or a law that discriminates against a 'discrete and insular' minority").

[266] *See* CHEMERINSKY ET AL., *supra* note 256, at 554.

[267] *Id.*

[268] *Id.*

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

truly vital interest is served by the law in question.[269] The Court has recognized compelling interests in situations involving war-related efforts and child welfare.[270]

Therefore, the first compelling interest for violating an individual's Fifth Amendment privilege against self-incrimination in situations involving the compelled disclosure of a password would likely be a national security interest to combat the "Global War Against Terror."[271] However, can this interest really be considered vital enough that the Supreme Court would allow the violation of a fundamental right?

In 1944, the Supreme Court in *Korematsu v. United States*, a decision that has never been overturned, held constitutional an order by the government to intern all Japanese Americans on the West Coast during World War II because the United States was at war with Japan.[272] Justice Black, writing for the majority, explained that to "cast [Korematsu's] case into outlines of racial prejudice, without reference to the real military dangers which were presented, merely confuses the issue. . . . Congress, reposing its confidences in this time of war in our military leaders—as inevitably it must [be]—determined that they should have the power to do just this."[273] The Court in a six to three decision determined that the possibility of espionage or disloyalty by some combined with the urgency of war created a compelling enough interest to sequester Japanese Americans.[274] As a result, the law passed the strict scrutiny test.[275]

The law and governmental interests at issue in *Korematsu* seem analogous to a law that, in the interest of the "global war against terrorism," seeks to compel a defendant's disclosure of a computer password to retrieve encrypted data. In fact,

---

[269] *Id.* at 817.

[270] *See id.*

[271] *See* Ari Shapiro, *Obama Team Stops Saying "Global War on Terror" But Doesn't Stop Waging It*, NPR (Mar. 11, 2013, 4:38 PM), http://www.npr.org/blogs/itsallpolitics/2013/03/11/174034634/obama-team-stops-saying-global-war-on-terror-but-doesnt-stop-waging-it (stating that George W. Bush after Sept. 11, 2001 argued that the U.S. was fighting a war without a typical battlefield, and that even though President Obama vowed to change the rhetoric that Bush coined the "Global war on terror," Obama is continuing the same type of actions under justified circumstances rhetoric).

[272] Korematsu v. United States, 323 U.S. 214, 223–24 (1944).

[273] *Id.*

[274] *See id.*

[275] *Id.* at 216 (The court found the test to be applied in the Korematsu case was a strict scrutiny standard by declaring "[t]his is not to say that all such restrictions are unconstitutional. It is to say that courts must subject them to the most rigid scrutiny. Pressing public necessity may sometimes justify the existence of such restrictions; racial antagonism never can.").

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

the internment of all Japanese Americans is a far more intrusive, and racist, interest. In the law proposed by this Note, a defendant would not be compelled to disclose her password unless there was probable cause that the defendant was acting in a manner that was against the interests of national security. There would be no interning of a group of people, instead just a way to compel a defendant, who the government has reason to believe might be a terrorist or is aiding a terrorist, to give up valuable national security related information. Otherwise, if the defendant does not cooperate with the government he could face a jury instruction that raises the inference of guilt at trial.[276]

Unlike World War II, the "War on Terror" is a significant daily threat. The world is different that it was in 1944; countries and economies are intertwined in what is known as the "global borderless world."[277] As Dr. John Psarouthakis of the Nyenrode Business University states, "[c]ommunication and information technology do not have nationalities anymore. They flow essentially freely in and out through national borders."[278] Terrorists looking to hurt the United States can easily communicate with other terrorists, through encrypted data technologies that operate globally. Because "backdoor" access to a potential terrorist's encrypted drives is not a realistic option[279] and holding a defendant in contempt for an indefinite duration is against due process rights,[280] how else might the government be able to get encrypted data that might disrupt a terrorist plot?

For example, in August 2004, the British authorities charged eight terrorist operatives with conspiracy to commit murder, and worldwide bombings.[281] This was a global terrorist operation. The United Kingdom plots targeted mass transit

---

[276] *See* John E.D. Larkin, *Compelled Production of Encrypted Data*, 14 VAND. J. ENT. & TECH. L. 253, 276–77 (2012) (Larkin explains how the missing witness instruction is not such a new concept. Today, when evidence or a potential witness is missing due to one parties bad faith, the court may instruct the "jury to draw an inference that the missing evidence or testimony would have been unfavorable."); *see also* Coates v. Johnson & Johnson, 756 F.2d 524, 551 (7th Cir. 1985) ("The prevailing rule is that bad faith destruction of a document relevant to proof of an issue at trial gives rise to a strong inference that production of the document would have been unfavorable to the party responsible for its destruction.").

