ARTICLE: Encryption, Forced Decryption, and the Constitution

Summer, 2015

Reporter
11 ISJLP 525 *

Length: 10512 words

Author: TIMOTHY A. WISEMAN *

* Graduate of the William S. Boyd School of Law. Special thanks to Prof. Ian Bartrum, Prof. Peter Shane, Sara Salari, and the staff of I/S for their recommendations.

Text

[*525] I. INTRODUCTION

Encryption and ciphers have been significant in diplomacy, military activities, privacy for individuals, and have allowed for free communications even in areas without free speech. Encryption is necessary for the proper functioning of the Internet, because it allows private and secure transactions and can help ensure the identities of all parties. [1] Authentication through encryption provides a layer of security on the Internet that helps prevent fraud and impersonation. [2] Without encryption, it would be impossible to safely make purchases, carry out banking, or perform most other actions which require confirmation of identity online. [3] Innovative uses of encryption have even allowed the creation of purely digital currencies which can be exchanged in relative anonymity. [4]

But encryption has also allowed illicit communications and materials to remain undetected. It has helped conceal attempts at [*526] fraud, gambling, and loansharking. [5] It has been used to conceal suspected child pornography. [6] It has even been used to build illicit markets which sell drugs and permit the hiring of hit men. [7]

Because of the effectiveness of cryptography at protecting illicit activity, contraband, and evidence, law enforcement and prosecutors have a strong interest in being able to view encrypted documents and information on encrypted devices. [8] In some cases, they are able to do this through investigation and observation of the suspect, and in

---

[1] Peter Bright, *Locking the Bad Guys out with Asymmetric* Encryption, ARSTECHNICA (Feb. 12, 2013), http://arstechnica.com/security/2013/02/lock-robster-keeping-the-bad-guys-out-with-asymmetric-encryption/.

[2] *Id.*

[3] *See Id.*

[4] Robert McMillan & Cade Metz, *Bitcoin Survival Guide: Everything You Need to Know About the Future of Money*, WIRED (Nov. 25, 2013), http://www.wired.com/wiredenterprise/2013/11/bitcoin-survival-guide/.

[5] U. S. v. Scarfo, 180 F.Supp.2d 572, 574-76 (D.N.J. 2001).

[6] U. S. v. Gavegnano, 305 Fed. Appx. 954, 955-56 (4th Cir. 2009).

[7] Cyrus Farivar, *Feds Say Silk Road Suspect's Computer Shows He (Thought He) Plotted 6 Murders*, ARSTECHNICA (Nov. 21, 2013), *available at* http://arstechnica.com/tech-policy /2013/11/feds-say-silk-road-suspects-computer-shows-he-thought-he-plotted-6-murders/.

[8] Certain groups within the law enforcement community have expressed concern with the growing use of encryption, particularly in the context of cell phones. *See e.g*. David Kravets, *Apple, Google Default Cell-Phone* Encryption *'Concerns' FBI Director*,

some cases they may be able to use technological means to overcome the encryption. But there are times when neither of those options will be available and law enforcement will have a strong and legitimate interest in compelling a defendant to decrypt their own files. This is in tension with the protections of the Fifth Amendment, which generally prevent a person from being forced to be a witness against themselves and may provide a shelter from being compelled to produce incriminating evidence to be used against them. [9]

This paper will look when it is appropriate to compel a defendant to decrypt data in their control notwithstanding the protections of the Fifth Amendment. It will review the jurisprudence that exists on the matter so far and then argue for a broad reading of the standards used to determine when decryption can be forced. It will suggest that the foregone conclusion doctrine should be applied broadly when the government has access to the encrypted files already and can show by a preponderance of the evidence that the defendant is capable of decrypting them. It will also examine the complications which steganography and deniable encryption can create for compelling the production of encrypted documents. It will conclude that, while the same standard should apply for standard encryption and for deniable [*527] encryption, those standards may be far harder to meet in practice when deniable encryption is used.

Part II of this paper will provide a background on the history of encryption and the privilege against self-incrimination and briefly touch on how that can affect the Constitutional analysis. Part III will explore the existing jurisprudence and the standards which courts have used in analyzing this question in the few times it has arisen. Part IV will explore analogies that have been used to look at encryption in the legal context and conclude that, while no analogy is perfect, viewing it as a combination locked safe is most appropriate. Part V will make the argument for a broad reading of the existing jurisprudence on compelled decryption that would create a reasonable standard for the prosecution to meet before they may use the power of the courts to compel decryption. Part VI will explore deniable encryption and steganography and the complications beyond standard encryption that they can introduce to this issue. Finally, Part VII will summarize the conclusions.

II. BACKGROUND

A. *Cryptography in History* Cryptography is an ancient art of transforming something with a plain meaning into something whose meaning is hidden until it is transformed or translated back. [10] The word itself is derived from the ancient Greek phrase for "secret writing" and there is evidence that it was used in ancient Egypt nearly four thousand years ago. [11] People have used encryption to keep religious information secret [12], protect military secrets [13], and shelter the communications between political dissidents or others with reasons to want privacy. [14] At times, members of unpopular religious orders have used encryption to hide their secrets and their identities, and because of that there was a [*528] period when a church might view the use of encryption as a reason for suspicion of heresy or witchcraft. [15]

ARSTECHNICA (Sept. 25, 2014), http://arstechnica.com/tech-policy/2014/09/applegoogle-default-cell-phone-encryption-concerns-fbi-director/.

[9] In relevant part, the Fifth Amendment reads "nor shall be compelled in any criminal case to be a witness against himself." U.S. CONST. amend. V.

[10] FRED WRIXON, CODES CIPHERS & OTHER CRYPTIC & CLANDESTINE COMMUNICATION 17 (1998).

[11] *Id.*

[12] *Id.* at 18-19.

[13] *Id.* at 21.

[14] *Id.* at 29.

[15] *Id.* at 24.

There are numerous forms of encryption. The Scytale provides an example of an early tool for encryption which was used around the fifth century B.C. in Sparta. [16] The Scytale was a wooden staff that the Spartans would wind a thin strip of parchment around, and then write their message down the paper. [17] When the parchment was removed from the Scytale, it was difficult to read. [18] The message could be read easily by wrapping the parchment again around the same Scytale or another with the same radius. [19]

Another early and simple form of encryption was used by Julius Caesar during his campaigns and is now frequently called the Caesar Cipher. [20] In the Caesar Cipher, a letter appearing a certain number of steps later in the alphabet replaces each letter. [21] For instance, if the number of steps chosen is three, then every "I" in the message would be replaced by "L". [22] However, ciphers like that are subject to relatively simple letter frequency analysis and can now be broken swiftly. [23] Letter frequency analysis attacks and other forms of early cryptanalysis were developed in the Arab culture during the Abbasid era, when the tax records of wealthy merchants were frequently protected by encryption and use of cryptography was relatively routine. [24]

Codes and cryptography were significant in the American Revolution as well. Spies for the British often sent their reports in codes. In 1775, men loyal to George Washington intercepted an [*529] encrypted report from Dr. Church, acting as a spy, to a British major. [25] The revolutionaries eventually managed to break the substitution cipher used and have Dr. Church arrested for his actions. [26] Similarly, Washington was confronted by the use of encryption in Benedict Arnold's efforts to betray West Point to the British. [27]

The Revolutionaries and the leaders of the young United States also made use of cryptography to protect their communications. Charles Dumas was, for a time, a secret agent for the United States and conducted much of his correspondence with the Continental Congress using a code in order to minimize the risks from postal intercepts. [28] Statesmen such as John Adams, Benjamin Franklin, John Jay, Henry Laurens, and Thomas Jefferson used cryptography with some of their communications during the Revolutionary Era. [29] George Washington used

---

[16] SIMON SINGH, THE CODE BOOK 8 (1999).

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] WRIXON, *supra* note 10, at 170.

[21] *Id.* at 171.

[22] *Id.* at 170-171.

[23] *See Id.* at 31.

[24] SINGH, *supra* note 16, at 15.

[25] RALPH E. WEBER, UNITED STATES: DIPLOMATIC CODES AND CIPHERS 1775-1938 22-23 (1979).

[26] *Id.* at 22-23.

[27] John A. Fraser, *The Use of* Encrypted*, Coded and Secret Communications Is an "Ancient Liberty" Protected by the Constitution*, 2 VA. J. L. & TECH. 2, 22 (1997).

[28] WEBER, *supra* note 25, at 23-25.

[29] *Id.* at 37.

encryption while exchanging letters with the Marquis de Lafayette around 1785. [30] Outside of matters of state, John and Abigail Adams encrypted some of their private correspondence during the Revolutionary Era. [31]

This may have significance beyond the historical curiosity and a demonstration of the importance of cryptography to this country. Some scholars have been concerned that the Constitution contains latent ambiguities. [32] These are issues that were unambiguous at the time they were written, but become ambiguous in other contexts. [33] These ambiguities most often arise because of new situations created [*530] in more modern eras that the framers of the Constitution could not have reasonably considered. [34] But history shows that this situation does not arise in the question of cryptography. At least some of the founders were accustomed to using it. Some, such as Benjamin Franklin and Thomas Jefferson, were quite well versed in the understanding of the cryptography of the day. [35] They were even accustomed to dealing with a spectrum of encryption systems including those where the entire system could be memorized, those that made use of passwords, and those that required a physical object, such as a code book, to decrypt. [36] Although encryption is now more common and sophisticated than it was for the Founders, they were well aware of its existence and its possible implications. They could have considered them during the drafting of the Constitution and its first set of amendments.

The American courts also dealt with ciphers and encryption quite early in their history. During the trial of Aaron Burr for treason, his secretary refused to identify whether Burr had authored an encrypted letter on Fifth Amendment grounds. [37] Aaron Burr had used both a dictionary code and a symbol cipher while communicating with some of his alleged co-conspirators, particularly James Wilkinson, and those communications were used as evidence during his trial. [38] Although the court ordered his secretary to answer the question of authentication for the encrypted documents as that could not itself incriminate the secretary, [39] Burr was eventually acquitted of treason in 1807. [40]

B. *Modern Cryptography*

In the modern era, there are multiple forms and categories of encryption, though almost all are handled primarily through computers. Computers and electronic communications have made [*531] cryptography both easier to use and more significant. It is now frequently used to protect access to sensitive data both in transit [41] and at rest. [42]

---

[30] Fraser, *supra* note 27, at 22.

[31] *Id.*

[32] LAWRENCE LESSIG, CODE VERSION 2.0 25-26 (2006). Prof. Froomkin, although using different terms, expressed a similar idea. He said that "[t]he Bill of Rights is predicated on assumptions about technological limits that may soon be falsified." A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 844 (1995).

[33] LESSIG, *supra* note 32, at 25-26.

[34] *See Id.* at 166.

[35] WEBER, *supra* note 25, at 23-37. *See also* Fraser, *supra* note 27, at 33.

[36] WEBER, *supra* note 25, at 48-50.

[37] U. S. v. Burr, 25 F. Cas. 38 (D.Va. 1807).

[38] WRIXON, *supra* note 10, at 49.

[39] Burr, 25 F. Cas. at 38.

[40] WRIXON, *supra* note 10, at 50.

[41] Network Working Group, *The Transport Layer Security (TLS) Protocol*, IETF (Aug., 2008), http://tools.ietf.org/html/rfc5246 (describing technologies used to provide communications security for electronic communications).

It is also used as a form of authentication to permit the identity of the sender of a message to be verified, to ensure that the message has not been tampered with, and to allow for a form of digital signature. [43] People protect both their traditional computers and modern smartphones and tablets with encryption. [44] It has significance in electronic commerce, and has been used to help dissidents communicate privately in countries where free speech is not deemed to be fundamental right. [45] Cryptography and the breaking of codes have remained vital for military applications. For instance, code breakers played a significant role in the Allies' victory during World War II. [46]

Although most encryption is secured by a password, sometimes other forms of cryptographic keys are used in place of or in addition to passwords. [47] This could take the form of a keyfile whose contents are used as part of the encryption process. [48] The keyfile may be stored [*532] separately from the encrypted document, and even if stored together, the fact that the user must identify the correct keyfile out of all the files on the device can provide security in addition to a password. [49] Alternatively, physical items such as security tokens or security cards may be used. [50]

Most modern forms of encryption are divided by their use of symmetric or asymmetric keys. [51] In symmetric key encryption, the same key is used both to encrypt and decrypt the message. [52] There are a variety of symmetric key encryption systems including ancient ones like the Caesar Cipher [53] and more modern ones like AES [54] or

---

[42] Timothy A. Wiseman, Encrypting *SQL Server Backups with Open Source Tools*, MSSQLTIPS (Jan. 24, 2013), http://www.mssqltips.com/sqlservertip/2861/encrypting-sqlserver-backups-with-open-source-tools/ (discussing the use of encryption to protect database backups).

