Brooklyn Law Review

Volume 75 | Issue 1 Article 7

2009

Lessons from the British and American Approaches to Compelled Decryption

Brendan M. Palfreyman

Lessons from the British and American Approaches to Compelled Decryption

As society careens faster and faster into the digital age, the amount of information stored electronically will only continue to grow.[1] This proliferation of electronic storage has given rise to new threats to data security, both legal and illegal.[2] To protect against these extrinsic threats, people have increasingly turned to data encryption, a process that renders data unintelligible to unauthorized viewers.[3] Due to the limits of current technology, encryption software programs, some of which are available free to the public,[4] can render data virtually indecipherable without access to the appropriate encryption key or password.[5] Encryption is a "double-edged

---

[1] The amount of data stored electronically has grown exponentially in the last several decades. *See generally* Larry Swezey, *It's Happening Now: This Is the Tera Era of Data Storage*, COMPUTER TECH. REV., Sept. 16, 2008, http://www.wwpi.com/index.php?view=article&id=6146.

[2] Illegal threats to electronically stored data include identity theft, corporate espionage, phishing, etc. *See generally* Terrence Berg, *The Changing Face of Cybercrime: New Internet Threats Create Challenges to Law Enforcement*, 86 MICH. B.J. 18, 18 (2007).

[3] *See generally infra* note 14; *see also* Press Release, PGP Corp., Aberdeen Group Research Reveals Increased Use of Encryption by Top Performing, Best-in-Class Companies (Nov. 20, 2008), *available at* http://www.pgp.com/insight/newsroom/press_releases/aberdeen_group_research.html ("[T]he use of encryption to protect sensitive data in the enterprise is becoming even more pervasive . . . .").

[4] A powerful encryption software program, named TrueCrypt, can be downloaded free of charge at the TrueCrypt web site. TrueCrypt, Downloads, http://www.truecrypt.org/downloads (last visited Aug. 28, 2009).

[5] In *In re Grand Jury Subpoena to Boucher*, with regard to the government's efforts to decrypt seized encrypted files, a Secret Service agent testified "that it is nearly impossible to access these encrypted files without knowing the password. . . . The only way to get access without the password is to use an automated system which repeatedly guesses passwords. According to the government, the process . . . could take years . . . ." *In re* Grand Jury Subpoena to Boucher (*Boucher I*), No. 2:06-mj-91, 2007 WL 4246473, at *2 (D. Vt. Nov. 29, 2007), *rev'd*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009); *see also* D. Forest Wolfe, *The Government's Right to Read: Maintaining State Access to Digital Data in the Age of Impenetrable Encryption*, 49 EMORY L.J. 711, 712 (2000) ("Modern computerized cryptography uses encryption algorithms to keep digital information private, and the most complex of these algorithms can encode data so thoroughly that it would take millennia to decipher it with current technology." (citations omitted)); *see infra* Part II.B. Of course, future

sword," and can be used by criminals and ordinary citizens alike.[6] This presents a major dilemma for law enforcement officials, who, without the proper legal mechanisms, would be practically powerless to gather electronic evidence in the face of widespread encryption.[7]

Because the trend towards the ever increasing use of data encryption is not confined to the United States, the aforementioned dilemma is an issue for law enforcement agencies around the world. Despite being faced with the same problem, countries have adopted different solutions. In particular, the United States and Great Britain have approached the dilemma in vastly different fashions.

Great Britain has taken a direct, and decidedly pro-law enforcement, approach. Under Part III of the Regulation of Investigatory Powers Act ("RIPA"), various British governmental actors are empowered to compel decryption and criminally charge citizens who refuse to comply.[8] This statute has drawn criticism from a variety of groups, ranging from civil rights activists to citizens concerned about the deleterious effect the statute could have on the British economy.[9]

The United States has adopted an entirely different approach.[10] Unlike Great Britain, the United States has, as of now, declined to statutorily grant law enforcement the power to compel decryption.[11] Due to this lack of statutory guidance, the issue of compelled decryption has been left to the judiciary. Although case law on the subject is extremely limited, at least one early decision has analyzed this problem under Fifth

---

advances in technology are hard to predict, and there could be major advances in either encryption or encryption-cracking technology. It is part of an ongoing struggle between those creating more powerful encryption and those creating more powerful computers to break encryption. *See* Dawn Walton, *A Quantum Leap in Information Security*, GLOBE & MAIL, Apr. 3, 2007, at B9 (discussing a very advanced form of encryption in development called quantum cryptography).

[6] Press Release, U.S. Senator Patrick Leahy, Statement at Hearing of Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information on "The Encryption Debate: Criminals, Terrorists, And the Security Needs of Business and Industry" (Sept. 3, 1997), *available at* http://leahy.senate.gov/press/199709/970903.html ("As with other dual-use technologies, encryption has both good and bad uses.").

[7] *Infra* Part I.B.

[8] Regulation of Investigatory Powers Act, 2000, ch. 23, §§ 49-56 (Eng.).

[9] *See infra* Part IV.A.

[10] Jeffrey Yeates, *CALEA and the RIPA: The U.S. and the U.K. Responses to Wiretapping in an Increasingly Wireless World*, 12 ALB. L.J. SCI. & TECH. 125, 141 (2001) ("Significantly, [under CALEA] telecom carriers have no responsibility to decrypt any encrypted communications or ensure that law enforcement can do so.").

[11] *See generally id*.

Amendment jurisprudence.[12] In *In re Grand Jury Subpoena to Boucher*, a magistrate judge in the District of Vermont ruled that the federal government could not compel a citizen to turn over his encryption password because doing so would infringe upon his Fifth Amendment privilege against self-incrimination.[13]

Both approaches are decidedly problematic, albeit in different ways. The British approach, while highly protective of law enforcement interests, encroaches too far on individual civil liberties. The American approach, as typified by *Boucher*, while adequately protecting civil liberties, leaves the government without the proper tools to effectively fight crime in a digital age. The consequences of the ubiquitous use of unbreakable encryption by criminals like terrorists, hackers, child pornographers, and members of organized crime syndicates, to name a few, would be devastating.[14] This Note

---

[12] The first case, as far as my research has revealed, to deal with this issue is *In re Grand Jury Subpoena to Boucher*, which analyzed the issue under Fifth Amendment jurisprudence. *In re* Grand Jury Subpoena to Boucher (*Boucher I*), No. 2:06-mj-91, 2007 WL 4246473, at *2 (D. Vt. Nov. 29, 2007), *rev'd*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009). Notably, on February 19, 2009, the decision was reversed by District Judge William K. Sessions on narrow grounds. *In re* Grand Jury Subpoena to Boucher (*Boucher II*), No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009); *see also infra* note 50. Judge Sessions held that, due to a body of law called the foregone conclusion doctrine, the defendant would not be able to resist the governmental order to turn over his password. *Boucher II*, 2009 WL 424718, at *3-4; *see also infra* notes 104-111 and accompanying text. This narrow holding does not alter the following analysis because where the foregone conclusion doctrine does not apply, defendants could still seek refuge in the Fifth Amendment.

[13] *Boucher II*, 2009 WL 424718, at *3.

[14] In a 1997 press release, Senator Patrick Leahy (D-VT) stated,

> We are all acutely aware of, and concerned about, the "bad" uses of encryption by criminals, who want to thwart police surveillance of their criminal activities, and by spies, who engage in activities harmful to our national security. The Working Group report contains startling estimates of 50 to 100 percent in the future annual growth rates for criminal uses of encryption. Even if the impact on law enforcement is not great now, the potential future impact is alarming.

Press Release, U.S. Senator Patrick Leahy, Statement at Hearing of Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information on "The Encryption Debate: Criminals, Terrorists, And the Security Needs of Business and Industry" (Sept. 3, 1997), *available at* http://leahy.senate.gov/press/199709/970903.html; s*ee also Security and Freedom through Encryption (SAFE) Act: Hearing on H.R. 850 Before the H. Armed Servs. Comm.*, 106th Cong. (1999) (statement of Janet Reno, Att'y Gen. of the United States), *available at* http://www.usdoj.gov/archive/ag/testimony/1999/agarmed071399.htm ("[I]t will become far more difficult for the FBI, DEA, and other federal, state, and local, law enforcement agencies, faced with the rising threat from the criminal use of commercially available encryption, to protect the public from crimes such as terrorism, narcotics trafficking, economic fraud, and child pornography.").

examines both methods and argues that America should devise a new approach by drawing upon the strengths of each tack and devise a middle ground that provides for both effective law enforcement and adequate protection of civil liberties.

Part I of this Note briefly describes the history and technical background of encryption. Then, Part II discusses the American approach to compelled decryption and the application of the Fifth Amendment, while Part III analyzes the British approach of statutorily compelled decryption. Next, Part IV discusses the criticisms levied at both of the approaches and proposes a statutory middle ground based, in part, on the federal wiretap statute in the Omnibus Crime Control Statute. Finally, the Note concludes with a reiteration of the notion that both approaches have fundamental flaws and that American policy makers should consider adopting a middle ground.

I. HISTORY AND TECHNICAL BACKGROUND OF ENCRYPTION

The goal of encryption is to safeguard important data from unauthorized viewing by third parties.[15] Although modern encryption in its digital form is a relatively recent innovation, more primitive forms have been in existence for thousands of years.[16] With the passage of time and advances in technology, encryption techniques have grown immensely more sophisticated.[17] Currently, freely available software can render data virtually undecipherable without the proper password or encryption key.[18]

A. History and Background of Encryption

Cryptography, the science of secret writing,[19] is the means by which parties can safeguard their important information by preventing unauthorized access. In order to keep information secret, a party will encrypt it, which is the method by which a message is rendered undecipherable to third parties, and in order for the authorized party to read the

---

[15] *See infra* text accompanying notes 19-20, 24-27.