[277] John Psarouthakis, *The Challenge of Rapid Change in a Borderless World*, THE BUSINESS THINKER (June 9, 2010), http://businessthinker.com/the-challenge-of-rapid-change-in-a-borderless-world/.

[278] *Id.*

[279] *See* Part III C *supra* discussing why this is not a realistic option.

[280] *See* Part III B *supra* discussing why this violates due process rights.

[281] *See Prosecution case against al-Qaeda Briton*, BBC NEWS (June 11, 2006, 2:35 PM), http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/uk_news/6122270.stm [hereinafter al-Qaeda Briton].

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

operations, including Heathrow airport, and the underground rail system.[282] Amongst the eight members indicted, Dhiren Barot, a British citizen of the Muslim faith, was suspected of conducting U.S. based surveillance of potential economic targets for possible attacks.[283] These locations included the International Monetary Fund and World Bank buildings in Washington D.C., the New York Stock Exchange and Citigroup buildings in New York City, and the Prudential building in Newark, New Jersey.[284]

Although Barot was arrested in Britain in August, 2004, the discovery of computer documents in Pakistan led the U.S. to raise the terrorism alert to 'high risk,' for the financial sectors in Washington, New York, and Newark.[285] This foiled plot was truly a global operation with data capture and information exchange having occurred in the United States, Pakistan, and England.[286]

In England, where the eight suspects were tried and convicted, the government employs an "inference of guilt" rule when a defendant refuses to answer a magistrate's inquiries regarding informational requests.[287] Therefore, the suspects' refusal to comply with the order to produce a password for any encrypted data would result in an inference of guilt due to the suspects' failure to comply. Had Barot been arrested in the United States, he could have asserted his right against self-incrimination not to reveal his password. Assuming that the foregone conclusion doctrine did not apply, the courts would be obligated to follow *Hubbell*'s premise that the contents of one's mind is protected from compelled disclosure by the Fifth Amendment's privilege against self-incrimination.[288] The Barot example illustrates how having an inference of guilt if a defendant fails to follow the informational requests by a judge may help serve a very vital interest—the assistance in capturing technologically savvy terrorists. The capturing of technologically savvy criminals that use global means and methods to wreak havoc

---

[282] *Id.*

[283] John Mintz & Kamran Khan, *Britain Charges 8 in Alleged Terror Plot*, THE WASHINGTON POST (Aug. 18, 2004), http://www.washingtonpost.com/wp-dyn/articles/A7913-2004Aug17.html.

[284] al-Qaeda Briton, *supra* note 281.

[285] Mintz & Khan, *supra* note 283.

[286] *See id.*

[287] *See Criminal Justice and Public Order Act 1994*, LEGISLATION.GOV.UK, http://www.legislation.gov.uk/ukpga/1994/33/part/III/crossheading/inferences-from-accuseds-silence (last visited Mar. 14, 2013) (under section 36 of the Criminal Justice and Public Order Act a magistrate is able to relate an inference of guilt to the jury if the defendant fails to give evidence at trial or answer any questions relating to the production of the evidence requested).

[288] United States v. Hubbell, 530 U.S. 27, 43 (2000).

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

on the U.S. as well as worldwide citizens should not be able to hide behind the United States' constitutional privilege against self-incrimination.

The second compelling state interest that the U.S. Attorney General would raise in response to a constitutional challenge against a law that creates an inference of guilt when a defendant refuses to follow a court order that compels disclosure of a password to a legally seized computer, is child welfare. Government research has estimated that approximately 300,000 children are abused every year in the United States.[289] One serious form of child abuse is child pornography. Attorney General Eric Holder Jr. has recognized how serious a problem child pornography has become, and stated the following in a recent conference: "Unfortunately, we've also seen a historic rise in the distribution of child pornography, in the number of images being shared online, and in the level of violence associated with child exploitation and sexual abuse crimes."[290]