[43] *The GNU Privacy Handbook: Making and Verifying Signatures*, GNUPG (1999), http://gnupg.org/gph/en/manual/x135.html.

[44] Cyrus Farivar, *Apple Expands Data* Encryption *Under iOS 8, Making Handover to Cops Moot*, ARSTECHNICA (Sept. 17, 2014), http://arstechnica.com/apple/2014/09/appleexpands-data-encryption-under-ios-8-making-handover-to-cops-moot/; Robert Lemos,*Latest Android* Encrypted *by Default, Adds "Smart" Device Locking*, ARSTECHNICA (Oct. 29, 2014), http://arstechnica.com/security/2014/10/latest-android-encrypted-by-defaultadds-smart-device-locking/.

[45] Tor relies on encryption along with sophisticated routing to protect the anonymity of communication made using it and has been used by dissident groups in countries such as Iran. Christopher Williams, *Iran Cracks Down on Web Dissident Technology*, THE TELEGRAPH (Mar. 18, 2011), http://www.telegraph.co.uk/technology/news/8388484/Irancracks-down-on-web-dissident-technology.html.

[46] SINGH, *supra* note 16, at 186-87. The work of Alan Turing and others in breaking the Enigma code was particularly notable in its effects on the war efforts. *Id.*

[47] TRUECRYPT FOUNDATION, TRUECRYPT USER'S Guide 66-69 (2012) [hereinafter TRUECRYPT].

[48] *Id.*

[49] *Id.* It is also possible to use multiple key files, which can be structured so that it requires multiple users for decryption if each user has access to only one of the key files. *Id.*

[50] *Id.*

[51] *Description of Symmetric and Asymmetric* Encryption, MICROSOFT SUPPORT (Oct. 26, 2007), http://support.microsoft.com/kb/246071 [hereinafter*Description*].

[52] *Id.* The key used in the encryption and decryption process is frequently not the password passed in by the user. *See e.g*. TRUECRYPT, *supra* note 47, at 138 (Discussing header key derivation and cryptographic salt). Rather, the password is normally used, possibly along with cryptographic salt, to generate a longer key, which is directly used in the encryption and decryption. *Id.* Though in some cases, even that generated key is used mostly to encrypt an even longer key that is used to encrypt or decrypt the actual contents. *Id.*

[53] *Description*, s*upra* note 51 (shifting each letter of the alphabet by a number of places is a description of the Caesar Cipher).

Twofish. [55] In systems where security is more important than speed, it is common to apply first one and then another symmetric key encryption system in combinations that are often referred to as cascades or multiple-encryption, such as applying AES first and then applying Twofish. [56]

A contrasting category of encryption is called asymmetric encryption, or public key encryption. [57] In asymmetric encryption, two [*533] keys are created, one public and one private. [58] The public key is used to encrypt messages and can be published to the world and distributed widely without compromising the private key. This solves the key distribution problem, which had caused major issues in secure communications before. [59] Meanwhile, the private key is kept secret and is used primarily to decrypt files that are encrypted by the public key. [60] The private key can also be used to generate an electronic signature to authenticate documents through use of the public key. [61]

A prominent algorithm used for public key encryption is called RSA after its designers Ron Rivest, Adi Shamir, and Leonard Adleman. [62] The RSA algorithm currently underlies a substantial amount of the security for Internet communications, both by keeping the exchanged communications private and by ensuring that both sides are able to authenticate the other. [63] Public key encryption is foundational to matters such as online commerce and private communications over a public network like the Internet. [64]

The RSA algorithm relies on the fact that multiplication is computationally easier than division or factoring, particularly when dealing with large integers. [65] Factoring is computationally expensive when dealing with large

---

[54] TRUECYRPT, *supra* note 47, at 75.

[55] *Id.* at 76.

[56] *See Id. See also* Himanshu Gupta & Vinod Sharma, *Multiphase* Encryption*: A New Concept in Modern Cryptography*, 5 INT'L J. COMPUTER THEORY & ENG'G 638, 638 (2013). Cascading encryption is meant to protect against weaknesses in the algorithm. If one algorithm is found to be fundamentally flawed and vulnerable, the other should retain its ability provide protective, even if they are all starting from the same password.

[57] *Description*, s*upra* note 51.

[58] Nick Sullivan, *A (Relatively Easy To Understand) Primer on Elliptic Curve Cryptography*, ARSTECHNICA (Oct. 24, 2013), http://arstechnica.com/security/2013/10/arelatively-easy-to-understand-primer-on-elliptic-curve-cryptography/.

[59] SINGH, *supra* note 16, at 258-259.

[60] Sullivan, *supra* note 58.

[61] *Id. The GNU Privacy Handbook: Making and Verifying Signatures*, GNUPG (1999), http://gnupg.org/gph/en/manual/x135.html.

[62] Peter Bright, *Locking the Bad Guys Out with Asymmetric* Encryption, ARSTECHNICA (Feb. 12, 2013), http://arstechnica.com/security/2013/02/lock-robster-keeping-the-badguys-out-with-asymmetric-encryption/. Though much of the work done by Rivest, Shamir, and Adleman was based on and extended the work done by Whitfield Diffie and Martin Hellman. SINGH,*supra* note 16, at 272-273.

[63] Bright, *supra* note 62.

[64] *Id.*

[65] *Id.*

numbers. [66] However, if a rapid way to factor [*534] large integers were discovered, it is likely that the RSA algorithm would become easy to break in a timely fashion. [67]

Because of that, researchers have continued to develop other mathematical operations, which are easy to perform in one direction, but whose inverse is extremely difficult, often called trapdoor functions. [68] New trapdoor functions can form the basis of other forms of public key cryptography, such as elliptic curve cryptography, which will remain secure even if an efficient method of factoring is discovered. [69] Elliptic curve cryptography relies on solving the discrete logarithm for an elliptic curve. [70] Elliptic curve cryptography is substantially harder than the RSA algorithm to crack by brute force. [71]

Public key cryptography is computationally expensive and slow compared to many forms of symmetric key cryptography. [72] For that reason, public key encryption algorithms are often used only to encrypt another long encryption key. Those randomly generated keys are then used with a symmetric key algorithm, like AES, to encrypt the actual message, and the key used for the symmetric key encryption is then stored or transmitted along with the encrypted contents. [73] This is sometimes referred to as a hybrid cipher. [74]

C. *Gaining Access in Spite of Cryptography*

If someone wants to gain access to encrypted data without the key, they are left with the options of attacking the cryptographic system [*535] directly, [75] attempting to use brute force to discover the key through trial and error, [76] or attempting to acquire the key by other means. Modern encryption systems, when implemented properly, can be impractical to unlock with brute force in any reasonable timeframe, and even more sophisticated attacks may not always be practical. [77] This means as a practical matter that decrypting modern, properly encrypted data often requires obtaining the key. There are a number of ways to acquire the key even if the holder of the key does not

---

[66] Sullivan, *supra* note 58. It has been proven mathematically to be equivalent in difficulty to other computationally intense problems. *Id.*

[67] *Id.*

[68] *Id.*

[69] *Id.*

[70] Describing an elliptic curve with any rigor goes outside the scope of this paper, but briefly it is the solution set to an equation of the form y2 = x3 + ax + b where a and b are held constant and y and x are variables. *Id.*

[71] One group calculated the amount of energy it would require to break elliptic curve encryption using brute force. They determined it would take enough energy to boil all water on earth to break a 228-bit elliptic curve key using currently available algorithms and technology. *Id.*

[72] Bright, *supra* note 62.

[73] *Id.*

[74] *The GNU Privacy Handbook: Hybrid ciphers*, GNUPG (1999), http://gnupg.org/gph/en/manual/x209.html.

[75] This is relatively easy for some systems such as the Caesar Cipher and can be done through a number of techniques such as letter frequency analysis. *See* WRIXON, *supra* note 10, at 31. However, for other systems this is impractical or even theoretically impossible. *See One-Time Pad (OTP): The Unbreakable Code*, CRYPTOMUSEUM.COM (Jan. 29, 2013, 11:05 CET), http://www.cryptomuseum.com/crypto/otp.htm.

[76] Mohit Arora, *How secure is AES against Brute Force Attacks*?, EETIMES (May 7, 2012) http://www.eetimes.com/document.asp?doc_id=1279619.

[77] *See Id.*

intend to reveal it. [78] Social engineering has repeatedly proven itself to be effective in acquiring passwords and other sensitive data. [79]

Law enforcement agencies have also had success acquiring passwords through the use of keylogging software. [80] For instance, while investigating Nicodemo Scarfo on accusations of gambling and loan shark operations, the F.B.I. executed a warrant and found a computer with encrypted files. [81] Later, they, with new search warrants, installed a keylogger on Scarfo's computer. [82] The keylogger [*536] acquired the password to the encrypted file along with much of his other activity on the computer. [83] This enabled the F.B.I. to decrypt the files and acquire useful evidence. [84] Their use of this evidence was upheld by the district judge despite the protestations of Scarfo on Fourth Amendment grounds. [85] Another effective way to acquire the password is to compel the holder of the password to provide it.

D. *History of the Right against Self Incrimination*

There is some scholarly disagreement over precisely when the right not to be compelled to incriminate oneself arose in the British and American Legal Systems. [86] One source of the right came from resistance in England to the oath *ex officio*, which required someone, who was not even informed of what they were being accused, to answer any question put to them by the official. [87] Although there were complaints and arguments against this oath long before, John Lambert may be the first person to object on official record to being forced to take the oath by asserting a right not to incriminate himself in 1532. [88] In 1533, Parliament took action to prohibit the oath *ex*

---

[78] One technique, that is only known to have been used in laboratory by security researchers, involves determining the encryption key used by the sounds emitted by the CPU. Sebastian Anthony, *Researchers Crack the World's Toughest* Encryption *by Listening to the Tiny Sounds Made by Your Computer's CPU*, EXTREMETECH (Dec. 18, 2013), http://www.extremetech.com/extreme/173108-researchers-crack-the-worldstoughest-encryption-by-listening-to-the-tiny-sounds-made-by-your-computers-cpu. Another technique involves measuring the current flowing through certain parts of the computer while it is encrypting or decrypting the data. Peter Bright,*Stealing* Encryption *Keys Through the Power of Touch*, ARSTECHNICA (Aug. 21 2014), http://arstechnica.com/security/2014/08/stealing-encryption-keys-through-the-power-of-touch/.

[79] *See* Sarah Granger, *Social Engineering Fundamentals, Part I: Hacker Tactics*, SYMANTEC (Nov. 3, 2010), http://www.symantec.com/connect/articles/social-engineeringfundamentals-part-i-hacker-tactics.

[80] U. S. v. Scarfo, 180 F.Supp.2d 572, 574-76 (D.N.J. 2001). Keyloggers have also been used by hackers to gain passwords from an unsuspecting user. Jose Pagliery, *2 Million Facebook, Gmail and Twitter Passwords Stolen in Massive Hack*, CNN (Dec. 4, 2013), http://money.cnn.com/2013/12/04/technology/security/passwords-stolen/index.html.

[81] Scarfo, 180 F.Supp.2d at 574.

[82] *Id.*

[83] Id. at 574-76.

[84] Id. at 576.

[85] *Id.*

[86] *See* E.M. Morgan, *The Privilege Against Self-Incrimination*, 34 MINN. L. REV 1 (1949). Professor Wigmore has asserted that the Framers of the Constitution may have been heavily influenced by resistance to inquisitorial system in France as well. R. Carter Pittman, *The Colonial and Constitutional History of the Privilege against Self- Incrimination in America*, 21 VA. L. REV. 763, 764-65 (2014). Professor Langbein has argued that the privilege against self-incrimination did not arise, at least not in a meaningful way, until the right to defense counsel was also thoroughly entrenched. *See generally* John H. Langbein, *The Historical Origins of the Privilege against Self- Incrimination at Common Law*, 92 MICH. L. REV. 1047 (1994).

[87] Morgan, *supra* note 86, at 1; LEONARD W. LEVY, ORIGINS OF THE FIFTH AMENDMENT 46-47 (1968); Pittman, *supra* note 86, at 769.