[16] *See infra* text accompanying notes 24-27.

[17] *See* Part I.B.

[18] *See supra* note 4.

[19] THE AMERICAN HERITAGE DICTIONARY OF ENGLISH LANGUAGE 439 (Houghton Mifflin Co., 4th ed. 2000) (defining cryptography as "1. The process or skill of communicating in or deciphering secret writings or ciphers. 2. Secret writing.").

hidden message, it must be decrypted, which is the method by which a secret message is turned into regular text.[20] Depending on whether the data is encrypted or decrypted, it is referred to as "plaintext" or "ciphertext." Plaintext is the underlying information that is being encrypted—i.e., the secret message or document that is meant to be protected.[21] Ciphertext is the product of the encryption—i.e., the undecipherable text in which the message is hidden.[22] Anyone wishing to uncover the secret message, including governments acting in their criminal investigatory capacities, will be after the underlying data, i.e., the plaintext.[23]

States and individuals have relied on cryptography to safeguard critical information and communications throughout history. A primitive example of the practice, reported by Greek historian Herodotus, involved the tattooing of a secret message on the scalp of a slave, allowing the slave's hair to grow back, and then sending the slave to the recipient of the message so that his head could be shaved and the secret message revealed.[24] Julius Caesar employed a slightly more advanced method of cryptography in ancient Roman times.[25] Fearing that his military communiqués would be intercepted, Caesar employed the simple cryptographic process of shifting every letter in the alphabet up three steps, such that a "B" would become a "E," and a "P" would become an "S."[26] Since the days of Herodotus and Julius Caesar, encryption methods have evolved from simple ciphers, to complex mechanical devices,[27]

---

[20] *Id.* at 589 (defining encrypt as "[t]o alter (a file, for example) using a secret code so as to be unintelligible to unauthorized parties"). *Id*. at 473 (defining decryption as "[a] deciphered or decoded message").

[21] Phillip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171, 172 n.8 (1996) ("'Plaintext' is unencrypted or decrypted text; 'ciphertext' is encrypted text.").

[22] *Id.*

[23] The government, in attempting to acquire criminal evidence where encryption has been utilized, will seek to gain either the plaintext, or the encryption key/password so that they can decipher the ciphertext on their own. Reitinger, *supra* note 21, at 175. Regardless, the ultimate aim of the government is to uncover the underlying data, i.e., the plaintext.

[24] HERODOTUS, 3 THE HISTORY OF HERODOTUS 197 (George Rawlinson trans., D. Appleton & Co. 1889) ("Thus accordingly he did; and as soon as ever the hair was grown, he despatched the man to Miletus giving him no other message than this—'When thou art come to Miletus, bid Aristagoras shave thy head and look thereon.'").

[25] Adam C. Bonin, *Protecting Protection: First and Fifth Amendment Challenges to Cryptography Regulation*, 1996 U. CHI. LEGAL F. 495, 497 (1996).

[26] *Id.*

[27] *See* Aaron M. Clemens, *No Computer Exception to the Constitution: The Fifth Amendment Protects Against Compelled Production of an Encrypted Document or*

and finally to digital encryption of electronic data. Today, electronic encryption has become standard practice for governments, corporations, and, to a somewhat lesser extent, individuals.[28]

B. Technical Background

Although the basic idea of cryptography is simple, in fact it can be a quite complex process. As one might suspect, in today's digital world, ciphers are no longer created and decoded simply by tattooing or transcribing letters. Rather, quite intricate methods are required to encrypt and decrypt messages.

First, in order to decrypt information that has been encrypted using modern techniques, an "encryption key" is needed. An encryption key is essentially a very long string of numbers whose length makes it extremely hard to memorize.[29] Users of encryption software generally do not have to remember this long number and, instead, can enter a more easily remembered password or passphrase, which in turn activates the encryption key.[30] Thus, when the government seeks to compel an ordinary citizen to turn over the means by which he can decrypt the data, the disclosure order will

---

Private Key, 8 UCLA J.L. & TECH. 2, 4 n.26 (2004) (describing the German Enigma machine).

[28] *See* David B. Walker, *Privacy in the Digital Age: Encryption Policy—A Call for Congressional Action*, 1999 STAN. TECH. L. REV. 3, 14 (1999) ("Encryption is becoming a central fixture in the burgeoning electronic commerce industry."). *See generally* Declan McCullagh, CNET NEWS, *Obama's New BlackBerry: The NSA's Secure PDA?*, Jan. 13, 2009, http://news.cnet.com/obamas-new-blackberry-the-nsas-secure-pda/ (discussing balancing President-Elect Barack Obama's desire to continue using his mobile email device with the paramount need to encrypt sensitive data).

[29] Anoop MS, *Public Key Cryptography: Applications Algorithms and Mathematical Explanations* 2 (2007), *available at* http://www.tataelxsi.com/whitepapers/pub_key2.pdf?pdf_id=public_key_TEL.pdf [hereinafter *Public Key Cryptography*] ("The public key algorithms operate on sufficiently large numbers to make [deriving the private key from the public key] practically impossible and thus make the system secure. For example, RSA algorithm operates on large numbers of thousands of bits long."); *see also* Reitinger, *supra* note 21, at 174 ("For example, the widely used Data Encryption Standard ("DES") algorithm uses a single key fifty-six bits in length—up to more than 70,000,000,000,000,000 in decimal notation—for both encryption and decryption. Public-key algorithms use different keys for encryption and decryption, and much longer keys, such as 512 (and greater) bit numbers—over 150 decimal digits." (footnote omitted)).

[30] Such a password would be similar to the password used to log into an email account, or the pin number used to access a bank account at an ATM.

typically compel him to turn over his password rather than the encryption key.[31]

There are two methods of using encryption keys—public key encryption and private key encryption. Historically, most encryption was accomplished via the private key method. In the simplest of terms, a private key system involves one key that is used for both encrypting and decrypting the encoded message.[32] The sender uses a certain key to encrypt the message, and the receiver uses that same key to decrypt it.[33]

In 1976[34] Whitfield Diffie and Martin Hellman proposed a new method of encryption: public key encryption.[35] In this system, there are two keys, a public key, which is used for encryption, and a private key, which is used for decryption.[36] The public key is available to the public at large, and the private key is known only to the person using the encryption.[37] Thus, for example, if one wishes to send a secure message using this type of encryption, he would encrypt the message using a public key, send it, and then the recipient would decrypt the message using her private key.[38] One hoping to intercept and decrypt this message would be unable to do so using only the public key because it is a "computationally infeasible" task to derive the private key from the public key.[39] In other words, the reason it is difficult to break strong encryption is that while it is a simple task to compute the public key from the private key, it is extremely difficult to do the opposite and derive the private key from the public key.[40]

---

[31] This was the case in *Boucher*. The government sought to force Mr. Boucher to turn over his encryption password. *See In re* Grand Jury Subpoena to Boucher (*Boucher I*), No. 2:06-mj-91, 2007 WL 4246473, at *2 (D. Vt. Nov. 29, 2007), *rev'd*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

[32] Wolfe, *supra* note 5, at 715.

[33] *Id.*

[34] Public key encryption was actually invented earlier than 1976 by members of the British Government Communications Headquarters, but their findings were not disclosed. Martin Campbell-Kelly, *Not All Bad: An Historical Perspective on Software Patents*, 11 MICH. TELECOMM. & TECH. L. REV. 191, 230 (2005).

[35] Whitfield Diffie & Martin E. Hellman, *New Directions in Cryptography*, 12 IEEE TRANSACTIONS ON INFO. THEORY 644 (1976).

[36] *Public Key Cryptography*, *supra* note 29, at 3.

[37] *Id.*

[38] *Id.*

[39] Diffie & Hellman, *supra* note 35, at 644.

[40] *Public Key Cryptography*, *supra* note 29, at 1-2. It is a computationally infeasible task to derive the private key because:

> The private and public key of a device is related by the mathematical function called the one-way function. One-way functions are mathematical

This is known as a "one-way function" because it is only easily solvable in one direction.[41] The only way to ascertain the private key in such circumstances is to use a specialized computer program that guesses, one at a time, the correct number.[42] This process can take an exceptionally long time.[43] Thus, it is virtually impossible to break strong public key encryption without compelling, or otherwise obtaining, access to the private key.[44]

II. THE AMERICAN APPROACH TO COMPELLED KEY DISCLOSURE

Encryption technology is a double-edged sword and, as such, can be utilized by criminals to shield evidence from governments.[45] Unlike Great Britain, which has dealt with the issue statutorily,[46] Congress has thus far declined to pass a statute directly addressing the issue of compelled decryption.[47] Thus, the problem has been left to the judiciary, and there it has been examined under Fifth Amendment jurisprudence.

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

Id.

[41] *Id.*

[42] *See supra* note 5 and accompanying text.

[43] *Id.*

[44] *See supra* text accompanying notes 41-44.

[45] *See supra* note 6.

[46] The Regulation of Investigatory Powers Act was passed in 2000. Regulation of Investigatory Powers Act, ch. 23, §§ 49-56.