The Supreme Court has found that child welfare is a valid compelling state interest even if it might restrict a defendant's fundamental right.[291] In *Zablocki v. Redhail*, the Court allowed Wisconsin to interfere with a defendant's ability to marry unless the defendant paid child support obligations.[292] Wisconsin's compelling state interest was to reduce the number of children that were not provided for by their biological parents and, consequently, the number of children requiring state support. The state's interest in trying to ensure that children are not being financially neglected pales in comparison to the government's interest in protecting children from being victims of child pornography. If the Supreme Court in *Zablocki* found a compelling state interest to protect children from the results of financial neglect, the Court by the same logic should find that a child's protection from sexual abuse and exploitation would be an equally vital interest. In both *Doe IV* and *Kirschner*, the defendants were accused of having child pornography in their encrypted drives, but the prosecution could not make its case due to the defendants' Fifth Amendment protection.[293] However, if a federal law had been in place allowing the fact-finders to infer guilt based on a missing evidence instruction, maybe the defendants would have been convicted.

---

[289] *Child sexual abuse: What parents should know*, AMERICAN PSYCHOLOGICAL ASSOCIATION, http://www.apa.org/pi/families/resources/child-sexual-abuse.aspx (last visited Mar. 14, 2013).

[290] *Child Exploitation & Obscenity Section*, THE UNITED STATES DEPARTMENT OF JUSTICE, http://www.justice.gov/criminal/ceos/subjectareas/childporn.html (last visited Mar. 14, 2013).

[291] Zablocki v. Redhail, 434 U.S. 374, 378 (1978).

[292] CHEMERINSKY ET AL., *supra* note 256, at 820.

[293] *Kirschner*, 823 F. Supp. 2d at 669; *Doe IV*, 670 F.3d at 1346. *See* Part II B *supra* discussing *Doe IV* and *Kirschner*.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

4. The Directive Could Pass the Narrowly Tailored Requirement

Under the strict scrutiny level of review it is not enough that the government is able to show that there is a compelling interest behind the law.[294] When there is an infringement of a fundamental right it is the government's burden to prove that there are no other less restrictive measures than the one that Congress fashioned.[295] This is the second prong of the strict scrutiny form of judicial review. The law proposed by this Note could be designed in a way that makes it the least restrictive way for a prosecutor to get a password to encrypted evidence from a non-cooperating defendant. The least restrictive way in which the state does not have to sacrifice its case against the defendant in order to gain access to the data is to simply allow the judge to give the jury a missing evidence instruction that presumes the data to be incriminating. This way the defendant is still afforded due process and the right to a trial by jury, unlike indefinite civil contempt. It is the least restrictive alternative because it is only an instruction, and provides for a rebuttable presumption that may be overcome by the defendant at trial.

The final prong that the government needs to prove in order for a constitutionally challenged law to pass strict scrutiny is that the law is "narrowly tailored" to further the government's compelling interests.[296] In order for a law to be narrowly tailored and therefore a justifiable means to an end, the law cannot be over or under inclusive.[297] A law is underinclusive "if it does not apply to individuals who are similar to those to whom the law applies."[298] For example, a driving law that excludes those under the age of sixteen from having a drivers' license is somewhat underinclusive because there are younger drivers that have the physical ability and the maturity to be acceptable drivers.[299] A law is overinclusive if it applies to those that the government does not need to include in order to achieve its purpose.[300]

In *Korematsu*, although the majority did not apply inclusivity in order to determine whether the law was narrowly tailored, the law was clearly both under

---

[294] CHEMERINSKY ET AL., *supra* note 256, at 816.

[295] *Id.*

[296] *See* Grutter v. Bollinger, 509 U.S. 306, 326 (2003).

[297] CHEMERINSKY ET AL., *supra* note 256, at 689–90.

[298] *Id.*

[299] *Id.* at 690.

[300] *Id.*

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

and over inclusive.[301] The decision to evacuate Japanese Americans during World War II was overinclusive because most of the Japanese Americans were not spies for the Japanese, and forcing all Japanese to evacuate to the West Coast included innocent Americans.[302] The law was underinclusive if the goal was to isolate those who were a threat to security, since other nationalities who might have posed a danger like German Americans were not evacuated.[303]

Comparing the law in *Korematsu* to a law, which creates a legal mechanism that allows a fact-finder to receive a missing evidence instruction, the latter would not be over-inclusive. Instead of signaling out a group of defendants the law is targeting, the law would apply only to those defendants in which the law has good reason to infer guilt. The law would allow for a judge to issue a missing evidence instruction that would infer the missing data to be incriminating only after the state was able to secure a warrant, subpoena, and the defendant was not willing to comply with the decryption order. Thus, the law will apply equally to all criminal defendants that the state would like to prosecute irrespective of the underlying crime. However, since the missing data instruction will be given only if the state has probable cause to believe that the defendant has committed the underlying crime, the jury instruction would not include defendants who did not do anything wrong. As the warrant requirement to get this instruction must be reviewed by a neutral magistrate, the limiting instruction law would not be over-inclusive.