[88] LEVY, *supra* note 87, at 62.

officio, [89] although it was once again permitted in 1583. [90] While resistance to the oath may have started the process, most of the people [*537] arguing against it focused specifically on it and not on a more general right. [91]

Resistance to the later Star Chamber and its techniques started to solidify the idea that, during trial, a person could not be compelled to answer questions that would directly reveal their guilt. [92] The Star Chamber was the judicial arm of the Privy Council and was authorized to use torture. [93] The plight of John Lilburne [94] helped drive the resistance to the Star Chamber when he was publicly punished for asserting a privilege not to testify against himself and refusing the oath. [95] The general right against self-incrimination in criminal proceedings seems to have been well established in Britain by the 1700s. [96]

In America, the privilege against self-incrimination was also firmly established by the late 1700s. [97] Before the end of the 1700s, seven states had some form of a privilege against self-incrimination written into their fundamental laws. [98] The common law of many of the colonies recognized the privilege before they wrote their constitutions. [99] When the Constitution of the United States was being ratified, several states, starting with Massachusetts, suggested that a privilege against self-incrimination be included as an amendment. [100] These recommendations eventually led to the Fifth Amendment and its protections against self-incrimination and other vital rights.

[*538] Overall, the Fifth Amendment safeguards several values in the American legal system. It prevents torture and other abuses of the accused to extort a confession. [101] It helps to ensure that the American system remains accusatorial rather than inquisitorial. [102] But beyond protection from physical compulsion, it helps protect the accused by preventing the cruel trilemma in which an accused person may be forced to select between perjury,

---

[89] Morgan, *supra* note 86, at 6.

[90] *Id.* at 6-7. Despite Parliament's action, the oath did not fall from use, as illustrated by the trial of Edmund Bonner. Levy, *supra* note 87, at 74.

[91] *See* LEVY, *supra* note 87, at 66.

[92] Morgan, *supra* note 86, at 9.

[93] LEVY, *supra* note 87, at 35. *See also Id.* at 49-51.

[94] The spelling of his name varies. Morgan, *supra* 86, at 9 n.34.

[95] Morgan, *supra* 86, at 9-10; LEVY, *supra* note 87, at 276-77.

[96] Morgan, *supra* note 86 at 12; Michael Dann, *The Fifth Amendment Privilege Against Self-Incrimination: Extorting Physical Evidence from a Suspect*, 43 S. CAL. L. REV. 597, 600 (1970). Despite this, forms of torture were still used to induce someone to make a plea. *See Id.* at 13. The requirement that the accused actually be informed of the option to not answer the questions if they did not assert the right themselves came even later. *Id.* at 18. *See also* LEVY, *supra* note 87 at 375.

[97] *See* Morgan, *supra* note 86 at 22.

[98] LEVY, *supra* note 87, at 409-10. *See* Pittman, *supra* note 86 at 764-65.

[99] Twining v. New Jersey, 211 U.S. 78, 107 (1908).

[100] LEVY, *supra* note 87, at 416, 418-22.

[101] Dann, *supra* note 96 at 602-03. *See also* Pittman, *supra* note 86 at 778-79 (discussing forerunners to the Fifth Amendment in the colonies that specifically banned the use of physical compulsion to extract confessions).

[102] Dann, *supra* note 96 at 602-03.

contempt, or providing evidence against themselves. [103] It provides a protection for the dignity of the accused as well as a degree of protection for an individual's private thoughts from government invasion. [104] Since the adoption of the Fifth Amendment, the precise nuances of the right against self-incrimination have been refined and defined by the courts in response to changes in both society and technology. Recently, the courts have been confronted with the question of precisely when the prosecution can demand decryption of potential evidence with some courts forbidding it on Fifth Amendment grounds while others have permitted it. [105]

III. COURTS WHICH HAVE CONSIDERED FORCED DECRYPTION

A. *Courts Rejecting Forced Decryption*

The Fifth Amendment provides protection against defendants being forced to incriminate or otherwise testify against themselves. [106] It reads, in part, "[n]o person … shall be compelled in any criminal case to be a witness against himself." [107] Courts that have considered [*539] whether an individual can be compelled to decrypt have generally found that forced decryption can implicate the Fifth Amendment. [108] In 2012, the Eleventh Circuit upheld a man's right under the Fifth Amendment to refuse to decrypt his hard drives. [109] In that case, law enforcement seized an array of digital media from a hotel room during a child pornography investigation. [110] Despite forensic examination, the FBI was unable to access some of the media due to encryption. [111] The grand jury issued a subpoena for the unencrypted contents of the digital media, but the accused refused to provide the data, claiming that it would violate his rights under the Fifth Amendment. [112] The accused continued to refuse to decrypt the drives even after the district court agreed to grant him limited act-of-production immunity. [113] The district court, after a hearing, thus held the accused in contempt and had him incarcerated. [114] He then appealed. [115]

On appeal, the Eleventh Circuit considered whether the Fifth Amendment could protect the accused from being forced to decrypt his hard drives. The Fifth Amendment comes into force when there is compulsion for a testimonial communication or act, which is incriminatory. [116] Here, and in most situations where the question of compelled

---

[103] Akhil R. Amar & Renee B. Lettow, *Fifth Amendment First Principles: The Self- Incrimination clause*, 93 MICH. L. REV. 857, 890 (1995). *See also* Dann, *supra* note 96 at 604.

[104] Dann, *supra* note 96, at 611. *But see* Amar, *supra* note 103, at 901-02 (arguing that reliability of confessions is the main purpose of the Fifth Amendment and that dignitary rights are better protected by other Constitutional limitations).

[105] *See infra* Part III.

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

[107] *Id.*

[108] *See e.g.* In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1341 (11th Cir. 2012); *In re* Boucher, No. 2:06-mj-91, 2007 WL 4246473, at *3 (D. Vt. Nov. 29, 2009).

[109] In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d at 1341. However, the court would have permitted forced decryption if he were granted both use and derivative use immunity. *Id.*

[110] Id. at 1339.

[111] *Id.*

[112] *Id.*

[113] *Id.*

[114] Id. at 1340.

[115] Id. at 1337.

[116] Id. at 1341 (citing U. S. v. Ghidoni, 732 F.2d 814, 816 (11th Cir. 1984)).

decryption would arise, the fact that the act is compelled and incriminatory can be taken for granted. [117] The Eleventh Circuit also found that the production of the files was testimonial. [118]

[*540] In considering the testimonial nature of the decryption, the court found it would "require the use of the contents of Doe's mind and could not be fairly characterized as a physical act" and that it would reveal "his knowledge of the existence and location of potentially incriminating files; of his possession, control and access to the encrypted portions of the drives; and of his capability to decrypt the files." [119] The court stated that it was precisely when an act of production requires the individual to use "the contents of his own mind" to provide a "statement of fact" that it becomes testimonial. [120] The court also decided that this case did not fall into categories that the Supreme Court has previously found to be not testimonial, such as a mere physical act or a production, which would fall under the foregone conclusion doctrine. [121]

The Supreme Court has found repeatedly that mere physical acts are not testimonial and can be compelled to aid in investigations or trials. For instance, the Court has found that a blood sample may be taken without consent. [122] Similarly, accused individuals can be compelled to provide examples of their handwriting for analysis. [123] Significantly, an individual can be compelled to turn over the key to a strongbox. [124] The Eleventh Circuit distinguished the situation [*541] involving encryption from these physical acts by saying that it required the contents of the defendant's mind. [125] Further, it noted that decrypting and producing these contents would "be tantamount to testimony by Doe of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives, and of his capability to decrypt the files." [126] It concluded that this production would be testimonial in nature. [127]

---

[117] *Id.* at 1341.

[118] *Id.* at 1346. Although not mentioned by the Eleventh Circuit here, the finding that a password was testimonial has also been reached by district courts. *See e.g*. U. S. v. Kirschner, 823 F. Supp. 2d 665 (E.D. Mich. 2010). In *Kirschner*, the accused was subpoenaed to testify and provide his passwords to a grand jury. Id. at 666. The court found that the passwords were testimonial and therefore protected by the Fifth Amendment. Id. at 669. Even some courts which have compelled a defendant to decrypt files have generally held that the password itself is testimonial. *See e.g. In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *7 (D. Vt. Feb. 19, 2009). *See also infra* Part III. B; Part IV.

[119] In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012).

[120] Id. at 1345 (citing Curcio v. U. S., 354 U.S. 118 (1957)).

[121] *Id.* at 1345-46.

[122] Schmerber v. California, 384 U.S. 757, 764-65 (1966). In that case, a blood sample was taken from a man who was accused of driving under the influence of liquor despite his objections. Id. at 758-59. The blood sample provided evidence that he was intoxicated and was used at his trial. *Id.* The accused appealed claiming that using the blood sample violated his Fourth, Fifth, Sixth, and Fourteenth Amendment rights. *Id.* Although the court found that using the blood sample did not violate his rights, it said in dicta that other physiological tests may do so. Id. at 764.

[123] Gilbert v. California, 388 U.S. 263, 266-67 (1967) (finding that handwriting was an "identifying physical characteristic," and was not testimonial).

[124] *See* U. S. v. Hubbell, 539 U.S. 27, 43 (2000); Doe v. U. S., 487 U.S. 201, 219 (1988) (Stevens, J., dissenting).

[125] In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012).

[126] *Id.*

[127] *Id.*

Even communications, which are found to be testimonial, can be compelled when the foregone conclusion doctrine applies. [128] The foregone conclusion doctrine applies when the government already knows of the existence of the evidence in question, knows where it is being stored, and can show the authenticity of the documents through means other than the testimony of the accused. [129] The Supreme Court articulated the foregone conclusion doctrine in *Fisher v. United States* in 1976. [130]

In *Fisher*, the Court dealt with two similar cases of taxpayers that received documents from their accountants and then turned those documents over to their attorneys. [131] In each case, the Internal Revenue Service served the attorney with a summons for the documents and the attorney refused to comply based, in part, on the protections provided by the Fifth Amendment for their client. [132] The Court agreed that if the Fifth Amendment shielded the client from producing the papers, then the lawyer could not be compelled to produce them. [133] However, it found that in this case the Fifth Amendment did not protect the papers. [134] The Court noted that here [*542] the government did not intend to rely upon the "truthtelling" of the taxpayer or accused, but merely needed access to the papers. [135] The "existence and locations of the papers are a foregone conclusion" which "adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers." [136] Thus, this was a matter "not of testimony but of surrender". [137] Later, Justice O'Connor would make note of the significance of this ruling saying that *Fisher* "sounded the death-knell for *Boyd"* which had held that private papers could often be protected by the privilege. [138] She also said explicitly in the concurrence that "the Fifth Amendment provides absolutely no protection for the contents of private papers of any kind." [139]

But the Eleventh Circuit distinguished this matter for the subpoena duces tecum from the matters that arose in *Fisher*. The court required that the government show that the "location, existence, and authenticity of the evidence is known with reasonable particularity." [140] However, here the government did not know the contents of the encrypted files, and had not made a sufficient showing that the defendant was able to decrypt the encrypted files. [141] Because of the way the TrueCrypt software used by the accused works, the government could not even prove

---

[128] *Id.*

[129] Id. at 1344.

[130] 425 U.S. 391 (1976).

[131] Id. at 394-95.

[132] Id. at 395.

[133] *Id.* (citing 8 J. WIGMORE, EVIDENCE § 2307, 592 (McNaughton rev. 1961)).

[134] Id. at 411-12.

[135] Id. at 411.

[136] Id. at 411-12.

[137] Id. at 411 (citing In re Harris, 221 U.S. 274, 279 (1911)).

[138] U. S. v. Doe, 465 U.S. 605, 618 (1984) (O'Connor, J., concurring).

[139] *Id.*

[140] In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1344 (11th Cir. 2012). *See also* U. S. v. Ponds, 454 F.3d 313, 320-21 (D.C. Cir. 2006); In re Grand Jury Subpoena, Dated April 18, 2003, 383 F.3d 905, 910 (9th Cir. 2004); In re Grand Jury Subpoena Duces Tecum Dated October 29, 1992, 1 F.3d 87 (2d Cir. 1993).