[47] Congress had an opportunity to address the issue of compelled decryption in the Communications Assistance for Law Enforcement Act ("CALEA"). 47 U.S.C. §§ 1001-1010 (2006). The only section that references encryption merely states that telecommunications providers will not be responsible for decrypting any encrypted information that happens to moving over its lines. *Id.* § 1002(b)(3) ("A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication."). Therefore, unlike its British counterpart, CALEA does not contain any language compelling individuals to decrypt their encrypted data. *See generally* RIPA, 2000, ch. 23 (Eng.).

A. Fifth Amendment Analysis

The first federal case to directly touch upon the issue of compelled decryption is *In re Grand Jury Subpoena to Boucher*, handed down in the Federal District Court of Vermont on November 29th, 2007.[48] In *Boucher*, Magistrate Judge Jerome J. Niedermeier held that the act of being compelled to turn over an encryption password has testimonial aspects.[49] As a result, the defendant was allowed to refuse to surrender his password under protection of the Fifth Amendment right to refrain from testimonial self-incrimination.[50] This case forms the basis of the American approach to compelled decryption under Fifth Amendment jurisprudence.

Early American legislators were so opposed to the ancient English system, in which admissions of guilt won under torture were admissible, that they made the right against self-incrimination a cornerstone of the Bill of Rights.[51]

---

[48] *See In re* Grand Jury Subpoena to Boucher (*Boucher I*), No. 2:06-mj-91, 2007 WL 4246473 (D. Vt. Nov. 29, 2007), *rev'd*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

[49] *Id.* at *3.

[50] *Id.* at *3-4. The holding of *Boucher* was reversed on narrow grounds by the District Court of Vermont. *In re* Grand Jury Subpoena to Boucher (*Boucher II*), No. 2:06-mj-91, 2009 WL 424718, at *3-4 (D. Vt. Feb. 19, 2009). Judge William K. Sessions reversed Judge Niedermeier's opinion on the grounds that the foregone conclusion doctrine precluded the use of Fifth Amendment protection. *Id.* As discussed later, in being forced to turn over a password, a defendant makes three implicit assertions which may be incriminating: that the sought after files exist, that they are authentic, and that the defendant has control over the files. *See infra* text accompanying notes 64-65. When the government is already aware of these three facts, a defendant is not able to seek refuge in the Fifth Amendment because the incriminating information that would be produced is a foregone conclusion. *See infra* text accompanying notes 104-105.

In *Boucher*, when Sebastien Boucher came over the border, his hard drive was unencrypted and government agents were able to view the files, thus learning of the existence of the purported child pornography. *Boucher II*, 2009 WL 424718, at *3-4. Further, in admitting that the computer was his, Boucher communicated to the government that the files were under his control and authentic. *Id.* at *4. Thus, the implicit assertions were foregone conclusions, and Judge Sessions ordered Boucher to comply with the order. *Id.*

This reversal does not alter the fundamental analysis presented here. It is easy to imagine a situation where the existence, authenticity, and control over a file or files were not a foregone conclusion. For example, the government could raid the headquarters of a criminal enterprise and find several encrypted hard drives. Because the hard drives were encrypted and the government never had initial access, a defendant ordered to turn over the password to these hard drives could potentially refuse to comply under the Fifth Amendment because the foregone conclusion doctrine would not apply.

[51] *See* Brown v. Walker, 161 U.S. 591, 597 (1896) ("So deeply did the iniquities of the ancient system impress themselves upon the minds of the American colonists that the States, with one accord, made a denial of the right to question an accused person a part of their fundamental law, so that a maxim, which in England

The Fifth Amendment states, "No person shall . . . be compelled in any criminal case to be a witness against himself."[52] This right against self-incrimination is not, however, absolute. In order for Fifth Amendment protection to attach, three prerequisites must be met: (1) the disclosure must be testimonial,[53] (2) the disclosure must be compelled,[54] and (3) it must be possible that criminal liability could result.[55] In the vast majority of criminal cases where the government is seeking an encryption key or password, that disclosure is being compelled and criminal liability could result, thus typically leaving only the question of whether disclosing the encryption key is testimonial in nature.[56]

A communication is considered testimonial when it "explicitly or implicitly, relate[s] a factual assertion or disclose[s] information."[57] Conversely, the Supreme Court has held that a communication is non-testimonial when the suspect is "not required 'to disclose any knowledge he might have,' or

---

was a mere rule of evidence, became clothed in this country with the impregnability of a constitutional enactment.").

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

[53] Fisher v. United States, 425 U.S. 391, 408 (1976) ("Fifth Amendment . . . applies only when the accused is compelled to make a *testimonial* communication that is *incriminating*." (second emphasis added)).

[54] *Id*. at 409 ("A subpoena served on a [person] requiring him to produce [documents] in his possession without doubt involves substantial compulsion."); *see also Boucher I*, 2007 WL 4246473, at *2 ("Subpoenas require compliance and therefore constitute compulsion.").

[55] Generally, Fifth Amendment protection does not attach unless there is the possibility that criminal sanctions could result. *Fisher*, 425 U.S. at 408 ("Fifth Amendment . . . applies only when the accused is compelled to make a *testimonial* communication that is incriminating."). Hence, if a suspect is granted complete immunity, he cannot seek refuge in the Fifth Amendment. United States v. Rose, 806 F.2d 931, 932 (9th Cir. 1986) ("The federal grant of use immunity is sufficient to overcome the Fifth Amendment privilege against self-incrimination."). More specifically, as a matter of common sense, encrypted information being sought by the government in its investigative capacity will likely be incriminating. In *Boucher*, the judge noted, "Because the files sought by the government allegedly contain child pornography, the entry of the password would be incriminating." *Boucher I*, 2007 WL 4246473, at *2.

[56] *See Boucher I*, 2007 WL 4246473, at *2. Generally, the plaintext which is hidden by the encryption would not be protected by the Fifth Amendment, because in most cases such plaintext would be voluntarily prepared, and thus would not be a testimonial statement afforded protection under the Fifth Amendment. Reitinger, *supra* note 21, at 178 ("[I]f law enforcement subpoenas information that I have encrypted, I must produce the information in plaintext if it remains available to me in that form, assuming I have no other proper objection, such as my privilege against self-incrimination").

[57] Doe v. United States, 487 U.S. 201, 210 (1988).

'to speak his guilt.'"[58] There are a number of compelled disclosures that are non-testimonial and thus do *not* violate the Fifth Amendment, including taking blood samples, taking fingerprints, taking voice and handwriting exemplars, compelling someone to wear particular clothing, and forcing someone to stand in a lineup.[59]

Typically, the contents of a document or hard drive will not be protected by the Fifth Amendment.[60] Nevertheless, in certain circumstances the very act of turning over a document or providing a password to an encrypted hard drive will implicitly communicate incriminating facts and hence will be protected.[61] In *Fisher v. United States*, the government sought to compel the production of certain incriminating documents, and the defendant refused to comply on the grounds that the act of producing the documents would constitute self-incrimination.[62] Although the documents themselves were voluntarily prepared and were therefore not protected, the defendants argued that the act of production implicitly asserted incriminating facts and should be protected by the Fifth Amendment.[63] Justice White's majority opinion for the Supreme Court held that complying with a subpoena to produce documents could implicitly communicate three facts: that the documents exist,[64] that they are in the control of the accused, and that the papers are authentic.[65] This is sometimes referred to as the "act of production doctrine."[66] Applying this

---

[58] *Id.* at 210 (quoting United States v. Wade, 388 U.S. 218, 222-23 (1967); *see also* Holt v. United States, 218 U.S. 245, 252-53 ("[T]he prohibition of compelling a man in a criminal court to be witness against himself is a prohibition of the use of physical or moral compulsion to extort communications from him, not an exclusion of his body as evidence when it may be material.").

[59] Doe v. United States, 487 U.S. at 210.

[60] *Boucher I*, 2007 WL 4246473, at *2.

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

[62] Fisher v. United States, 425 U.S. 391, 409-12 (1976).

[63] *Id.* at 410-11.

[64] The first element, that the documents actually exist, is interesting with regard to encryption software programs, such as TrueCrypt, which specifically market the ability to hide even the fact that the encrypted files even exist within the ciphertext. TrueCrypt, *Plausible Deniability*, Hidden Volume, http://www.truecrypt.org/docs/?s=plausible-deniability (last visited Aug. 29, 2009).

[65] *Fisher*, 425 U.S. at 410 ("Compliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer. It also would indicate the taxpayer's belief that the papers are those described in the subpoena."); *see also* Clemens, *supra* note 27, at 11-12 (discussing the application of the three *Fisher* prongs to encryption key disclosure).

[66] *See* Reitinger, *supra* note 21, at 180. Notably, turning over an encryption password would not be explicitly incriminating, unless the password itself

doctrine to compelled decryption, it can be argued that being forced to turn over a password would implicitly communicate that the electronic files that the government is seeking exist, that the defendant actually has control over and access to the files, and that the electronic files are authentic. This is the defense that Sebastien Boucher raised when the government attempted to compel him to turn over his password in *Boucher*.[67]

Nevertheless, the government may be able to draft a subpoena compelling disclosure in a manner such that the testimonial aspects of the act of production are not implicated. In such circumstances, the protection against self incrimination would not attach and the defendant would be left no recourse save compliance. This was the case in *Doe v. United States*.[68] There, the government subpoenaed bank records for several accounts in the Cayman Islands and Bermuda.[69] The unnamed defendant failed to respond to the subpoena, and so the government attempted to force the defendant to sign a number of release forms that would allow the banks to turn over the records.[70] The defendant claimed Fifth Amendment protection.[71] The Supreme Court held that the forms the defendant was asked to sign spoke only in the hypothetical, and, that because of the non-specific way in which they were drafted, signing them did not acknowledge the existence of, or control over, any account, or communicate the authenticity of any records.[72] Thus, the three implicit assertions about which the *Fisher* Court was concerned were not implicated, and the defendant was not entitled to Fifth Amendment protection.