Critics of a "negative inference" solution to the password compulsion quandary might argue that even if the law would not be over-inclusive as proposed, it is under-inclusive. The crux of this argument lies in the fact that Congress' reason for having this inference, mainly to protect children and national security interests, does not included other potential interests. Computer fraud, wire fraud, and other white collar crimes to name a few, could easily be the underlying criminal activity in a state's case that requires the government to get a defendant's computer password.

However, even if a proposed law is under-inclusive that does not mean it is sure to be invalidated.[304] The question that was answered in *Korematsu* relates to whether the solution is the best fit between the "government's means and its ends" even if the law is over or under inclusive.[305] As previously examined, many of the

[301] *See id.*

[302] *Id.*

[303] *See* CHEMERINSKY ET AL., *supra* note 256, at 690.

[304] *Id.*

[305] *See id.*

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

other possibilities could not accomplish a way around the password problem in a less restrictive fashion. Having a negative inference of guilt would still afford the defendant the ability to rebut the presumption. Also, the negative inference would not be allowed by a judge unless there was probable cause of the crime, and a significant connection established between the defendant and the computer password in question.

Therefore, because this law would be the least restrictive way to enforce the state's compelling interests, and the law could be drafted in a way that is not over-inclusive, the law would pass the narrowly tailored strict-scrutiny prong.

IV. CONCLUSION

Data encryption technologies currently offer cyber thieves, terrorists, and child predators a safe haven for their illegal activities. Currently, a criminal can commit an illegal act and store it on a personal computer using an encryption technology, like TrueCrypt, making the data inaccessible without the criminal's password. The criminal is therefore free to continue with his or her illegal activities because a prosecutor will not be able to charge the criminal without the evidence.

Unless the prosecutor is able to use the foregone conclusion doctrine by proving to the judge that the government has reason to know what is on the encrypted device, the prosecutor is basically out of luck. Compulsion of a computer password is covered by a defendant's Fifth Amendment privilege against self-incrimination.

However, there are some strategies that have been employed or suggested in order to solve the password compulsion problem. Prosecutors may grant a defendant production immunity in order to get the defendant's password, but that strategy would make the evidence uncovered after the password is obtained inadmissible against the defendant. This strategy might be good for a prosecutor who is trying to compel a password from a small fish in a large criminal pond, but barring that scenario, the immunity would be pointless.[306] Another solution to the password problem entails keeping the defendant in coercive civil contempt if the defendant does not provide the password under court order. This solution can lead to long periods of incarceration, infringing on a defendant's due process rights.[307]

At first glance, law enforcement's use of "backdoors" to access the defendant's encrypted data looks like an efficient theoretical solution. However,

[306] *See* Part III A *supra* discussing this solution.

[307] *See* Part III B *supra* discussing this solution.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu

"backdoors" raise Fourth Amendment privacy concerns, and are unrealistic because the major encryption software providers have all refused to entertain such a notion. Because the Supreme Court has not granted certiorari to hear the question of whether the Fifth Amendment privilege against self-incrimination extends to defendant computer passwords, a legislative option might be the only viable solution. A federal law that permits a judge to give a missing evidence instruction after a combination of a warrant and subpoena could not induce a defendant to decrypt his data is a viable solution. Because the law would infringes upon a fundamental right—the Fifth Amendment's right against self-incrimination—the law would have to survive the strict scrutiny test to be constitutional. The government can prove that the law serves a compelling interest because the encrypted data could involve child pornography and terrorist activities, both criminal activities that the state has a vital interest to stop. Such a law would not open a defendant's computer or electronic device, and does not compel the disclosure of incriminating testimony, and therefore would be the least restrictive way to solve the password disclosure problem. Finally, because the inference would be given only after a warrant and probable cause were present, the law is not over-inclusive. It only applies to defendants for which probable cause exists to search their encrypted device in the first place. Accordingly, the law should pass a strict scrutiny level of judicial review.

A law that does not compel a defendant to provide a password, but holds the defendant accountable for criminal activities, will afford justice for the victims, instead of a technological get out of jail free card.

Volume XIV – Fall 2013 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2013.132 ● http://tlp.law.pitt.edu