[141] In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d at 1346.

absolutely that there was actual data contained within the encrypted volumes. [142] Thus, the court found that the foregone conclusion doctrine did not fit in this case even though [*543] the government in a sense already physically possessed the files that it wanted access to. [143]

Finally, the Eleventh Circuit stated that the district court could have compelled decryption if it had offered "constitutionally sufficient immunity" and the government had shown that the accused was actually capable of decrypting the drive. [144] Referring to the landmark case of *Kastigar v. United States*, the Eleventh Circuit noted that to be constitutionally sufficient, the immunity must be "co-extensive with the scope of the privilege." [145]

The prosecutor offered to grant the accused act of production immunity, in which the prosecution would not use the fact that the accused had the decryption key or decrypted the drive at trial, but they would be permitted to introduce the decrypted contents of the drive into evidence. [146] The Eleventh Circuit, based on the precedent from *Kastigar* and other cases, declared that not to be constitutionally sufficient; the immunity had to cover both use and derivative use. [147] The Circuit Court said that the prosecution may not treat the documents as though they appeared like "manna from heaven" by using the contents of the drives without saying how they were acquired. [148] Offering both forms of immunity would prohibit the prosecution from using the information decrypted by the accused at trial, and would have been of little value to the prosecution in this instance. [149]

B. *Permitted Forced Decryption*

Although the Eleventh Circuit denied the government the ability to compel the suspect to decrypt his files, other courts have forced [*544] defendants to decrypt their data. In 2009, the District Court in Vermont considered Sebastian Boucher's assertion of his Fifth Amendment right regarding a grand jury subpoena related to suspected child pornography on his computer. [150] In that case, a Customs and Border Protection officer had inspected Boucher's laptop while he was crossing into the United States from Canada. [151] The officer found files on the computer, which at the time did not require a password or the removal of any encryption to access, with names that suggested child pornography. [152] After another officer inspected the computer, the agents arrested Boucher and read him his Miranda rights, which he then voluntarily waived. [153] With some cooperation from Boucher, the agents continued their inspection and identified more files that appeared to depict child pornography. [154]

---

[142] Id. at 1347. TrueCrypt will, by default, entirely fill a new encrypted volume with random data which makes it effectively impossible to determine how much actual data is stored in an encrypted volume without decrypting it. TRUECRYPT, *supra* note 47, at 27. *See also* TRUECRYPT, *supra* note 48, at 37-54 (discussing plausible deniability).

[143] In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d at 1346.

[144] Id. at 1349-50. The grant of immunity the district court had granted was under 18 U.S.C. §§ 6002-03.

[145] Id. at 1350-51 (quoting Kastigar v. U. S., 406 U.S. 441 (1972)).

[146] *Id.* at 1350-51.

[147] *Id.*

[148] *Id.* at 1352 (citing U. S. v. Hubbell, 530 U.S. 27 (2000)).

[149] *Id.* at 1350-51. In addition to this, the Circuit Court questioned whether the prosecution and trial court were even authorized to offer only act of production immunity by 18 U.S.C. § 6002. *Id.* at 1350 fn. 30. The court also noted that transactional immunity would exceed the protections offered by the Fifth Amendment. *Id.* at 1351 fn. 32.

[150] *In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *1 (D. Vt. Feb. 19, 2009).

[151] *Id.* at *1-*2.

[152] *Id.* at *2.

[153] *Id.* at *2.

Later, when other officers attempted to review the evidence, they found that the portion of the hard drive, which contained the incriminating files, was encrypted. [155] Despite the help of specialists trained in computer forensics, the government was unable to decrypt that portion of the hard drive. [156] The specialist stated that it was "nearly impossible to access these encrypted files without knowing the password." [157] The grand jury then subpoenaed Boucher to provide unencrypted forms of all data encrypted on the drive, and Boucher moved to quash the subpoena based on the protections of the Fifth Amendment. [158] A magistrate judge granted Boucher's request, but Boucher appealed to the district court. [159]

[*545] The district court noted that the contents of the laptop are not themselves testimonial. [160] However, the court said that, under some circumstances, producing documents may be testimonial even when the documents themselves are not testimonial. [161] This is because the act of production necessarily implies that the files do exist, that the producer had control of them, and that they were in some sense authentic. [162] Since the Fifth Amendment can apply to actions, which directly imply an incriminating fact, the Fifth Amendment can shelter the production of such material. [163]

However, the foregone conclusion doctrine, which was established in *Fisher*, can allow the defendant to be compelled to produce files or documents when the government already knows their existence and location. [164] The magistrate judge that issued the original order to quash the subpoena had concluded that the foregone conclusion rationale was inapplicable because the government did not know what all of the files were and had failed to view the majority of them. [165] The district court overruled that, saying that the government does not need to be aware of the contents of the files but only needed to show "with reasonable particularity that it knows of the existence and location of subpoenaed documents." [166] In this case, government agents had seen some of the

---

154 *Id.*

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

156 *Id.*

157 *Id.*

158 *Id.*

159 *In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *1 (D. Vt. Feb. 19, 2009).

160 *Id.* at *2 (citing Fisher v. U. S., 425 U.S. 391, 409 (1976)). The court noted that the contents of the drive were prepared voluntarily, and since they are not testimonial they were not protected by the Fifth Amendment. *Id.*

161 *Id.* at *2-*3 (D. Vt. Feb. 19, 2009). In considering that matter, the magistrate judge had specifically found that either providing the password to the grand jury and entering the password into the computer would be testimonial. *In re* Boucher, No. 2:06-mj-91, 2007 WL 4246473, at *7 (D. Vt. Nov. 29, 2007). On appeal from the magistrate's order, the government narrowed the matter to only producing the unencrypted version without necessarily providing the password itself. *In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *1 (D. Vt. Feb. 19, 2009).

162 *In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *2 (D. Vt. Feb. 19, 2009) (citing United States v. Hubbell, 530 U.S. 27, 36, 120 S.Ct. 2037, 147 L.Ed.2d 24 (2000)).

163 *Id.* at *2 (citing Doe v. U. S., 487 U.S. 201, 209 (1988)).

164 *Id.* at *3 (citing Fisher v. U. S., 423 U.S. 391, 411 (1976)).

165 *Id.*

166 *Id.*

contents and that was sufficient for them to know the existence and location of the encrypted data. [167] Therefore, the request to quash the subpoena was denied, but the government [*546] was directed to make no use of Boucher's production of the contents in its case. [168]

In 2012, the District Court for the District of Colorado faced a similar decision when dealing with the case of Ramona Fricosu, and applied the reasoning from *Boucher*. [169] In that case, the government had seized six computers from Fricosu's house while executing a search warrant. [170] One of those computers was encrypted with PGP and the government failed in its efforts to decrypt that computer without assistance from the defendant. [171] Later, the government recorded a conversation between Fricosu and her husband implying that incriminating information was on the laptop which was password protected. [172] Using that conversation as evidence, the government asked the court for a writ requiring Fricosu to assist in executing a warrant to search the computer by producing an unencrypted version. [173]

The court largely followed the logic in *Boucher* and cited to it frequently. It concluded that the government had proven, by a preponderance of the evidence, that Fricosu was either the owner or primary user of that computer and that she had access to the encrypted data on the computer. [174] It also concluded that the government knew of the location and existence of the files on that computer. [175] Therefore, it concluded that the Fifth Amendment did not prevent an order for her to produce the unencrypted contents of [*547] the drive, [176] though the court also ordered that the government may not use the actual act of production against her. [177]

The Supreme Court of Massachusetts has similarly agreed that decryption may be compelled so long as the act of decryption does not reveal new testimonial facts to the state. [178] In *Commonwelth v. Gelfgatt*, Mr. Gelfgatt was accused of fraud and was believed to be concealing much of the evidence on his computers' hard drives, which were encrypted with DriveCrypt Plus. [179] When investigators asked him to decrypt the drive or provide the

---

[167] *Id.*

[168] *Id.* at *4. This naturally means that the government will need to authenticate the contents of the drive in some other fashion. *Id.*

[169] *See generally* U.S. v. Fricosu, 841 F.Supp.2d 1232 (D. Colo. 2012).

[170] Id. at 1234.

[171] *Id.* PGP is the same program which Boucher used to encrypt his data. *In re* Boucher, No. 2:06-mj-91, 2007 WL 4246473, at *2 (D. Vt. Nov. 29, 2007).

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

[173] *Id.* In asking for this writ, the government relied on the All Writs Act. *See* 28 U.S.C. § 1651 (2012).

[174] Fricosu, 841 F.Supp.2d at 1235-36.

[175] Id. at 1237.

[176] *Id.*

[177] Id. at 1238. The Tenth Circuit denied Fricosu's request for an interlocutory appeal. Order, Fricosu v. U. S., No. 12-701 (10th Cir. Feb. 21, 2012), *available at* http://federalevidence.com/pdf/Encrypt/Fricosu.v.US.pdf. *See also Compelling Access To* Encrypted *Information (Part III)*, FED. EVIDENCE REV. (Feb. 27, 2012), http://federalevidence.com/node/1415.

[178] Commonwealth v. Gelfgatt, 468 Mass. 512, 513-14, 11 N.E.3d 605, 608-09 (Mass. Sup. Ct., 2014).

[179] Id. at 516, 11 N.E.3d at 610. The Commonwealth asserted that the encryption would be virtually impossible to break. *Id.* Although it was not discussed by the court in this opinion, DriveCrypt Plus has features to have different amounts of data revealed when different passwords are provided. Andrew Brandt, *First Look: PGP Whole Disk* Encryption *9.5 and SecurStar DriveCrypt Plus Pack 3.5*, PCWORLD (Nov. 7, 2006), http://www.pcworld.com/article/127620/article.html. The implications of this ability to reveal a password and continue hiding some information are discussed in Part VI.B.

password, he refused, citing his Fifth Amendment rights, and the trial court, on motion to compel, agreed with Mr. Gelfgatt. [180] As have other courts, the Massachusetts Supreme Court affirmed that the production of evidence could be testimonial, and thus protected by the Fifth Amendment, if it revealed to the government new information about the existence of the evidence, the fact of the person's control over that evidence, or its authenticity. [181] However, in this case the court found that, because of some of the statements made by Mr. Gelfgatt, the investigators already knew that he controlled the computers and had the encryption keys. [182] They also knew that the computers had been used in the suspect transactions and were connected to the matter being investigated. [183] Because of that, they satisfied the requirements of the [*548] foregone conclusion doctrine as articulated by this court, which required the government to establish that it knew "(1) the existence of the evidence demanded; (2) the possession or control of that evidence by the defendant and (3) the authenticity of that evidence." [184] Thus, the Fifth Amendment was no bar to the production and the defendant could be ordered to decrypt the files. [185]

C. *Comparing the Standards Used*

These cases each look at a situation in which the government sought to compel a defendant to provide a decrypted version of their hard drive in response to a subpoena and over the defendant's objections on the grounds of the Fifth Amendment. The Fifth Amendment privilege provides protection for an individual when the statement or action they are being asked for is compelled, testimonial, and incriminating. [186] When the government uses its authority through a grand jury, the courts, or otherwise to attempt to force an accused person to decrypt or provide a password, then compulsion is clear and the fact that the evidence is potentially incriminating is a safe inference. [187] Although the question is more nuanced, revealing a password is also generally testimonial.

Courts and commentators have generally found that passwords are testimonial in nature. [188] The magistrate judge that first considered Boucher's request to quash the subpoena explicitly found [*549] that entering or providing the password would be testimonial. [189] That magistrate found that forcing him to enter the password would ask the question, "Do you know the password to the laptop?" and thus confront him with the "forbidden trilemma;

---

[180] Id. at 517-19, 11 N.E.3d at 610-12.

[181] *Id.*

[182] Id. at 523-24, 11 N.E.3d at 615.

[183] *Id.*

[184] Id. 522-23, 614.

[185] Id. at 524, 11 N.E.3d at 615-16. They also found that the foregone conclusion doctrine was also sufficient show that this material was not privileged under article 12 of the Massachusetts Declaration of Rights even though that generally provides greater protection than the Fifth Amendment does. Id. at 525-26, 11 N.E.3d at 616-17.

[186] *See e.g*. Fisher v. United States, 423 U.S. 391, 408 (1976); In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1350-51 (11th Cir. 2012).

[187] In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1341-42 (11th Cir. 2012). *See also* Fisher, 425 U.S. at 409 (finding that a subpoena for physical evidence involved compulsion).

[188] *See* Andrew Winkler, *Password Protection and Self-Incrimination: Applying the Fifth Amendment Privilege in the Technological Era*, 39 RUTGERS COMPUTER & TECH. L.J. 194, 209-210 (2013) (arguing that passwords are always testimonial); Erica Fruiterman, *Upgrading the Fifth Amendment: New Standards for Protecting* Encryption *Passwords*, 85 TEMPLE L. REV. 655, 678-79 (2013). *But see* Greg Sergienko, *Self Incrimination and Cryptographic Keys*, 2 RICH. J. L. & TECH. 1 (1996) (arguing that some keys can be constructed so as to be testimonial, but that most should not be viewed as testimonial in and of themselves).