---

communicated some incriminating fact, for example, if, in a child pornography case, the password was "iluvyoungkidz."

[67] *In re* Boucher (*Boucher I*), No. 2:06-mj-91, 2007 WL 4246473, at *3 (D. Vt. Nov. 29, 2007), *rev'd*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

[68] Doe v. United States, 487 U.S. 201, 218 (1988).

[69] *Id.* at 202-03.

[70] *Id.* at 203.

[71] *Id.* at 203-04.

[72] *Id.* at 215-16 ("It is carefully drafted not to make reference to a specific account, but only to speak in the hypothetical. Thus, the form does not acknowledge that an account in a foreign financial institution is in existence or that it is controlled by petitioner. . . . Nor would his execution of the form admit the authenticity of any records produced by the bank.").

B. In re Boucher

Boucher is the first case to apply this Fifth Amendment logic to the issue of compelled decryption. On December 17, 2006, while crossing the border from Canada into the United States at the town of Derby Line, Vermont, Sebastian Boucher's car was pulled over and inspected by Customs and Border Protection agent Chris Pike.[73] While performing the inspection, Officer Pike noticed a laptop in the back seat, opened it, and was able to access the hard drive without entering a password.[74] After investigating the computer's contents, Officer Pike located approximately 40,000 images, some of which appeared to be pornographic.[75] When asked if any of the images contained child pornography, Boucher responded that he was not sure.[76] After discovering several file names that appeared to reference child pornography, Officer Pike called in Special Agent Mark Curtis of Immigration and Customs Enforcement.[77] During the course of his investigation, Agent Curtis found a file, entitled "2yo getting raped during diaper change."[78] Although Agent Curtis could tell that the file had been recently opened, he was unable to open it at that time.[79]

Boucher was then arrested and subsequently waived his *Miranda* rights.[80] When asked about the aforementioned file,

---

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

[74] *Id.* A reason that the officer may not have had to enter a password is that with most encryption software, when you simply close your laptop, thereby putting it to "sleep," instead of actually shutting it down, the encrypted drive will remain accessible without re-entering the password ("mounted"). *See* TrueCrypt, FAQ, http://www.truecrypt.org/faq.php (last visited Jan. 28, 2009) ("TrueCrypt automatically dismounts all mounted TrueCrypt volumes on system shutdown/restart."). Once the computer is shut down, the encrypted drive is dismounted and cannot be accessed again without entering the password. *Id.*

[75] *Boucher I*, 2007 WL 4246473, at *1.

[76] *Id.*

[77] *Id.*

[78] *Id.*

[79] *Id.*

[80] *Id.* The purpose of *Miranda* rights is to counteract the inherently coercive nature of custodial interrogation and protect the privilege against self incrimination. *See generally* Miranda v. Arizona, 384 U.S. 436, 444 (1966). "[T]he [suspect] must be warned that he has a right to remain silent, that any statement he does make may be used as evidence against him, and that he has a right to the presence of an attorney, either retained or appointed." *Id.* Here, Boucher waived his Miranda rights so the police were allowed to interrogate him without counsel present. *Boucher I*, 2007 WL 4246473, at *1. However, the Fifth Amendment can be invoked at anytime, so even

Boucher said that, because he downloaded many pornographic images, sometimes he would "unknowingly" download child pornography.[81] When he discovered the child pornography, Boucher claimed he would immediately delete the images.[82] Boucher then showed Agent Curtis the drive ("drive Z") on which he downloaded the pornography, and Agent Curtis discovered several "images and videos of child pornography in drive Z."[83] The laptop was shut down and seized.[84]

On December 29, 2006, Mike Touchette of the Vermont Department of Corrections restarted Boucher's computer, and made a mirror image copy of its hard drive.[85] However, Touchette was then unable to access drive Z because it had been encrypted using a software program named Pretty Good Privacy ("PGP").[86] In fact, because of this encryption, the government has not been able to view any of the files on drive Z since December 17, 2006, the day the laptop was seized.[87] In an attempt to gain access to the files, the government obtained a grand jury subpoena for the production of "all documents, whether in electronic or paper form, reflecting *any passwords* used or associated with the Alienware Notebook Computer . . . seized from Sebastien Boucher at the Port of Entry at Derby Line, Vermont on December 17, 2006."[88] Boucher motioned to quash the subpoena, claiming that the act of turning over the password violated his Fifth Amendment right against self-incrimination.[89]

In addressing the motion, Judge Niedermeier began his analysis with the conclusion that, because the subpoena sought to compel Boucher to enter his key for the purposes of subjecting Boucher to criminal liability, the self-incrimination issue turned entirely on whether this act was testimonial in nature.[90] He determined that entering the password "implicitly

---

though Boucher initially waived his rights, he is permitted to subsequently claim them at any later time. *Miranda*, 384 U.S. at 444-45.

[81] *Boucher I*, 2007 WL 4246473, at *1.

[82] *Id.*

[83] *Id.*

[84] *Id.*

[85] *Id.*

[86] *Id.*

[87] *See supra* Part I.B.

[88] *Boucher I*, 2007 WL 4246473, at *2 (emphasis added).

[89] *Id. See generally* Fisher v. United States, 425 U.S. 391 (1976).

[90] *See Boucher I*, 2007 WL 4246473, at *2 ("Because the files sought by the government allegedly contain child pornography, the entry of the password would be

communicates facts," and that if Boucher was forced to comply, he would "be faced with the forbidden trilemma; incriminate himself, lie under oath, or find himself in contempt of court."[91] Judge Niedermeier rejected the government's argument that, like signing the non-specific release forms at issue in *Doe*, the act of entering the password was non-testimonial.[92] He distinguished the two cases on the grounds that, in *Doe*, the Court found that no implicit facts would be communicated due to the artful drafting of the release form, whereas in the present case, entering the password would implicitly communicate that Mr. Boucher had access to the files.[93] According to Judge Niedermeier, in *Doe*, "the suspect was compelled to act to obtain access without indicating that he believed himself to have access. Here, when Boucher enters a password he indicates that he believes he has access."[94]

In an attempt to avoid a Fifth Amendment challenge, the government offered immunity specifically with regards to the act of producing the password, as opposed to immunity for any child pornography charge.[95] The government argued that a grant of immunity would permit compelled disclosure because the Fifth Amendment does not protect communications for which no criminal liability could result.[96] The Supreme Court passed on a similar government tactic in *United States v. Hubbell*.[97] There, the government subpoenaed documents from the defendant, and they were supplied after immunity was granted solely for the act of production.[98] After the defendant turned over the documents, the government sought to use them against him in an unrelated tax case.[99] The Supreme Court

---

incriminating. Whether the privilege against self incrimination applies therefore depends on whether the subpoena seeks testimonial communication.").

[91] *Id.* at *3 (citing Doe v. United States, 487 U.S. 201, 212 (1988)).

[92] *Id.*

[93] *See id.* at *4.

[94] *Id.*

[95] *Id.* The government was attempting to only grant use, and not derivative use, immunity. A grant of both "use" and "derivative use" immunity prevents the government from using a particular piece of the suspect's testimony against him, and from using any evidence which is derived only from that particular testimony. 22 C.J.S. *Criminal Law* § 98 (2009). In any event, use or derivative use immunity "is not full immunity from prosecution for the offense to which the compelled testimony relates, [as it] allows . . . a prosecution using evidence from legitimate independent sources." *Id.* (citations and footnotes omitted).

[96] *See Boucher I*, 2007 WL 4246473, at *4.

[97] 530 U.S. 27 (2000).

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

[99] *Id.* at 31-32.

rejected this tactic, holding that the grant of immunity for the production of the documents included immunity for any information that was derived from that act of production.[100]

Similarly, in *Boucher*, "the government offered not to use the production of the password against Boucher," and thus, in their eyes, "remove[d] the testimonial aspect from the" disclosure.[101] Judge Niedermeier disagreed and, relying on *Hubbell*, stated that the "testimonial aspect of the entry of the password precludes the use of the files themselves *as derivative of the compelled testimony*."[102] Thus, Judge Niedermeier concluded that the government's offer of immunity for the act of production was unavailing because obtaining the plaintext would be a derivative use of the compelled act.[103] Under the court's reasoning, immunizing a person solely for the act of typing in his encryption password would prevent the government from using the derivatively acquired plaintext in a criminal trial against him.

The government also argued that it should have access to the files under the "foregone conclusion" doctrine.[104] Under this doctrine, if the government is already aware of the existence and location of a particular document or file, and if producing the document or file would not "implicitly authenticate" it, then any evidence gained would be a foregone conclusion, and the suspect would not be entitled to Fifth Amendment protection.[105] Simply restated, if the act of production would not implicitly communicate the three *Fisher* elements because the government already could prove each of them, then the three assertions would be a foregone conclusion and Fifth Amendment protection would not attach. In *Boucher*, the government argued that because its agents were able to access drive Z and view child pornography before the computer was shutdown, it already knew the location and existence of at least some child pornography on Boucher's laptop and, thus, the foregone conclusion doctrine applied.[106]

---

[100] *Id.* at 40.