[189] *In re* Boucher, No. 2:06-mj-91, 2007 WL 4246473, at *2 (D. Vt. Nov. 29, 2007).

incriminate himself, lie under oath, or find himself in contempt of court." [190] Although the district court overturned the magistrate's conclusion, it did so by finding that the foregone conclusion doctrine provided an exception, rather than by finding that it was not testimonial. [191] Similar reasoning led the Eleventh Circuit to the same conclusion in a comparable matter. [192]

This reasoning is in accord with other cases that have dealt with passwords or combinations. For instance, the district court in *Kirschner* found explicitly that passwords to computers were testimonial because it required a defendant to reveal knowledge and use his mind. [193] Many of the cases that consider this matter have looked to the Supreme Court's 1998 decision in *Doe v. United States*. [194]

In *Doe*, the Supreme Court considered whether a defendant could be compelled, under the Fifth Amendment, to sign documents which would instruct foreign banks with which he was alleged to have done business to turn over all records pertaining to him. [195] The Court found that this did not violate his Fifth Amendment rights. [196] In that case, the majority found that signing these consent decrees, which had in themselves little information, was not testimonial. [197] Justice Stevens, in his dissent, noted that a defendant could neither be compelled to turn over the combination to his wall safe, nor open it with a [*550] combination, since that implicated using his mind. [198] The majority opinion, in a footnote, agreed with that assessment, but found that signing the documents was more like handing over a key than using or revealing a combination. [199] Based on that line of cases, it is clear that passwords and combinations will virtually always be viewed as testimonial, though that does not always mean that their production will be banned.

Since the government sought compelled production of information that was testimonial and at least potentially incriminating, it sought an exception to the Fifth Amendment in the form of the foregone conclusion doctrine. In these cases, the courts said that in order for the government to compel decryption under the foregone conclusion doctrine, it had to show that it knew that the person being subpoenaed was able to decrypt the drive or files in question. [200] This is in accordance with a Fourth Circuit statement that the foregone conclusion doctrine would prevent suppression on Fifth Amendment grounds of a password given by the defendant when the government could show that the defendant was "the sole user and possessor of the computer". [201] Further, in each case the

---

[190] *Id.* at *2-*3.

[191] *See generally In re* Boucher, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

[192] In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012).

[193] U. S. v. Kirschner, 823 F.Supp.2d 665, 668-669 (E.D. Mich. 2010).

[194] Doe v. U. S., 487 U.S. 201 (1988).

[195] Id. at 202-203.

[196] *Id.*

[197] Id. at 219.

[198] Id. at 219-220 (Stevens, J., dissenting).

[199] Id. at 210 n. 9.

[200] *See* In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012); U. S. v. Fricosu, 841 F.Supp.2d 1232, 1236 (D. Colo. 2012).

[201] U. S. v. Gavegnano, 305 Fed.Appx. 954, 955-56 (4th Cir. 2009). In that case, it was a government computer that only the defendant had used. *Id.* The court noted that the defendant had consented to monitoring of his use of that computer, but that was significant in the analysis of the Fourth Amendment, rather than the Fifth Amendment, claim. *See Id.*

government was required to provide authentication of the files by some means other than the defendant's act of production of the decrypted data. [202]

But the three courts examined different levels of knowledge on behalf of the prosecution regarding the contents of the encrypted drive or files. The Eleventh Circuit, when it gave the defendant the protection of the Fifth Amendment, emphasized the fact that the government did not know "what, if anything, was hidden based on the facts before us" even though the government knew the exact location of the encrypted data. [203] The court in *Boucher*, in denying protection [*551] to the defendant, found it significant that the government had knowledge of at least some of the files protected by encryption, even if it had not viewed all of the data. [204] However, in *Fricosu*, the court required only limited knowledge of the contents of the encrypted drive. [205] The court specifically said, "the fact that it does not know the specific content of any specific documents is not a barrier to production." [206] The court in *Fricosu* referred to the decision in *Boucher* in making that statement, even though the government had viewed at least some of the encrypted files in *Boucher*. [207] Unlike the case before the Eleventh Circuit, the government in *Fricosu* at least knew that there was meaningful data, rather than a drive filled with random data, contained on that computer. [208]

Although the Eleventh Circuit distinguished the situation before it from the matters in *Boucher* and *Fricosu* based partially on how much the government knew about the encrypted contents, the court did not reject the reasoning on which they relied. [209] Rather, the Eleventh Circuit Court merely said that the standards for the foregone conclusion doctrine were not met in that particular case. [210] Taken together, these cases could indicate that the foregone conclusion doctrine is applicable to compel decryption if the government knows the existence and location of the encrypted files, has some knowledge of the data the files contain, knows that the user is capable of decrypting the files, and can authenticate the files without use of the defendant's act of production. The government must show that it can [*552] specify the contents it is requesting with "reasonable particularity", [211] but based on the reasoning in *Fricosu* and *Boucher*, that can be achieved with only partial knowledge of those contents, and that knowledge may be inferred from other sources. Further, the government may be able to show that the user can decrypt the data if the government can show that they are the sole user of the computer. [212] Under current

---

[202] *See e.g.* Fricosu, 841 F.Supp.2d at 1237.

[203] In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012). Due to the way TrueCrypt works, it is possible that the encrypted drive would have had no meaningful data when decrypted, though the government pointed out that it already physically possessed the encrypted data even if the encrypted data would translate into nothing meaningful. *Id.*

[204] *In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *3 (D. Vt. Feb. 19, 2009).

[205] U. S. v. Fricosu, 841 F.Supp.2d 1232, 1237 (D. Colo. 2012).

[206] *Id.*

[207] *Id.*

[208] *Id.* The government knew this based on the recorded conversation. *See* Id. at 1235.

[209] In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1349 (11th Cir. 2012).

[210] Id. at 1348-49. The court, in a footnote, specifically said that if the government could demonstrate its knowledge of the files, that the defendant was in possession of the files, and that the files were authentic that it could then compel the production of those. Id. at 1344.

[211] *See e.g.* In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1344 (11th Cir. 2012).

[212] Despite its success in cases like *Fricosu* and *Gavegnano*, it may not always be appropriate to permit this to be sufficient. For instance, some "malware", particularly some "ransomware" may place encrypted data on a user's computer against their will.

precedent, the government will likely be able to compel a defendant to provide decrypted versions of the data despite Fifth Amendment objections.

IV. ANALOGIES FOR ENCRYPTION AND THEIR RELEVANCE

Courts frequently approach novel matters through the use of analogy. The choice of analogy when dealing with a new situation can radically alter the way the law is applied. Many analogies suggest themselves for encryption. One frequently used analogy is to say that encryption is like a safe, the data is like its contents, and the password is like the combination. [213] This analogy, like all analogies, is not perfectly accurate. For instance, being placed into a safe in no way changes the contents of the safe. But encryption does change the contents. It transforms them from plaintext to ciphertext, which is essentially meaningless without the ability to decrypt it. [214] Also, any physical safe can eventually be destroyed or forced open to retrieve the contents if law enforcement has physical control of the safe, but effective encryption may be virtually unbreakable by any means other than guessing every possible password. [215] Despite these flaws, this is [*553] likely to be one of the best analogies for considering encryption in a legal context. Using this analogy would suggest, as some courts have already ruled, that passwords for encryption are generally protected from disclosure by the Fifth Amendment, though exceptions such as the foregone conclusion doctrine may be available to permit the government to compel the production of the unencrypted files under some circumstances.

However, other analogies have been used. For instance, it is possible to retain the safe analogy but argue that the password is more akin to a key than it is to a combination to a safe. [216] The literature dealing with cryptography outside of the legal context often does refer to the password or other information needed to decrypt a file as a key. [217] If this view were adopted, it would permit decryption to be compelled under many circumstances as a "mere physical act". [218] This view can be supported by the fact that in some forms of cryptography, the password entered by a user protects only a much longer password, which was formed by the computer itself and used for the actual encryption. [219] In other cases, the key comes in the form of a file whose data was involved in the process of encryption and without that file turning over a password is of no value. [220]

Viewing the encryption key as more similar to a physical key than to a combination presents a number of problems. For one thing, the Eleventh Circuit has already explicitly rejected that comparison. [221] Even if another circuit wished to reconsider it, not all encryption works by using an extensive computer generated string as the key or using a file as part of the key. It is possible to use the password itself [*554] as all that is needed to encrypt or

---

See e.g. Dan Goodin, *You're Infected - If You Want to See Your Data Again, Pay Us $ 300 in Bitcoins*, ARSTECHNICA (Oct. 17, 2013) http://arstechnica.com/security/2013/10/youreinfected-if-you-want-to-see-your-data-again-pay-us-300-in-bitcoins/.

213 *See e.g.* In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012).

214 EFF, Encryption *Basics*, SURVEILLANCE SELF DEFENSE, https:// ssd.eff.org/tech/ encryption (last visited Dec. 8, 2013).

215 One analysis indicates it would take billions of years to break AES encryption through brute force assuming the key size was at least 128 bits. Arora, *supra* note 76. The computer security specialist said somewhat more optimistically during questioning that it could take the government years to decrypt the files in question in the *Boucher* case without the cooperation of the defendant. *In re* Boucher, No. 2:06-mj-91, 2007 WL 4246473, at *4 (D. Vt. Nov. 29, 2007).

216 *See* Philip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171, 173-175 (1996).

217 *See e.g*. Arora, *supra* note 76.

218 In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1345-46 (11th Cir. 2012).

219 *See e.g*. TRUECRYPT, *supra* note 47, at 138.

220 *Id.* at 66.

221 In re Grand Jury Subpoena Duces Tecum Date March 25, 2011, 670 F.3d 1335, 1345-46 (11th Cir. 2012).

decrypt the data. [222] In that case, there is nothing separate from the password that the user could even hypothetically hand over. Drawing a distinction between those two forms of encryption, especially when such implementation details are virtually always hidden from the end user, is a strain of logic. Even when something other than the password is technically used in the decryption process, that item itself is generally protected by the password, and in the case of the keyfile, the user must identify which file serves as the keyfile. That may still make it easier for the government to compel decryption by asserting that they know with reasonable particularity that what they are requesting is the computer generated encryption key that actually unlocks the encryption. But it would not remove the fact that the government is trying to compel the defendant to use the contents of their mind and must therefore show that the foregone conclusion doctrine or some similar exception provides a reason that the Fifth Amendment does not privilege it. Thus, it is both logically cleaner and closer to the literal truth to consider the password more akin to a combination.

Another commentator, Mr. McGregor, has suggested that encryption is much like a translation of the document. [223] This is also problematic. A translation is generally expected to continue to have meaning when the translation is completed, albeit in a different context and perhaps to different people or technologies than the original. But encryption creates something which becomes meaningless without the decryption key or password. Further, translation at least risks changing the meaning in a way that cannot be perfectly recovered. If a document is translated from English to Japanese, and then back again, the new document translated from Japanese will rarely be identical to the original, even if the essential meaning is preserved. This is necessarily so due to the quirks in each language, which may have idioms lacking in the other, and words with multiple meanings or words which lack a direct translation into the other language. Encryption, though, perfectly preserves the ability to restore the original. Moreover, viewing encryption as a mere translation is likely to remove any presumption that encryption creates an expectation of privacy for purposes such as the Fourth [*555] Amendment, given that speaking in another language has been held to not create an expectation of privacy. [224] Although there is a sense in which encryption is a translation, it is not helpful as an analogy.

At least one paper suggests that encryption can also be viewed as a special form of shredding the encrypted documents. [225] In this form of shredding, each piece of the shredded paper contains an identifier to show where it should go, but the shredding also requires a map to show how the pieces of paper should be arranged in order to extract any meaning from it. [226] While there is some appeal to this comparison, it is not overly useful in this context. Analogies to aid reasoning should be as simple as possible and grounded as nearly as possible to something which is both concrete and familiar to those considering the analogy. This one is far less concrete and familiar to most people than would be either a safe or a translator. More than that, it could be misleading. It suggests that it would require far more work and information from the defendant to get the unencrypted version back than it does with the use of automated encryption, while at the same time making it seem far more realistic that law enforcement could create the decrypted version without help from the defendant than is true with effective encryption.

While no analogy is perfect, encryption in this context is most aptly described as storing digital items within a safe that is secured by a combination. This is less reflective of the actual process that the computer uses to encrypt

---

[222] Although it could not be seriously relied upon for security today, the Caesar Cipher uses a simple number as its key and the process can reasonably be done by hand. WRIXON, *supra* note 10, at 170.

[223] Nathan McGregor, *The Weak Protection of Strong* Encryption*: Passwords, Privacy, and Fifth Amendment Privilege*, 12 VAND. J. ENT. & TECH. L. 581, 600 (2010).

[224] U. S. v. Longoria, 177 F.3d 1179, 1184 (10th Cir. 1999) (dealing with drug dealers that attempted to avoid interception of their conversations by speaking in Spanish). *See generally* Sean Edgett, *Double-Clicking on Fourth Amendment Protection:* Encryption *Creates a Reasonable Expectation of Privacy*, 30 PEPP. L. REV. 339 (2003).

[225] McGregor, *supra* note 222, at 602-03.

[226] *Id.* at 602-03.

documents than either the translation or the shredding analogies. But it comes closest to capturing the experience of computer users and how they actually use encryption, which is more significant when determining how to treat it in jurisprudence and how to compare it to precedent already in place.

[*556] V. TOWARDS BROADER USE OF THE FOREGONE CONCLUSION DOCTRINE

A. *The Argument for a Low Standard for Finding a Foregone Conclusion*

Looking at encryption through the analogy of a safe and examining the precedent which has been created so far provides a test for when the government can compel a defendant to decrypt potentially incriminating files. The Fifth Amendment will generally prevent forced decryption by a criminal defendant unless the government gives constitutionally sufficient immunity or an exception applies. Constitutionally sufficient immunity requires both use and derivative use immunity regarding that particular defendant. In this context, the exception that will apply most often and be most useful to the prosecutor is the foregone conclusion doctrine.

The foregone conclusion doctrine requires the government to establish that it can show with reasonable particularity the existence and location of the documents and be able to authenticate them without use of the defendant's production of the documents. [227] Currently, established precedent indicates that the government must have some idea of the contents it expects to find protected by encryption. The Eleventh Circuit quashed the subpoena based largely on the fact that the government could not establish that there would be any data at all if the drives were decrypted. [228] In both *Boucher* and *Fricosu*, the government had some knowledge of some of the encrypted contents either through agents that had seen some of the contents or by hearing about them from conversations the defendant had about the contents. [229]

But the doctrines on which these decisions are based do not require that the government have actual knowledge of the contents they are requesting, but merely the location and existence of those contents and the ability to authenticate them independently. [230] The [*557] *Fisher* court, which originally laid out the foregone conclusion doctrine, based the doctrine largely on the fact that the government was "in no way relying on the 'truthtelling' of the taxpayer." [231] But when the government is asking for compelled decryption, it is not asking for the defendant to tell the truth about anything. It is instead asking for the defendant to surrender the voluntarily prepared documents. The Eleventh Circuit noted that the government does not need to "identify exactly the documents it seeks," [232] and the court in *Fricosu* made a slightly stronger statement that "the fact that [the government] does not know the specific content of any specific documents is not a barrier to production." [233]

---

[227] *See* Fisher v. U. S., 425 U.S. 391, 410-412 (1976).

[228] In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1349-50 (11th Cir. 2012).

[229] *In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *2 (D. Vt. Feb. 19, 2009); U.S. v. Fricosu, 841 F.Supp.2d 1232, 1235 (D. Colo. 2012).

[230] Even if the Eleventh Circuit had taken this broad view of the foregone conclusion doctrine, it is likely that it still would have quashed the subpoena and not forced the defendant to decrypt the drive. In that case, the court did not find that the government could show the defendant's ability to decrypt the drive and the government could not establish that it could authenticate any documents produced without using the defendant's act of production. In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012).

[231] Fisher v. U. S., 425 U.S. 391, 411 (1976).

[232] In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1347 (11th Cir. 2012). The quote goes on to say that "but it does require some specificity in its requests-categorical requests for documents the Government anticipates are likely to exist simply will not suffice." *Id.*

[233] Fricosu, 841 F.Supp.2d at 1237.

The fact that the government does not know what is contained, or that anything meaningful is contained, inside the encrypted data should not be a barrier to production. In saying that the government did not know enough to meet the standard in that case, the Eleventh Circuit said that the government could only establish that there were "random characters" on the drive since "the TrueCrypt program displays random characters if there are files and if there is empty space" and "random character are not files." [234] But even an empty file is a file, [235] and if the government does not need to know the exact contents of what it is requesting, then there is no reason it should be barred from receiving a decrypted copy just because the decrypted file would be blank. The Eleventh Circuit said that the government needed to have "some specificity in its requests - categorical requests for documents the Government anticipates are likely to exist simply will not suffice." [236]

[*558] In making that statement, the court relied on the Supreme Court's decision in *Hubbell*. [237] In that case, Webster Hubbell was prosecuted for tax-related crimes and fraud. [238] The prosecution built its case largely on documents provided by Hubbell himself after he had been granted immunity to the extent allowed by law. [239] Those documents had been assembled by Hubbell, after he asserted his Fifth Amendment rights and was granted immunity, from the documents in his collection in response to a broad subpoena for eleven categories of documents. [240] Prior to Hubbell's response, the government could not have shown that it had any knowledge of the existence of these documents other than through a broad argument that a businessman would always keep such records. [241] The Court concluded that, under those circumstances, the grant of immunity covered both use and derivative use and that the foregone conclusion doctrine did not apply and the documents could not be used against Hubbell. [242]

But the situation where the government seeks to force decryption of encrypted files it already possesses is different from the situation the Supreme Court faced in *Hubbell*. In *Hubbell*, the government did not know prior to granting immunity that the documents it was going to receive existed. [243] When the government seeks to force decryption it clearly knows that a document exists in the form the encrypted file or partition that it seeks to decrypt. The government may not be able to show ahead of time that the file will have meaningful content once decrypted, but that is different from not knowing its existence at all. In *Hubbell*, the government did not know the location of the files ahead of time, and Hubbell was forced to expend considerable thought and effort assembling those documents that were responsive to the subpoena. [244] When the government asks for decryption, it already knows where the files are because it has them in its possession. Under the current Supreme Court precedent, the government should not [*559] need to prove that it has any knowledge of the content of the encrypted drive, or even that there is content beyond a blank file.

Adopting this standard would make it easier for the government to compel a defendant to decrypt protected information than it is now. But that is wise from a policy standpoint, and supported by current precedent. The Fifth

---

234 In re Grand Jury Subpoena Duces Tecum Date March 25, 2011, 670 F.3d 1335, 1347 (11th Cir. 2012).

235 There are in fact reasons for empty files or files with random content to be created on a computer, such as for testing purposes. A file filled with random data may also be used as a keyfile for encryption. TRUECRYPT, *supra* note 47, at 66.

236 In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1347 (11th Cir. 2012).

237 U. S. v. Hubbell, 530 U.S. 27 (2000).

238 Id. at 31-32.

239 Id. at 38.

240 Id. at 31.

241 Id. at 44-45.

242 Id. at 44-46 (2000).

243 *Id.*

244 *Id.*

Amendment, according to the Supreme Court, "does not independently proscribe the compelled production of every sort of incriminating evidence" and "protects a person only against being incriminated by his own compelled testimonial communications." [245] Someone could not effectively protect documents merely by placing those documents in a safe locked by a combination, so they should not be able to shield them from the view of the courts merely by placing them digitally behind the wall of encryption.

Although taking this view of the foregone conclusion doctrine would make it simpler for the government to compel decryption in some cases, it would not remove all hurdles or safeguards preventing the government from demanding decryption in all cases. The government must legitimately gain access to the encrypted file itself, which will mean at least in some instances that it must have satisfied the requirements of the Fourth Amendment. [246] Even when the government has the encrypted file in hand and has obtained it in a legitimate way, it must show that the defendant is capable of decrypting it. This is part of the authentication standard it must meet for the foregone conclusion doctrine, and a person cannot be compelled to do something they are incapable of doing. The court in *Fricosu* properly found that Fricosu was capable of decrypting the drive in question and used a preponderance of the evidence standard. [247]

There, the court focused on the fact that she was the "sole or primary user" of the computer. [248] That may not always be enough to [*560] show that someone has the ability to decrypt files on their computer. For instance, public key cryptography allows a person to encrypt a file in such a way that someone else, and only that other person, is able to decrypt it. [249] This is frequently used on sensitive files before they are transmitted over the Internet, and it is entirely possible that an unencrypted version would not be retained. Similarly, there are distributed storage systems and distributed communications systems in which the user permits some of their hard drive space to be used by others to store encrypted fragments of files for other users, and in exchange the other users allow them to do the same. [250] Such systems may be used for backup purposes or to allow remote access to data. [251] Under such a system the user does not have the ability to directly access the encrypted data stored on the drive. [252] Similarly, there are certain programs that will encrypt part of a user's hard drive against their will in order to try to extort money, often in the form of bitcoins, from the user to get the encryption key to recover the data. [253] With

---

[245] Fisher v. U. S., 425 U.S. 391, 410-412 (1976).

[246] *See* Edgett, *supra* note 223; David Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2223-24 (2009) (arguing that encryption can create an expectation of privacy even when the data itself is stored by a third party, such as when it is being stored by a cloud computing service).

[247] U. S. v. Fricosu, 841 F.Supp.2d 1232, 1234 (D. Colo. 2012).

[248] *Id.* Although the court did have other evidence on the record such as the conversation between Fricosu and her husband which at least implied that she was able to decrypt the drive. Id. at 1235. The court in *Gavegano* similarly focused on the fact that the defendant was the sole user of the computer when it applied the foregone conclusion doctrine, though in that case there was no doubt he was capable since he had already provided the decryption before the trial and was then challenging admissibility. U. S. v. Gavegnano, 305 Fed. Appx. 954, 955-56 (4th Cir. 2009).

[249] *See supra* Part II.B.

[250] *See e.g., How Symform Works*, SYMFORM, http://www.symform.com/join-therevolution/how-symform-works/ (last visited Aug. 20, 2014).

[251] *Free Cloud Backup & Storage*, SYMFORM, http://www.symform.com/free-cloudbackup/ (last visited Aug. 20, 2014).

[252] Encrypt, *Shred, and Geo-Spread*, SYMFORM, http://www.symform.com/join-therevolution/how-symform-works/encrypt-shred-and-geo-spread/ (last visited Aug. 20, 2014).

[253] *See generally* GAVIN O'GORMAN & GEOFF MCDONALD, RANSOMWARE: A GROWING MENACE (Symantec, 2012) *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growingmenace. pdf.

these possibilities for a user to not be able to decrypt all data on their own systems, it may be necessary in many instances for a prosecutor to provide more evidence than merely ownership of a system to establish that the defendant can decrypt the data in question.

Adopting this standard would make it relatively easy for prosecutors to demand decryption of files, while still providing safeguards for cases where the accused is genuinely incapable of decrypting the file. It requires the prosecutor to show that they know the files in question exist and where the file is by legitimately acquiring the encrypted version of the files first. The prosecutor would also need to show that the defendant is able to decrypt the file. [*561] Similarly, in order to make use of the files at trial, the prosecutor will need to be able to authenticate them without relying on the fact that the defendant decrypted them, though the same evidence that the defendant was able to decrypt them would be applicable in most cases.

B. *Literature Review and Responses*

Other methods have been proposed to logically and efficiently handle the complications that strong encryption can create for law enforcement. One note, by Mr. Ungberg, recommended a system in which prosecutors who wanted access to an encrypted file would seek a warrant with probable cause for a search of the file that specified precisely what data they were seeking. [254] The note gave an example of the warrant laying out tax returns for certain years. [255] The prosecutor would then be able to obtain a subpoena for the encryption password, but would be barred from using any evidence other than what was specified in the warrants, and in particular would be barred from using evidence of crimes for which they were not yet investigating the defendant. [256]

This proposed system is appealing in many ways. It provides a clean and clear procedure for police and prosecution to follow and would not permit strong encryption to form an absolute bar to the prosecution. But it does not explain how this new proposal could be fit into existing jurisprudence where passwords have repeatedly been held to be testimonial, even if some exceptions have permitted them to be compelled under some circumstances. Nor does the proposed system answer whether the prosecution would be able to use the defendant's production as authentication by itself. Finally, it seems inconsistent with current Fourth Amendment jurisprudence to ban the use of absolutely all other data not described in the warrant and not allow investigators to "stumble upon" at least some forms incriminating evidence while executing their allowed search. [257] Once the metaphorical safe of an encrypted file is open, then seeing images which are clearly child pornography would likely fall under the plain [*562] view doctrine in the same way that finding a silencer in a filing cabinet that was properly being searched under a warrant would. [258]

Another article claimed that the foregone conclusion doctrine could never apply to the production of a password or to the act of decryption. [259] The article relies on the magistrate's decision in *Boucher* to assert that the foregone conclusion doctrine "would not apply to the production of non-physical evidence existing only in a suspect's mind where the act of production can be used against him." [260] Based on that, and the fact that the password exists only in the mind of the defendant, it is immune to a foregone conclusion doctrine.

---

[254] Andrew J. Ungberg, *Protecting Privacy Through a Responsible Decryption Policy*, 22 HARV. J.L. & TECH. 537, 556 (2009).

[255] *Id.*

[256] *Id.*

[257] U. S. v. Scarfo, 180 F.Supp.2d. 572, 578 (D.N.J. 2001).