[101] *Boucher I*, 2007 WL 4246473, at *4.

[102] *Id.* at *5 (emphasis added).

[103] *Id.*

[104] *Id.* at *5-6. This is the argument Judge Sessions seized upon in reversing *Boucher I*. *See supra* note 50 and accompanying text.

[105] *See In re* Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d 87, 93-94 (2d Cir. 1993) (internal quotation marks omitted) (quoting United States v. Fox, 721 F.2d 32, 36 (2d Cir. 1983)).

[106] *See Boucher I*, 2007 WL 4246473, at *5-6.

Judge Niedermeier disagreed. With regard to turning over the files, he wrote that the government only knew the location of a couple of files, and that there was a lot of information on drive Z about which the government had no knowledge.[107] Because "the files the government has not seen could add much to the sum total of the government's information," Judge Niedermeier held that "the foregone conclusion doctrine [did] not apply."[108] With regard to solely turning over the password, Judge Niedermeier argued that "[t]he foregone conclusion doctrine does 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."[109]

In reversing Judge Niedermeier's holding, Judge Sessions seized upon the foregone conclusion doctrine and held that, because government agents were able to view the files before they were encrypted, and because Boucher admitted the laptop was his, the foregone conclusion doctrine did, in fact, apply.[110] Thus, Boucher was directed to comply with the order and turn over an unencrypted version of the Z drive.[111] Regardless, it is easy to imagine a scenario in which the foregone conclusion would not apply. For example, if agents seized an encrypted computer, but they were not sure if it belonged to a particular suspect, they would never have had access to the encrypted files, and they could not prove it was under the suspect's control. In such a situation, it is likely that the foregone conclusion doctrine would not apply, and a defendant could seek refuge in the Fifth Amendment.

Ultimately, Judge Niedermeier's opinion in *Boucher* exemplifies the American approach to the dilemma posed by powerful encryption: the idea that compelled password disclosure can have *Fisher*-like testimonial aspects, and thus Fifth Amendment protection can, in certain circumstances, be invoked to avoid compliance with a governmental order to turn over a password.

---

[107] *Id.* at *6.

[108] *Id.*

[109] *Id.*

[110] *In re* Grand Jury Subpoena to Boucher (*Boucher II*), No. 2:06-mj-91, 2009 WL 424718, at *3-4 (D. Vt. Feb. 19, 2009); *see also supra* note 50 and accompanying text. At least one commentator presaged this holding. *See* Posting of Orin Kerr to The Volokh Conspiracy, http://volokh.com (Dec. 19, 2007, 16:38).

[111] *Boucher II*, 2009 WL 424718, at *4.

III. THE BRITISH APPROACH TO COMPELLED KEY DISCLOSURE

Great Britain is one of the most heavily surveilled countries on the planet.[112] In 2006, there were an estimated 4.2 million closed circuit televisions in Britain, meaning there was roughly one surveillance camera for every fourteen people.[113] In light of the this, it is not surprising that, contrary to the American legislative avoidance of the issue, Great Britain enacted a statute which expressly permits the government to compel decryption.[114] This statute, the Regulation of Investigatory Powers Act ("RIPA"), empowers certain governmental actors, like the judiciary, high-level police, customs and excise officials, and military officers to compel decryption by threat of imprisonment and fines for noncompliance.[115]

A. Background of RIPA

As a member of the Council of Europe,[116] the United Kingdom and its laws are subject to the jurisdiction of the European Court of Human Rights ("ECHR").[117] In 1997, the ECHR held that Britain's then-applicable law on the interception of communications violated the European Human Rights Convention because it did not address "interceptions carried out over private communication networks."[118] In response, Great Britain passed the Regulation of Investigatory Powers Act ("RIPA").[119] RIPA was designed not only to comply with the ECHR decision, but also to address the rapid growth

---

[112] *See Britain is 'Surveillance Society,'* BBC NEWS, Nov. 2, 2006, http://news.bbc.co.uk/2/hi/uk_news/6108496.stm.

[113] *Id.*

[114] Regulation of Investigatory Powers Act, 2000, ch. 23 (Eng.).

[115] *Id.*

[116] Tarik Abdel-Monem, *Precedent of the European Convention on Human Rights to the CIA's High Value Detainees Program in and Through Europe*, 31 SUFFOLK TRANSNAT'L L. REV. 45, 52 n.38 (2007).

[117] European Court of Human Rights, How the Execution of Judgment Works, http://www.echr.coe.int/ECHR/EN/Header/The+Court/Execution/How+the+execution+of+judgments+wo-rks/ (last visited Jan. 28, 2009) ("The [parties] to the European Convention on Human Rights have committed themselves to secure to everyone within their jurisdiction the rights and freedoms defined in Section I of the Convention and, in this respect, have undertaken to 'abide by the final judgments of the Court in any case to which they are parties.'").

[118] Yeates, *supra* note 10, at 133.

[119] Regulation of Investigatory Powers Act, ch. 23.

of communications technology and the fervent desire of government officials to ensure that police agencies were able to keep up with this shifting landscape.[120]

The preamble of RIPA identifies the purposes of the Act, and specifically singles out encryption as a primary focus:

> An Act to make provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and *the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed* . . . .[121]

RIPA was passed by Parliament in 2000, and Part III of the Act, which addresses forced decryption, was put into effect in October of 2007.[122]

B. RIPA

1. Section 49

Part III of RIPA is entitled "Investigation of Electronic Data Protected by Encryption etc."[123] The statute lays out several important definitions. First, it defines a key as "any key, code, password, algorithm or other data the use of which (with or without other keys) . . . (a) allows access to the electronic data, or (b) facilitates the putting of the data into an intelligible form."[124] Protected information is "any electronic data which, without the key to the data . . . (a) cannot, or cannot readily, be accessed, or (b) cannot, or cannot readily, be put into an intelligible form."[125] Lastly, rendering a document into intelligible form requires putting the document "in the condition in which it was before an encryption or similar process was applied to it."[126]

Section 49 of Part III governs the conditions under which the British government is permitted to compel citizens to

---

[120] Yeates, *supra* note 10, at 134-38 (discussing in more depth the technological changes that led to the passage of both CALEA and the RIPA).

[121] Regulation of Investigatory Powers Act, ch. 23, §§ 49-56 (emphasis added).

[122] Jeremy Kirk, *Contested UK Encryption Disclosure Law Takes Effect*, WASH. POST, Oct. 1, 2007, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/10/01/AR2007100100511.html.

[123] Regulation of Investigatory Powers Act, ch. 23, §§ 49-56.

[124] *Id*. § 56(1).

[125] *Id.*

[126] *Id.* § 56(3).

turn over the plaintext of the requested encrypted documents.[127] Accordingly, the orders which the government employs to compel disclosure are known as "Section 49 Notices."[128] Notably, turning over the plaintext of an encrypted document is tantamount to divulging the encryption password because, if one is being forced to turn over the plaintext, one must enter the password against his will.[129]

Section 49 first requires that the ciphertext be obtained in a lawful manner.[130] There are several enumerated examples of how this can be done.[131] The two most prominent are when information has come into a government agent's possession either by "means of the exercise of a statutory power to seize, detain, inspect, search," or "by means of the exercise of any statutory power to intercept communications."[132] This includes the common situation in which information is seized pursuant to a judicial warrant.[133] The requirement to obtain the ciphertext in a lawful manner is important because it means that the British government is not permitted to compel decryption unless it has obtained possession of the encrypted information lawfully.[134] For example, if a police officer seized a computer without a valid warrant, the government would not have lawful possession of that computer, and thus could not compel plaintext disclosure.

In the ordinary case, a law enforcement agency will receive permission to issue a Section 49 notice from an official with the appropriate authorization, then serve the notice upon the target of the investigation. The recipient, in turn, must

---

[127] *Id.* § 49.

[128] *See* Home Office for Security and Counter Terrorism, Encryption, Disclosure of Keys, http://security.homeoffice.gov.uk/ripa/encryption/disclosure-of-keys/ (last visited Jan. 28, 2009).

[129] Additionally, there is a section in Part III which empowers the government to require that the key itself be turned over. Regulation of Investigatory Powers Act, ch. 23, § 51. The British government is more reluctant to compel disclosure of the actual key when the plaintext will suffice so it adds several extra burdens that must be met in order compel key disclosure as compared to plaintext disclosure. *See* Explanatory Notes to Regulation of Investigatory Powers Act, ¶ 272 (2000) [hereinafter Explanatory Notes].

[130] Regulation of Investigatory Powers Act, ch. 23, § 49(1); *see also* Explanatory Notes, *supra* note 129, ¶ 256.

[131] *Id*.

[132] *Id*. § 49(1)(a)-(b).

[133] Explanatory Notes, *supra* note 129, ¶ 256.

[134] Regulation of Investigatory Powers Act, ch. 23, § 49(1)(a)-(e).

hand over the requested plaintext within a reasonable amount of time.[135] Failure to comply is a crime.[136]

Subsection (2) of Section 49 places certain limiting factors on the ability of the government to compel decryption, and also references Schedule 2, which describes the governmental actors that have the authority to compel decryption.[137] First, the key must be in the possession of the person on whom the notice is being served.[138] Second, decryption can be compelled only if there is a specifically enumerated justification for doing so[139] (the acceptable justifications are delineated in subsection (3), discussed in the next paragraph).[140] Third, the "imposition of such [compelled disclosure must be] proportionate to what is sought to be achieved by its imposition."[141] Thus, the statute implements a balancing test in which the governmental interest in obtaining the plaintext must be equal to or greater than the interests of the individual seeking to prevent compelled decryption. Finally, it must not be "reasonably practicable" for the government agent to obtain the plaintext without such compulsion.[142] Thus, for example, if the encryption is very weak and could be easily deciphered, or if the password is written down on a piece of paper whose location is known to the police, compelled decryption would not be appropriate because it would be reasonable to acquire the plaintext by other means.[143] This has the effect of making compelled disclosure a last resort.

Subsection (3) of Section 49 delineates the three specific justifications for compelled key disclosure.[144] Under this subsection, plaintext disclosure can be compelled only "in the interests of national security," "for the purpose of preventing or detecting crime," or "in the interests of the economic well-being of the United Kingdom."[145]

---

135 *See* Home Office for Security and Counter Terrorism, *supra* note 128.

136 *Id.*

137 Regulation of Investigatory Powers Act, ch. 23, § 49(2).

138 *Id.* § 49(2)(a); *see also* Explanatory Notes, *supra* note 129, ¶ 257.

139 Regulation of Investigatory Powers Act, ch. 23, § 49(2)(b).

140 *Id.* § 49(3).

141 *Id.* § 49(2)(c).

142 *Id.* § 49(2)(d).

143 *See id*.

144 *Id*. § 49(3).

145 *Id*.

2. Schedule 2

Schedule 2 of RIPA addresses who is allowed to authorize compelled disclosure. First, in order to compel plaintext disclosure, one must have appropriate written permission from a judge, unless one of the statutory exceptions applies.[146] These exceptions are laid out in Paragraphs 2 through 5 of Schedule 2, which also discuss the level of authority required to grant permission to force plaintext disclosure. Importantly, the level of authority "varies depending on the powers under which [the] unintelligible information . . . is likely to be obtained."[147] As a result, the statute allows for non-judicial governmental actors to authorize compelled decryption.

Under Paragraph 2 of Schedule 2 ("Data obtained under a warrant etc"), a government officer may serve a notice compelling plaintext disclosure if he or she obtained unintelligible information pursuant to a warrant issued by "the Secretary of State or a person holding judicial office,"[148] so long as the officer was given authorization to do so either in the warrant itself, or subsequently.[149] Paragraph 2 specifically excludes from compelled disclosure any encrypted information that was seized without a warrant.[150]

Pursuant to Paragraph 3 of Schedule 2 ("Data obtained by the intelligence services under statute but without a warrant"), where an intelligence service comes into possession of unintelligible information[151] in the course of lawful surveillance but without a warrant, the intelligence service can issue a notice compelling disclosure of the plaintext if it has written permission from the Secretary of State.[152] In these instances, there is no requirement of prior judicial approval.

Paragraph 4 of Schedule 2 ("Data obtained under statute by other persons but without a warrant") covers situations when a government agency other than the intelligence services comes into the possession of encrypted information which was not obtained pursuant to a warrant, but

---

[146] *Id*. sched. 2, ¶ 1(1).

[147] Explanatory Notes, *supra* note 129, ¶ 357.

[148] *Id.* at ¶ 360.

[149] Regulation of Investigatory Powers Act, ch. 23, sched. 2, ¶ 2(2).

[150] *Id*. ¶ 2(9).

[151] Explanatory Notes, *supra* note 129, ¶ 366. Unintelligible information refers to encrypted data.

[152] Regulation of Investigatory Powers Act, ch. 23, sched. 2, ¶ 3(2).

was acquired legally pursuant to statutory power.[153] In such situations, the high ranking members of these agencies[154] may grant permission to compel plaintext disclosure.[155] To compel disclosure, a police officer must be of at least the rank of superintendent to give such permission, with some exceptions.[156] With regard to Customs and Excise, the official must be the Commissioner of Customs and Excise, or above a lesser rank set by the Commissioner.[157] Finally, for the military, the officer must be above the rank of lieutenant colonel, or above a rank set by a lieutenant colonel.[158]

Similarly, Paragraph 5 ("Data obtained without the exercise of statutory powers") grants the aforementioned officials the power to authorize compelled disclosure where the encrypted information has come into the hands of the police, Customs and Excise, or an intelligence service lawfully, but not via their respective statutory powers—i.e., if it was voluntarily handed over.[159] Thus, when encrypted information is seized pursuant to the statutory power of one of the enumerated agencies, there is no requirement of judicial oversight for compelled disclosure.

3. Section 50

Section 50 discusses some of the formalities that accompany receiving a Section 49 notice. Under this section, recipients of an order to compel disclosure are given the option to turn over the encryption key instead of the requested plaintext.[160] Moreover, Subsection (8) of Section 50 requires a person no longer in possession of the key to provide information that could help law enforcement gain possession of it.[161]

---

[153] Explanatory Notes, *supra* note 129, ¶ 368.

[154] The agencies are the police, Customs and Excise, and the military. *Id.* ¶ 369.

[155] *Id.*

[156] Regulation of Investigatory Powers Act, ch. 23, sched. 2, ¶ 6(3) (concerning information that has come into the police's hands through the exercise of power of section 44 of the Terrorism Act 2000 or section 13A or 13B of the Prevention of Terrorism Act of 1989).

[157] *Id.* ¶ 6(4).

[158] *Id.* ¶ 6(5).

[159] *Id.* ¶ 5; *see also* Explanatory Notes, *supra* note 129, ¶ 371.

[160] Regulation of Investigatory Powers Act, ch. 23, § 50(1)-(2) ("A person subject to a requirement [of disclosing plaintext] . . . shall be taken to have complied with that requirement if . . . he makes, *instead*, a disclosure of any key to the protected information that is in his possession." (emphasis added)).

[161] *Id.* § 50(8).

4. Section 51

Section 51 addresses the situation where the government specifically wants the encryption key, instead of merely the plaintext.[162] In such a case, Section 51 requires that the government satisfy several extra burdens.[163] First, a government official may only require disclosure of the actual key when "special circumstances" exist such that the purpose of the disclosure, to get the plaintext, would be defeated without obtaining the actual key.[164] Second, the official must balance the imposition of compelling the disclosure of the key against two factors: (1) the risk that other private information, not including that which the government is specifically seeking, may be turned over; and (2) the risk that compelled disclosure might have an adverse effect on the business of the person being compelled.[165]

5. Section 53

In Section 53, RIPA criminalizes failure to comply with these disclosure requirements[166]: it is a crime to "knowingly fail[] . . . to make the disclosure required" by a Section 49 notice.[167] The punishment resulting from a conviction is up to two years imprisonment, a fine, or both.[168]

There are several affirmative defenses to this crime. First, an individual who fails to comply with a Section 49 notice can demonstrate that he could not have complied with the disclosure requirement in the time required, and that he did comply as soon as it was reasonable to do so.[169] Second, an individual can argue that he was not actually in possession of the key.[170] If an individual is able to raise an issue of fact with regard to this second defense, the burden then shifts to the government to prove beyond a reasonable doubt that he does indeed have possession of the key.[171] Thus, the government can

---

[162] *Id.* § 51.
[163] *Id.*
[164] *Id.* § 51(4).
[165] *Id.* § 51(5)(b).
[166] *Id.* § 53-54.
[167] *Id.* § 53(1).
[168] *Id.* § 53(5)(a).
[169] *Id.* § 53(4); *see also* Explanatory Notes, *supra* note 129, ¶ 283.
[170] Regulation of Investigatory Powers Act, ch. 23, § 53(3).
[171] *Id.* § 53(3)(b).

only prosecute under Section 53 if it has successfully proven beyond a reasonable doubt that the accused is in possession of the encryption key.[172]

6. Section 54

Under Section 54, RIPA also criminalizes "tipping off."[173] This refers to the notion that, in some situations, a Section 49 notice will include a requirement that the recipient of the notice keep its delivery and its contents secret.[174] A Section 49 notice may contain such a secrecy requirement only when the encrypted information has come into the possession of the police "by means which it is reasonable, in order to maintain the effectiveness of any investigation . . . , or in the interests of the safety or well-being of any person, to keep secret from a particular person."[175] Therefore, where the authorities can articulate a reason why their investigation would be hampered by disclosing the fact that they had served a Section 49 notice, they can include what amounts to a gag order.[176] When the recipient of such a Section 49 notice "tips off" another person to the fact that he received the notice, or discloses the contents of the notice to another person, he can be subject to criminal liability.[177] A person convicted of this "tipping off" offense will be subject to "imprisonment for a term not exceeding five years or to a fine, or to both."[178]

Section 54 also includes a number of affirmative defenses. These include: when the tipping off was the result of software which automatically informed other people that the encryption key was compromised,[179] when the disclosure is made to legal counsel in a conversation about one's options under Part III of RIPA,[180] when the disclosure is made to persons within an organization so that they can comply with

---

[172] *Id.* § 53.
[173] *Id.* § 54 (Eng.); *see also* Explanatory Notes, *supra* note 129, ¶ 285.
[174] Regulation of Investigatory Powers Act, ch. 23, § 54(1).
[175] *Id.* § 54(3).
[176] *Id.*
[177] *Id.* § 54(4).
[178] *Id.* § 54(4)(a).
[179] *Id.* § 54(5).
[180] *Id.* § 54(6)-(7).

the notice,[181] and when a person is told about a notice but does not know that there was a secrecy requirement.[182]

In contrast to the prospective American system, officers of the British government are thus empowered to compel decryption without so much as prior approval of a member of the judiciary. This system lends a powerful tool in the burgeoning war against modern criminals.