[258] U. S. v. Carmany, 901 F.2d 76, 77-78 (7th Cir. 1990).

[259] Winkler, *supra* note 188, at 214.

[260] *Id.* at 211.

There is some merit to this argument where the password does exist only in the defendant's mind and where the government seeks the password for its own sake. But passwords frequently exist in some tangible form, whether written down or held in a password management program. [261] Even for passwords that have never existed in a tangible form, it is rare for the government to seek the password itself. Rather, the prosecution wants the password only as a means to get the documents. If the defendant wishes to maintain the secrecy of the password, the government will virtually always be content with turning over an unencrypted version of the encrypted file or having the defendant enter the password for them. This avoids the defendant ever directly providing something that "exists only in his mind." [262] The possibility of the act of production being used against the defendant does raise further Fifth Amendment concerns, but those are handled by forcing the prosecution to establish the authenticity of the documents without aid from the defendant and further safeguarded by a court order that the prosecution may not use the defendant's possession of the key against them, as the courts in *Boucher* and *Fricosu* did. [263]

[*563] A more moderate approach, suggested by Mr. Clemens, would continue to permit the foregone conclusion doctrine to be used to compel encryption, but would demand an exceptionally high standard of proof from the prosecutor to show that it was applicable in the case at hand. [264] That note asserts each prong of the *Fisher* test to establish that the contents of the encrypted file should be shown with clear and convincing evidence. [265] It further asserts that in proving that the government knows the location of the documents, it must show that the defendant was the only person who had access to the decryption key or that the defendant specifically accessed a particular document within the encrypted file. [266] Finally, he asserts that the government must prove the authenticity of the documents that it is seeking, prior to compelling the decryption. [267]

But he goes too far. The courts when looking at the foregone conclusion doctrine have generally required only reasonable particularity in establishing that the government knows the existence and location of the files that it seeks. [268] Clearly, the government must show that the defendant has the ability to decrypt the files the government wants them to decrypt, but at least one court has held that it is sufficient to show this by preponderance of the evidence. [269] Furthermore, as a matter of policy, showing this by a preponderance of the evidence is sufficient. If the files were in a safe, the government would be able to obtain them by breaking open the container if the government first acquired a warrant. [270]

Additionally, there is no requirement that the government make full proof of its ability to authenticate the documents prior to receiving them. The district court in *Boucher* was willing to compel decryption [*564] on the government's statements that it would authenticate any document which it did use later and explicitly refused to rule at that time

---

[261] *See e.g. KeePass Password Safe*, KEEPASS, http://keepass.info/ (last accessed Aug. 20, 2014).

[262] Winkler, *supra* note 188, at 214.

[263] *See supra* Part III.B.

[264] *See* Aaron M. Clemens, *No Computer Exception to the Constitution: The Fifth Amendment Protects Against Compelled Production of an* Encrypted *Document or Private key*, 2004 UCLA J.L. & TECH. 2 (2004).

[265] Id. at 11.

[266] Id. at 18.

[267] Id. at 23-24.

[268] *See e.g.* In re Grand Jury Subpoena Duces Tecum Date March 25, 2011, 670 F.3d 1335, 1344 (11th Cir. 2012). Mr. Clemens acknowledges this and specifically argues against using this standard. Clemens, *supra* note 264, at 13.

[269] U.S. v. Fricosu, 841 F.Supp.2d 1232, 1235-36 (D. Colo. 2012).

[270] 18 U.S.C. § 3109 (2012) (authorizes the breaking of items within a house when needed to execute a warrant if denied admittance). *See also* U. S. v. Schleis, 543 F.2d 59 (8th Cir. 1976) (finding proper the forcing open of a briefcase during a drug investigation).

on whether the government would succeed in doing so. [271] Moreover, some documents may prove easy to authenticate once received, especially if those documents contain a scanned signature or a digital signature. [272] The claim that the government must show that the defendant is the only one capable of decrypting the file or has personally accessed the file is simply not supported by either current jurisprudence or policy, so long as the government can show that the defendant is capable of decrypting it.

Mr. Clemens also stated that compelling key disclosure could provide far more than compelling the decryption of a particular encrypted file since the same key may be able to decrypt numerous documents. [273] This is particularly true regarding public key encryption where a user may have one key that decrypts virtually all of his documents. This is a good reason to favor compelling the defendant to provide a decrypted version of the documents rather than turn over the key itself. [274]

Mr. Reitinger took almost the opposite views from Mr. Clemens. [275] Mr. Reitinger has noted that there is an obligation to produce documents in a readable format, in other words, unencrypted, when they are responsive to a subpoena. [276] The results in that case would not be different if they were locked in safe or sitting on a desk, the defendant must respond to a legally authorized subpoena even if the files are encrypted. [277] He is entirely right on that, except when the subpoena may be challenged on some grounds such as it being in [*565] violation of the Fifth Amendment. The Supreme Court in *Hubble* found that the production of documents of broad classes could be incriminating and would not fall into an exception of the foregone conclusion doctrine if the defendant made use of extensive contents of his mind in assembling those documents and revealed their existence precisely by turning them over. [278] In some instances, the government will be able to subpoena specific documents and will know they exist, such as when the government wants to acquire a specific tax record. In those cases, whether the party has stored them physically inside a safe, digitally protected by encryption, or left them lying on the table is irrelevant.

However, this argument will not be sufficient when the government must make a broader request. For instance, in *Boucher*, the government wanted to view all of the files that were within the encrypted drive, not merely those which it could specifically name, because they had been viewed before. [279] Since the files it was seeking were contraband by nature, any production of those files which revealed the existence of files the government did not know about previously would implicate the Fifth Amendment by showing their existence unless some exception to that privilege applied. Mr. Reitinger correctly points out that a subpoena that requires the defendant to produce plaintext is no different from one that requires the defendant to produce the documents from a safe. [280] While this is correct, if the safe were secured by a combination, the government would have to prove some exception to the

---

[271] *In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *2 (D. Vt. Feb. 19, 2009).

[272] Philip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171, 191 (1996).

[273] Clemens, *supra* note 264, at 16-17.

[274] The password may be distinct from the key, especially when dealing with some form of asymmetric or public key encryption. *See supra* Part II.B. However, surrendering the password will normally permit the key to be obtained by decrypting it, so long as the fullencrypted key is available, and so the distinction is of little significance in practice. *See Id.*

[275] Mr. Clemens directly responds to many of Mr. Reitinger's arguments in his paper. Clemens, *supra* 264, at 15.

[276] Reitinger, *supra* note 272, at 175.

[277] Reitinger, *supra* note 272, at 173-175.

[278] U. S. v. Hubbell, 530 U.S. 27, 44-46 (2000).

[279] *See In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *1 (D. Vt. Feb. 19, 2009).

[280] Reitinger, *supra* 272, at 187.

Fifth Amendment to compel the defendant himself to open it so that they could view all the documents within it. [281] Thus, this helps little with the analysis when the government is faced with an encrypted file which it believes holds relevant data but cannot decrypt without the defendants help, and only helps if the government is holding a list of specific, nonprivileged documents which it would like the defendant to turn over.

Mr. Reitinger also asserts that a decryption key stored on the computer can be subpoenaed by the same standards as the plaintext of [*566] the documents that it protects, since the key has an independent existence even if it resides on the computer in an encrypted form. [282] This is true for some types of cryptography, but handing over the key may grant far more than the ability to decrypt a specific file. It may grant the ability to decrypt large amounts of data in that person's possession, as well as vast swaths of communications sent to or by that person if the key is used to secure e-mail. [283] It may also grant the ability to sign or authenticate digital documents as though they were from that person. [284] Also, the key itself is likely to be encrypted and may well be hidden or stored with other personal digital information, which returns to the question of whether the person with the key can be compelled to locate and decrypt it. [285]

On the other hand, Mr. Reitinger suggests that keys that are never actually stored and only memorized may be immune to subpoena, but that the government is likely to be able to break the encryption that "use small, memorized keys". [286] This idea is problematic. Where the government can show that the Fifth Amendment does not provide protection, such as by showing that an exception applies, then the fact that the key exists only in the memory should not be a bar to the government compelling the use of that key to decrypt the files that it wishes to access. It may prove a bar to forcing the defendant to turn over the actual password or key, but that is rarely what the government is actually seeking. Moreover, if courts were to give additional protection to keys that were purely memorized, those wishing to conceal contraband would likely find ways to memorize long keys with sufficient complexity. Many Muslims memorize the entire Quran, which is roughly 80,000 words long, to earn the title Hafiz and show their devotion to Islam. [287] There is also a large number of people who memorize thousands of digits of Pi, which are [*567] essentially random since Pi is a provably irrational number. [288] Using quotes from the Quran or digits from Pi as a password would provide poor security, as many others would likely duplicate it, but it shows the capability of people to memorize long tracts when they are motivated to do so. Further, if special protection was given to encryption schemes that did not use an independent key and instead favored encryption which encrypted directly with the password, then programmers would likely oblige by creating new interfaces which made use of exceedingly long passwords easier, and perhaps with use of tools to help people create and memorize passwords which were both strong and memorable without ever writing them down. Precedent does not require memorized

---

[281] Doe v. U. S., 487 U.S. 201, 219-220 (1988) (Stevens, J., dissenting). Of course, with a physical safe the government could destroy the safe to get the documents if it knew they were there and if it had legal access to the contents of the safe. *See supra* note 270 and accompanying text.

[282] Reitinger, *supra* note 272, at 203-204.

[283] Sullivan, *supra* note 58.

[284] *The GNU Privacy Handbook: Making and Verifying Signatures*, GNUPG (1999) http://gnupg.org/gph/en/manual/x135.html.

[285] *See supra* notes 72-74 and accompanying text.

[286] Reitinger, *supra* note 272, at 204-205.

[287] Tim Townsend, *Those Who Have Memorized Quran Are in High Demand*, ST. LOUIS POST-DISPATCH (Aug. 08, 2013), http://www.stltoday.com/lifestyles/faith-andvalues/those-who-have-memorized-quran-are-in-high-demand/article_5abf4f9b-ea6b-5b21-bd12-31bd2917ceac.html.

[288] *See* PIE WORLD RANKING LIST, http://www.pi-world-rankinglist. com/index.php?page=lists&category=pi&sort=digits (last visited Aug. 21, 2014). The current world record is 67890 digits memorized.*Id.*

keys to have special protection over those that are recorded on a computer, and policy suggests that it would yield poor results if they were given special treatment over other keys.

VI. DENIABLE ENCRYPTION, STEGANOGRAPHY, AND COMPLICATIONS

A. *Stenography*

Although it should generally be relatively easy for the prosecutor to demand decryption when there is a need, deniable encryption and steganography could make it difficult for the prosecutor to meet even a low standard of proof when they are properly employed. Steganography is a collection of techniques for concealing data inside of other data.

Steganography, at least in its modern form, involves altering a file to contain additional information while concealing the fact that the file has been altered. [289] The word itself is from a Greek phrase for "concealing writing" and versions of steganography have been used since at least 440 B.C. [290] Demeratus used steganography to pass concealed messages about a planned invasion of Sparta by Xerxes. [291] [*568] At the time, writing tablets that were covered in wax were in common use, with messages being written onto the wax. [292] The wax could later be melted to reuse the table. [293] Demeratus removed the wax from his tablet and wrote his concealed messages directly upon the wood backing, and then covered them with wax before sending them back to Sparta. [294]

In the more modern era, steganography has been used by al-Qaeda agents to pass messages and conceal documents. [295] It has allegedly been used by Russian spies to send messages among themselves over the Internet. [296] Other groups have used it to attempt to get around restrictions on free speech by more totalitarian governments. [297] In more commercial settings, steganographic techniques are used to embed unobtrusive watermarks into media files to help media companies track and combat piracy. [298] There are several different forms of digital steganography, but they all involve modifying a file to embed additional information into it in a way that is difficult to detect. [299]

One of the simplest forms of steganography is called least significant bit substitution and involves modifying the last bit out of every byte of a file, such as an image, to carry the intended message. [300] This can result in the file being

---

[289] Sean Gallagher, *Steganography: How Al-Qaeda Hid Secret Documents in a Porn Video*, ARSTECHNICA (May 2, 2012) http://arstechnica.com/business/2012/05/steganography-how-al-qaeda-hid-secret-documents-in-a-porn-video/.

[290] Fabien A. P. Peticoalas, *Information Hiding - A Survey*, 87 PROC. OF THE IEEE 1062, 1065 (1999).

[291] *Id.*

[292] *Id.*

[293] *Id.*

[294] *Id.*

[295] Gallagher, *supra* note 289.