IV. CRITICISMS AND A MIDDLE GROUND

America and Great Britain have approached the dilemma posed by powerful encryption in vastly different manners. Each resides at one end of a continuum between providing adequate protection of civil rights and ensuring the effectiveness of law enforcement. The American approach favors the protection of civil liberties, while the British approach favors law enforcement interests. Ultimately though, each method is fraught with unique problems. Accordingly, America should seek to adopt a suitable middle ground that draws upon the strengths, and avoids the weaknesses, of both approaches.

A. Criticisms of the American and British Approaches

The major problem with the American approach, as exemplified by *Boucher*, is that the government's power to investigate and prosecute crimes, especially those of a technological nature, will be significantly hampered if criminals are able to hide their activities behind a virtually unbreakable wall of encryption.[183] It is easy to imagine nightmare scenarios in which law enforcement efforts are thwarted by criminals utilizing powerful encryption. In her testimony before the House of Representatives, then U.S. Attorney General Janet Reno described three such hypothetical situations: terrorists seeking to detonate a bomb in a major city using encrypted communications, a child abuser and distributor of child pornography encrypting photographs so as to hide them from law enforcement, and a computer hacker stealing personal financial data and then encrypting his hard

---

[181] *Id.* § 54(9).

[182] *Id.* § 54(10).

[183] *See supra* text accompanying note 5.

drive so as to avoid detection and prosecution.[184] In each of these scenarios, the consequences to the public would be dire if the government were unable to access the information it needed.

The principal problem with the American approach is that, in the face of widespread encryption, the government might be severely hindered in its efforts to investigate and prosecute criminal activity. Despite the notion that there are some testimonial aspects implicated in forced decryption, affording sweeping Fifth Amendment protection to such actions would be impractical because of the possibility that prosecutions could grind to a halt as a result of widespread encryption. Moreover, leaving the issue solely to the judiciary might create uncertainty because the rules pertaining to compelled decryption could develop in different fashions and at different paces in the various jurisdictions confronting the issue. This would be detrimental as legitimate users of encryption, such as travelling businesspersons would be forced to alter their data protection strategies depending on in which jurisdiction they were located.

The British approach, while accounting for the law enforcement related problems of the American approach, is fraught with problems of its own. Most fundamentally, in an attempt to prevent criminals from being able to hide their activities behind a wall of encryption, RIPA does not provide adequate provisions for the protection of civil liberties.[185] Ultimately, there is very little in the way of safeguards standing between the government and the encrypted files it seeks. For example, it is not even always necessary to gain judicial approval before a Section 49 notice is sent, as frequently the approval of a high ranking police, Customs and Excise, or military official will suffice.[186] According to one commentator, RIPA is a "sledgehammer law designed to

---

[184] *Security and Freedom Through Encryption (SAFE) Act: Hearing on H.R. 850 Before the H. Armed Servs. Comm.*, 106th Cong. (1999) (statement of Janet Reno, Att'y Gen. of the United States), *available at* http://www.usdoj.gov/archive/ag/testimony /1999/agarmed071399.htm.

[185] *See Police Decryption Powers Flawed*, BBC NEWS, Aug. 15, 2006, http://news.bbc.co.uk/2/hi/technology/4794383.stm; *RIPA Could Be Challenged on Human Rights*, OUT-LAW.COM, Jan. 24, 2008, http://www.out-law.com//default.aspx?page=8826.

[186] Kirk, *supra* note 122 ("A Section 49 request must . . . be approved by a judicial authority, chief of police, the customs and excise commissioner or a person ranking higher than a brigadier or equivalent."); *supra* Part III.B.2.

support security services at the expense of civil liberties which are taken for granted in most of the western world."[187] This commentator continues that "Britain does not join the best company with [RIPA]—other places to have similar laws include Russia and Malaysia."[188]

A further problem with the British approach is the inclusion of the gag order provision. Such orders are reminiscent of the unsuccessful National Security Letters ("NSLs") which were authorized by the USA PATRIOT Act.[189] NSLs are administrative subpoenas issued by certain governmental agencies which require no probable cause or judicial oversight.[190] They also contained a gag order provision similar to Section 54 of RIPA, which forbids the recipient of the NSL from disclosing to anyone that he received it.[191] The gag order provision was held unconstitutional by a judge in the Southern District of New York as violative of the First Amendment.[192] The statute was partially amended by Congress in response to this decision and still it was held unconstitutional by the same district judge on remand from the Second Circuit.[193] There was also massive popular outcry in America against the NSL gag orders on civil rights grounds.[194] Considering the controversy surrounding the NSL gag orders, one could imagine that an analogous gag order section in a potential American compelled decryption statute would be met with similar dissent.

RIPA has also faced stiff criticism from those who fear it will hurt e-commerce in Great Britain. Their concern is that RIPA will drive technology-centered companies out of Great Britain and into countries with more legal protections for

---

[187] Nick McIntosh, *Curbing our Right to Online Freedom*, GUARDIAN, Apr. 18, 2001, http://www.guardian.co.uk/technology/2001/apr/18/news.childprotection/.

[188] *Id.*

[189] Doe v. Gonzales, 500 F. Supp. 2d 379, 385 (S.D.N.Y. 2007), *aff'd in part, rev'd in part sub nom.*, Doe v. Mukasey, 549 F.3d 86, 864 (2d. Cir. 2008).

[190] Press Release, Fed. Bureau of Investigation, Frequently Asked Questions: National Security Letters, *available at* http://www.fbi.gov/pressrel/pressrel07/nsl_faqs030907.htm (last visited Sept. 8, 2009).

[191] Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2709 (2006).

[192] Doe v. Ashcroft, 334 F. Supp. 2d 471, 526-27 (S.D.N.Y. 2004).

[193] Doe v. Gonzales, 500 F. Supp. 2d at 425-26.

[194] *See generally* Op-Ed, *My National Security Letter Gag Order*, WASH. POST, Mar. 23, 2007, at A17; Press Release, Electronic Frontier Foundation, EFF Urges Court to Rule National Security Letters Unconstitutional, Mar. 20, 2008, http://www.eff.org/press/archives/2008/03/20; *Challenge to the "National Security Letter" Authority*, ACLU, *available at* http://www.aclu.org/safefree/patriot/17458res 20040929.html (last visited June 13, 2009).

encryption.[195] In fact, after the passage of RIPA, Ireland passed a law which specifically made it clear that the Irish government would not be permitted to compel key disclosure.[196] An independent report prepared for the British Chambers of Commerce on the economic impact of RIPA stated:

> As it stands, RIP[A] is likely to create a legal environment which will inhibit investment, impede the evolution of e-commerce, impose direct and indirect costs on business and the consumer, diminish overall trust in e-commerce, disrupt business-to-business relationships, place UK companies at a competitive disadvantage, and create a range of legal uncertainties that will place a growing number of businesses in a precarious position.[197]

Critics have also criticized the criticized the perverse incentives and harsh operation of the statute. They stress that the purported principal targets of Part III—terrorists and purveyors of child pornography—would likely take the two or five year sentence resulting from nondisclosure rather than face what would assuredly be a much longer sentence if the data was decrypted and their crimes were revealed.[198] Further, critics argue that a person served with a Section 49 notice could legitimately have forgotten the requested encryption key, and could be subject to a two year sentence for nothing more than absentmindedness.[199]

Lastly, a structural problem with RIPA is that there are software programs which foresee the possibility that one could

---

[195] *See* Yeates, *supra* note 10, at 153 ("Substantial apprehension exists in Britain as to whether the RIPA will blunt the growing U.K. e-economy . . . . [N]umerous critics bitterly pointed out the contrast between Prime Minister Tony Blair's stated desire to make the U.K. the friendliest place in the world for e-commerce and the perceived negative impact of the RIPA on e-commerce."); *see also* Victor Keegan, Op-Ed, *Internet Monitoring 'Time Bomb' for E-commerce*, THE GUARDIAN, June 13, 2000, http://www.guardian.co.uk/technology/2000/jun/13/freespeech.internet ("[RIPA] will produce one of the most draconian regimes in the world driving e-commerce to safer havens like Ireland and most countries in Europe.").

[196] *See* Yeates, *supra* note 10, at 153. The Irish Electric Commerce Bill states, "Nothing in this Act shall be construed as requiring the disclosure or enabling the seizure of unique data, such as codes, passwords, algorithms, private cryptographic keys, or other data, that may be necessary to render information or an electronic communication intelligible." Electronic Commerce Act, 2000 (Act No. 27/2000) § 28 (Ir.) *available at* http://www.irishstatutebook.ie/2000/en/act/pub/0027/sec0028.html.

[197] BRITISH CHAMBERS OF COMMERCE, THE ECONOMIC IMPACT OF THE REGULATION OF INVESTIGATORY POWERS BILL (2000).

[198] Julian Glover & Patrick Barkham, *The RIP Act*, THE GUARDIAN, Oct. 24, 2000, *available at* http://www.guardian.co.uk/world/2000/oct/24/qanda ("[D]rug smugglers and paedophiles [sic] would happily settle for a two-year prison sentence rather than face far harsher penalties for being found guilty of the crime they are suspected of.").

[199] *Id.*

be forced to turn over a password and plan for this eventuality by allowing one to create a false "secret" location that is accessed by a dummy password. TrueCrypt, one such encryption software program, has a function which allows a user to set up a section of the encrypted portion of a hard drive that contains some files, but not the ones actually meant to be kept secret.[200] A different password or passphrase accesses this false drive and TrueCrypt recommends that the user store some files in this section that appear sensitive but that can become public.[201] Under such a set-up, when compelled, the user can give the authorities the password to this false location. This allows him to seemingly comply with the compulsion order, but still keep his real secret files hidden.[202]

B. Middle Ground

To alleviate these problems, America must seek a middle ground between the current American approach and the British approach. Such a middle ground would be well served by incorporating the unique strengths of each approach, and avoiding some of their pitfalls.

Leaving the issue solely to the judiciary on a case by case basis would likely create uncertainty and leave the government ill-equipped to gain the plaintext they need to prosecute violations of the law. Because of this, a statutory solution is needed, and a bill should be passed that creates a standardized procedure that government agents must follow in order to get an order compelling decryption. The American government's response to wiretapping is instructive, for wiretapping similarly involved the intersection of constitutional protections and modern technology. Fourth Amendment issues raised by wiretapping were initially handled by the judiciary; first in *Olmstead v. United States*,[203]

---

[200] *See* TrueCrypt, Hidden Volume, http://www.truecrypt.org/hiddenvolume (last visited Aug. 30, 2009).

[201] *Id.* ("[Y]ou should copy some sensitive-looking files that you actually do NOT want to hide. These files will be there for anyone who would force you to hand over the password.").

[202] *Id.* ("[I]t is impossible to prove whether there is a hidden volume within it or not, because free space on *any* TrueCrypt volume is always filled with random data when the volume is created and no part of the (dismounted) hidden volume can be distinguished from random data." (emphasis added)).

[203] 277 U.S. 438 (1928) (Court held wiretapping did not violate the Fourth Amendment because they were reluctant to expand Fourth Amendment protections beyond the literal language of the text).

and later in *Katz v. United States*[204]. Then, in 1968, Congress passed the Omnibus Crime Control and Safe Streets Act of 1968 ("Omnibus Crime Control Act"), which functionally took the wiretapping issue out of the hands of the judiciary.[205]

This new statute laid out a detailed set of procedures, discussed below, that police must follow in order to be granted permission to run a wiretap.[206] From this statute, and the above-discussed experiences of the American and British approaches to compelled decryption, a number of recommendations for a statutory middle ground can be made.

First, there should be an absolute prerequisite of prior approval by a member of the judiciary for the grant of a compelled decryption order. The Omnibus Crime Control Act contains a similar requirement with regards to prior judicial approval for wiretaps.[207] Such a requirement would likely ease some of the criticism that would be leveled at a RIPA-like bill in America.[208] Congress should not incorporate the portions of RIPA that allow compelled decryption orders to be authorized by non-judicial actors like high-ranking police, Customs and Excise, and military officers.

Second, Congress would have to account for the fact that the act of being compelled to produce a password or an encryption key can communicate any of the three incriminating *Fisher* elements: the existence of the plaintext, the defendant's control over the plaintext, and the authenticity of the

---

[204] 389 U.S. 347 (1967) (Court overruled *Olmstead* holding that the protections of the Fourth Amendment extended to a government listening device attached a phone booth because it constituted a search).

[205] Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2522 (2006).

[206] *Id.* § 2518.

[207] *Id.* § 2518(1) ("Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application.").

[208] An example of the American preference for prior judicial approval can be found in Fourth Amendment jurisprudence regarding search warrants. The Supreme Court has stated its preference for neutral magistrates, and not police officers personally involved in criminal investigations, to issue search warrants. Johnson v. United States, 333 U.S. 10, 14 (1948) (stating a preference for search warrant decisions to be made "by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime"); *see also* Mark Tran, *RIP Bill and Civil Liberties*, GUARDIAN, June 12, 2000, http://www.guardian.co.uk/world/2000/jun/12/qanda.marktran (quoting British "inventor of the world wide web" Tim Berner-Lee as stating RIPA "would have been thrown out in the US 'in a second'" as it "gives the government great power to abuse personal liberties" and commercial innovation).

plaintext.[209] This could be accomplished by requiring, through means unrelated to the defendant's act of producing the password, proof of the existence of the plaintext, proof that the defendant has control of the plaintext, and proof that the plaintext is authentic.[210] The standard of proof by which the government would have to prove each of these elements, in keeping with the Omnibus Crime Control Act,[211] could be probable cause.

Third, a compelled decryption order should only be available for a certain list of specifically enumerated crimes. Such an approach was taken in the Omnibus Crime Control Act, which limits the types of crimes for which a wiretap may be sought.[212] Commensurate with the serious intrusion on privacy, compelled decryption orders should only be available to law enforcement when the serious nature of the crime merits compelled disclosure.

Fourth, for a compelled decryption order, Congress should require that the government agent meet a heavy burden of proof in order to receive judicial approval.[213] In the Omnibus Crime Control Act, the burden of proof typically required is probable cause,[214] and that same level could be applied in a new compelled decryption statute. This burden could function on several fronts. First, the government should prove that the subject of the order is actually in possession of the encryption key or password.[215] Second, the government should demonstrate that it has exhausted all other possible methods of obtaining the plaintext short of compelled disclosure.[216] Third, the

---

[209] *See supra* text accompanying notes 64-66.

[210] The idea the government should be required to account for each of the three *Fisher* elements was proposed in an article by Aaron M. Clemens. *See* Clemens, *supra* note 27, at 1. Mr. Clemens recommended that the burden for proving each of these elements should be clear and convincing evidence. *Id.* Notably, this concept rings of the foregone conclusion doctrine in that if the government can already prove the three assertions of *Fisher*, nothing would be gained by compelling disclosure, and any incriminating assertions accompanying the act of production would be a foregone conclusion. *See supra* text accompanying notes 104-106.

[211] *See* 18 U.S.C. § 2518(1)(d).

[212] *Id.* § 2516(1).

[213] This burden could, for example, be proof beyond a reasonable doubt or even clear and convincing evidence.

[214] *See* 18 U.S.C. § 2518(3).

[215] *Cf.* Regulation of Investigatory Powers Act, 2000, ch. 23, § 49(2)(a) (Eng.). RIPA only requires that there by "reasonable grounds" to believe that the person served with the section 49 notice actually be in possession of the key, and a higher standard of proof would be better suited to a new American approach. *Id.*

[216] *Cf.* 18 U.S.C. § 2518(3)(c) (Judge may only authorize wiretap if "normal investigative procedures have been tried and have failed or reasonably appear to be

government should demonstrate that the plaintext it seeks goes to a material issue of their investigation.[217] Lastly, the government should prove that one of the specifically enumerated crimes has been, or is about to be, committed.[218]

Fifth, it is likely that an equivalent to RIPA's Section 54 gag order would not pass muster in America.[219] Based on the controversy surrounding similar provisions related to National Security Letters, any compelled disclosure statute would wisely omit any analogous section.

Sixth, the compelled decryption statute should precisely lay out the technical procedures that must be followed in order to obtain a compelled decryption order. For example, in borrowing from features of the Omnibus Crime Control Act, the statute could require that the application for the compelled decryption order include factual details pertaining to the identity of the suspect,[220] the physical location and description of the electronic files to be decrypted,[221] the other methods the police have exhausted to get the plaintext,[222] and the factual details from the investigation that have led the police to believe that the suspect has committed, or is about to commit, a crime.[223]

CONCLUSION

As the use of encryption becomes increasingly prevalent, governments will face a growing need to develop a comprehensive and coordinated response to situations where powerful encryption stands between the government and valuable evidence. The responses by Great Britain and America, while entirely different, are uniquely problematic. Nonetheless, the lessons of each, in addition to the Omnibus

---

unlikely to succeed if tried or to be too dangerous"). RIPA only requires that it not be "reasonably practicable" to acquire the plaintext in another manner. *See* Regulation of Investigatory Powers Act, ch. 23, § 49(2)(d). A higher standard of proof would be better suited to a new statutory approach to compelled decryption.

[217] This would ensure that compelled decryption orders were only being used when absolutely necessary for the successful prosecution of a crime.

[218] *Cf.* 18 U.S.C. § 2518(3)(a) (Judge may only authorize wiretap if there is "probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense").

[219] *See supra* text accompanying notes 189-194.

[220] 18 U.S.C. § 2518(1)(b).

[221] *Id.*

[222] *Id.* § 2518(1)(c).

[223] *Id.* § 2518(1)(b).

Crime Control Act, offer valuable insight into the creation of a more enlightened statutory approach.

The British statutory response very effectively gives law enforcement the ability to compel decryption in furtherance of criminal investigations, but it does so at too high a cost to civil liberties. The American approach, as exemplified by Judge Niedermeier's opinion in *Boucher*, does an excellent job of protecting civil liberties, but leaves law enforcement severely handicapped in its ability to investigate and prosecute serious crimes. Criminals with even minimal technical expertise are able to hide their activities behind virtually unbreakable walls of encryption, and the American government would be practically powerless to access the evidence.

Thus, while both the British and American approaches to compelled decryption are valuable, they are also fraught with their own unique difficulties. Consequently, America should seek a middle ground that better takes into account the competing ideals of civil liberty and law enforcement interests.

Brendan M. Palfreyman[†]

[†] B.A., Haverford College, J.D. candidate, 2010, Brooklyn Law School. I would like to thank the members of the *Brooklyn Law Review*, especially Andrei Takhteyev and Joseph Roy, for their tireless efforts. Thanks also to my mom, dad, brother, sister, nieces, Chase, Hudson, and Kimberlee.