[296] Jon Stokes, *How Even the Dumbest Russian Spies Can Outwit the NSA*, ARSTECHNICA (July 4, 2010), http://arstechnica.com/tech-policy/2010/07/how-even-the-dumbestrussian-spies-outwit-the-nsa/.

[297] Peticoalas, *supra* note 290, at 1062.

[298] *Id.* at 1062-63.

[299] Gallagher, *supra* note 289.

[300] *Id.*

noticeably degraded, which may arouse suspicion. [301] More sophisticated methods exist that are less likely to be apparent on casual inspection and are also more resilient to damage or modification to the file. [302] Generally, the larger and [*569] more complex the file is, the more data may be hidden in it without making the hidden information obvious. [303] Steganography can occasionally be located by statistical analysis, but this is difficult if the amount of data hidden is small. [304] In some less sophisticated forms of steganography, or where the data being concealed is large compared to the file in which it is hidden, steganography can introduce noticeable distortions in the file. [305] This is particularly true of audio files. [306] The data may be encrypted as well as concealed, or it may merely be concealed by techniques from steganography. [307] A video file had 141 text files contained within it in a terrorism case in Berlin. [308] Although media files such as videos, images, or sound files are often used, software exists to hide messages inside of e-mails that would appear to be spam on the surface. [309]

The challenge for prosecutors and law enforcement is that steganography, by design, can be hard to detect. [310] Even after seizing a hard drive or otherwise acquiring the files that contain information hidden in this way, the prosecution may not be aware of the hidden data. Most likely, if they do discover data that is both concealed and encrypted then they will be able to demand decryption under the foregone conclusion doctrine. [311] By that point they would have [*570] discovered that the encrypted data existed, and would know precisely where it was, and the fact that it was specifically concealed by steganography would be an indication that the data was not random and did not represent a blank file after decryption. [312]

---

[301] *Id.*

[302] *Id.*

[303] *Id.*

[304] *Id.*

[305] Gallagher, *supra* note 289.

[306] *Id.*

[307] *Id.*

[308] *Id.*

[309] Declan McCullagh, *Bin Laden: Steganography Master*, WIRED (Feb. 07, 2001), http://www.wired.com/politics/law/news/2001/02/41658?currentPage=all.

[310] Though clearly not impossible, as some steganographically hidden files used by al-Qaeda were found by the computer forensics experts in Berlin. Gallagher, *supra* note 289. One technique that is used to try to locate steganography is digital fingerprints. This technique looks for patterns in the file that would indicate they have been manipulated to conceal additional information. *Id.*

[311] It is likely that even under the standards used by the Eleventh circuit that the prosecution would be able to meet the standards the foregone conclusion doctrine. The presence of steganography would plainly indicate that something was hidden and provide some indication that it is likely incriminating. Under the standards recommended in Part V of this paper, it would be relatively easy for the prosecution to acquire a court order demanding decryption.

[312] The Eleventh Circuit directly rejected the idea that the fact encryption was used implied that there was incriminating evidence. In re Grand Jury Subpoena Duces Tecum, 670 F.3d 1335, 1347 (11th Cir. 2012). There are indeed many reasons to use encryption, and even steganography, where the data being protected is not incriminating or illicit in any way. However, steganography unlike most other forms of encryption, benefits strongly from minimizing the amount of data that it stores. It makes sense in certain encryption strategies to encrypt vast swaths of a hard drive to store tiny amounts of data or even to leave the encrypted container blank for some period of time. Steganography however becomes easier to detect as the amount of data hidden becomes larger, so it is unusual to use steganography to hide a vast amount of data. The hidden data may not

However, the prosecution most likely will not be able to compel a defendant to tell them if they are using steganography. Even if the prosecution had independent confirmation that steganography was used, they would not be able to demand that the defendant tell them what files had the hidden information or where on a hard drive the data was hidden. If the prosecution needed to ask that question, it would be clear that it could not specify where the files in question were with any particularity. Thus, while prosecution may be able to compel decryption of steganographically hidden data that is also protected by cryptography, it must locate the data without the aid of the defendant.

B. *Deniable* Encryption

Deniable encryption can create a similar issue. Deniable encryption comes in several forms and generally exists to provide the ability to plausibly deny that encryption was used at all. Alternatively, it can enable someone to reveal some files within an encrypted container and plausibly deny that there are other files still encrypted within that container. [313] One of the more commonly used forms is a Deniable File System, which is implemented by products such as TrueCrypt. [314] In a standard Deniable File System setup, the user [*571] creates an encrypted file system whose existence and status as an encrypted file is not hidden. [315] This encrypted file is protected by a password and the normal technological protections given to an encrypted file. [316] It may be filled up with data which appears sensitive so that, should anyone acquire the password for this encrypted file, it will not appear to be unusually empty. [317] Then, another encrypted volume, often called a hidden volume, is created within the outer encrypted volume using mathematical techniques to make it difficult to tell that there is additional data rather than merely space within the encrypted file that has not yet been populated with data. [318]

This technique is meant to make it possible to reveal the password to the outer volume or decrypt the outer volume in front of third parties while those third parties remain unable to decrypt or even prove the existence of the inner hidden volume. [319] Security experts have shown that there may be ways to determine that a hidden file system exists, but those methods are not reliable. [320] Most of those methods exploit leakage from the operating system or applications that work with the data inside the hidden file system, rather than through anything which may be inherently discovered about the hidden file system itself or the container encrypted file. [321] In order to address the possibilities of such leaks, later versions of TrueCypt implemented a Deniable Operating System Feature. [322]

---

necessarily be incriminating, but it is justified to presume that something is there unlike an encrypted file which may turn out to be blank when decrypted.

313 Alexei Czekis, et al., *Defeating* Encrypted *and Deniable File Systems: TrueCrypt v5.1a and the Case of the Tattling OS and Applications*, HOTSEC 1-2 (2008), https://www.schneier.com/paper-truecrypt-dfs.pdf.

314 *Id.* TrueCrypt is hardly the only example of an encryption suite that offers options for deniable encryption. *Id.*

315 *Id.*

316 *Id.*

317 *See e.g.* TRUECRYPT, *supra* note 47, 38-39 (discussing Hidden Volumes, a form of a deniable file system).

318 *Id.* Czekis, *supra* note 313 at 1-2. The space will appear to contain random data whether it is empty or contains a hidden volume. *Id.*

319 TRUECRYPT, *supra* note 47, 38-39.

320 *See generally* Czekis, *supra* note 313.

321 *See generally Id.*

322 *See Id.* at 1-2.

With a Deniable Operating System, TrueCrypt sets up a partition for a regular operating system which will be used only with less sensitive data and may serve as a decoy. [323] This regular operating system is encrypted by TrueCrypt with a password, but is not meant to [*572] be denied. [324] The program also sets up another partition that contains an outer volume along with a hidden volume and a hidden operating system. [325] The outer volume is protected by a different password and is not meant to be denied, while the hidden volume is protected, along with the hidden operating system, by a third password. [326] The user should be able to reveal the password for the decoy operating system and the outer volume on the second partition while still concealing the existence, much less the password, for the hidden volume. [327] Because the hidden volume is only accessed by the hidden operating system, it avoids many of the data leakage problems which are endemic to deniable file systems. [328] It may create other unusual indictors, which could arouse suspicion that additional data is being concealed. [329] For instance, it is unusual, even if there are some plausible reasons for it, to have two partitions protected by encryption on a single drive. [330] Whether it is hidden as a deniable file system or with a hidden operating system, the significant part of both forms of deniable encryption is that they possess a hidden volume whose existence can be concealed even while supplying one of the passwords.

For an analogy, if the outer encrypted file is a safe, then the hidden volume is the locked, false bottom inside the safe. This presents a somewhat different case than examining a simple encrypted file, which may be decrypted in its entirety with one password. Even if the prosecutor can establish that they know the existence, location, and authenticity of the outer encrypted file and may even have substantial knowledge of the contents, they may not know of the existence of the inner hidden volume. If a prosecutor knows through other evidence, [*573] such as an overheard conversation or leakage of data from applications, that there is a hidden volume on the drive, they still may not be able to establish with reasonable particularity that they know where it is. For instance, if there are multiple encrypted files capable of housing a hidden volume, the prosecutor is unlikely to know which of those encrypted files stores the hidden volume even if they have knowledge of the existence of a hidden volume.

If a prosecutor knows of the existence of a hidden volume within a particular encrypted file system, then whether or not the prosecutor can demand decryption may depend on the standard used. Under the standard proposed in this paper, that would be sufficient and the prosecutor would be able to demand decryption of the file. Under the standard as articulated by the Eleventh Circuit, this would likely not be sufficient, but the prosecutor could remedy that if they could show some knowledge of the actual contents of that hidden volume. [331] However, if the prosecutor merely knows that a hidden volume is used with a machine but it may be in any of several encrypted files associated with that machine than this is unlikely to be sufficient to satisfy the foregone conclusion doctrine

---

[323] TRUECRYPT, *supra* note 47, 47-48.

[324] *Id.*

[325] *Id.*

[326] *Id.*

[327] *Id.*

[328] *Id.*

[329] TRUECRYPT, *supra* note 47, 47-48.

[330] *Id* at 50. Some of the plausible reasons are helpfully given in the documentation for users of the system to learn. *Id* at 51-52. For instance, they list the fact that the user may elect to use a stronger cascade encryption algorithm on highly sensitive data while using a faster non-cascade encryption on the part of the hard drive which stores the operating system and applications. *Id.* These explanations do provide plausible reasons for the setup, but the existence of that configuration would appear unusual and raise questions to those who are knowledgeable about encryption and deniable operating systems. *Id.*

[331] *See supra* Part III.

even under a broad standard. It may not be sufficient to meet the standard even if the prosecutor has some knowledge of what files they expect to find. In that situation, they would not be able to show that it knew the location of the requested files with reasonable particularity.

It is most likely that demanding that the defendant turn over the unencrypted contents would not compel them to reveal the existence or the contents of a hidden volume unless that was specified with sufficient particularity. Although the hidden volume is, in a sense, within the encrypted volume, there is a sense in which it is separate and distinct from it. The hidden volume is tracked and handled separately by the encryption software and is mounted [332] separately by the operating system. Even if the prosecution later discovers the existence of the hidden file system, it is likely that it would not be able to sustain a perjury charge or other remedy [333] since the defendant could say that the hidden volume is a separate entity from the one the [*574] prosecutor and court identified in the subpoena or warrant, and in a technological sense this would be true. [334] Thus, even under compulsion to provide decryption, a defendant is likely entitled to conceal the existence of the hidden volume unless and until the prosecutor can establish that it exists.

VII. CONCLUSION

In order to best protect the interests of the public in retaining their right to avoid incriminating themselves while providing the prosecution with the evidence it needs, the foregone conclusion doctrine should be read broadly when determining if the defendant can be compelled to decrypt files that are already in the prosecution's possessions. As the test requires, the prosecution must establish that it knows with reasonable particularity the existence and location of the data that it seeks, and that it can authenticate the encrypted documents or devices independently. But, this test should be met when the prosecution can show the location and existence of the encrypted files along with showing that the defendant is actually capable of decrypting the files, and that it will be able to authenticate the files. In particular, the prosecution should not have to, and the line of cases from the Supreme Court does not require the prosecution to, demonstrate knowledge of the actual contents of the encrypted files. After receiving the unencrypted version, the prosecution should be banned from using the defendant's act of decrypting or producing the unencrypting version against them but allowed to use the recovered documents. This best provides the prosecution with evidence to which it should be entitled, while respecting the Fifth Amendment rights of the defendant.

This standard should also apply to data which is protected by steganography or deniable encryption. However, their nature as hidden information may make it substantially harder for the prosecution to show that it has knowledge with reasonable particularity of either the location or the existence of files protected in this way. As an extension of that fact, a subpoena compelling a person to produce an unencrypted version of an encrypted file should be satisfied by the production of the unencrypted form of the outer layer when deniable encryption has been used to create a hidden volume. To get an unencrypted copy of the contents of a hidden volume, the [*575] prosecution must specify that they wants the contents from the hidden volume in the subpoena after establishing that it knows the existence and location of the hidden

---

[332] Mounting refers to the operating system making a drive or portion of a drive accessible and active. *Mount*, TECHTERMS, http://www.techterms.com/definition/mount (last accessed Aug. 22, 2014).

[333] Though, depending on the standards being used, the prosecutor may then be able to acquire court authorization to compel the decryption of the inner volume since the prosecution would then know if its existence and location.

[334] *See* TRUECRYPT, *supra* note 47, at 38-39. The hidden volume encompasses a separate space from the standard volume and even has a separate header. The fact that this separate space is located where some of the free space for the standard volume would have been if the hidden volume did not exist does not change this fact. *Id.*

End of Document