Saint Louis University Public Law Review

Volume 34
Number 2 *General Issue (Volume XXXIV, No. 2)*

Article 10

2015

The Encryption Problem: Why the Courts and Technology Are Creating a Mess for Law Enforcement

J. Riley Atwood
jatwood3@slu.edu

THE ENCRYPTION PROBLEM: WHY THE COURTS AND TECHNOLOGY ARE CREATING A MESS FOR LAW ENFORCEMENT

I. INTRODUCTION

The recent proliferation of powerful and inexpensive encryption technology has given law-abiding citizens and criminals alike an unprecedented ability to keep their secrets safe.[1] Potent encryption software is freely available online, and even a novice computer user now has the power to protect her private and confidential data behind a virtually impenetrable wall of protection.[2] Yet, the spread of encryption has also seriously hindered law enforcement during the investigation of cybercrimes.[3] Criminals are able to hide incriminating digital evidence in encrypted hard drives and volumes, which can make it impossible for investigators to access the data.[4]

Sometimes the only way for the Government to gain access to a defendant's incriminating data is to attempt to compel the defendant through a court order to divulge her password.[5] However, this tactic, which has been called "compelled decryption," has had mixed results, since some courts have found that the Fifth Amendment privilege against self-incrimination protects a defendant from being forced to disclose her password or decrypt her data.[6] There has been no authoritative ruling by the Supreme Court on the issue, and the lower courts have reached conflicting decisions, which has left law enforcement in the lurch.

This article will not engage in an in-depth discussion of how the courts should decide this constitutional issue,[7] but will instead analyze the past court

[1] Eoghan Casey et al., *The Growing Impact of Full Disk Encryption on Digital Forensics*, 8 DIGITAL INVESTIGATIONS 129, 129 (2011).

[2] *Id.* at 130.

[3] *Id.*

[4] Dario Forte, *Do Encrypted Disks Spell the End of Forensics?*, 2 COMPUTER FRAUD & SECURITY 18, 19 (2009).

[5] Erica Fruiterman, *Upgrading the Fifth Amendment: New Standards for Protecting Encryption Passwords*, 85 TEMP. L. REV. 655, 656 (2013).

[6] *Id*. at 657.

[7] S*ee, e.g.*, Aaron M. Clemens, *No Computer Exceptions to the Constitution: The Fifth Amendment Protects Against Compelled Production of Encrypted Document or Private Key*, 8 UCLA J.L. & TECH., no. 1, 2004, at 1, 24–27; Adam C. Bonin, *Protecting Protection: First and Fifth Amendment Challenges to Cryptography Regulation*, 1996 U. CHI. LEGAL F. 495, 514;

decisions on the issue and predict what future court holdings regarding compelled decryption will likely be. Furthermore, this article will explore how the proliferation of encryption technology, when combined with the rise in cybercrime and the mixed signals from the courts on the issue of compelled decryption, is causing significant difficulties for law enforcement. Finally, the article will examine possible solutions to these problems.

II. RISE OF CYBERCRIME

The beginning of cybercrime[8] as we know it[9] occurred in the early 1970s when a teller at New York's Dime Savings Bank used a computer to embezzle over $2 million.[10] It was not until 1981, however, that a person was charged and convicted of a felony computer crime.[11] In the 1990s the rates of cybercrime increased dramatically as more and more people were able to access computers and the Internet.[12] By the 2000s, the rates of reported cybercrimes had risen to extraordinarily high levels and are, as of this writing, at a record high.[13]

Aside from simply higher rates of reported cybercrimes, the actual cost to society resulting from these crimes has risen dramatically as well.[14] Despite predictions that the cost of cybercrime would begin decreasing after 2012 due to improvements in security technology, the costs and occurrences of cyber attacks have risen in 2013.[15] This is partially due to the increased costs of hiring security professionals to prevent and clean up after cyber attacks, but

Fruiterman, *supra* note 5, at 662–87, for in-depth constitutional analysis and arguments on this issue.

[8] Numerous academic works have attempted to define "cybercrime," yet there is no agreed-upon definition of the word. Most statutes and legislation do not refer directly to cybercrime, but instead call it "high-tech crime," "computer crime," "electronic communications," or "information technologies." UNITED NATIONS OFFICE ON DRUGS & CRIME, COMPREHENSIVE STUDY ON CYBERCRIME 11–12 (Feb. 2013).

[9] Pooja Aggarwal et al., *Review on Cyber Crime and Security*, 2 INT'L J. RES. ENGINEERING & APPLIED SCI. 48, 48 (2014) (arguing that the first cybercrime actually occurred in 1820 when employees at a textile manufacturing factory in France sabotaged the factory's loom out of fear that the machine would replace them).

[10] Paul Danquah & O.B. Longe, *Cyber Deception and Theft: An Ethnographic Study on Cyber Criminality from a Ghanian Perspective*, 11 J. INFO. TECH. IMPACT, 169, 170 (2011).

[11] *Id.* (describing the incident where Ian Murphy, aka "Captain Zap," broke into AT&T's computer system and changed the billing clock so that people received discounted rates during normal business hours).

[12] *Id.*

[13] *See* RSA, THE CURRENT STATE OF CYBER CRIME 2013, at 1–8 (2013), *available at* http://www.RSA.com.

[14] *See* Triska Hamid, *Playing with Firewalls*, WALL ST. J., Oct. 5, 2010, http://online.wsj.com/news/articles/SB10001424052748703453804575479632855718318?mod=_newsreel_3.

[15] Sean M. Kerner, *Cyber-Crime Costs Continue to Rise: Study*, EWEEK, Oct. 8, 2010, http://www.eweek.com/security/cyber-crime-costs-continue-to-rise-study.html.

mainly it is due to the increased frequency and audacity of the cyber attacks themselves. It is difficult to quantify the damage of cybercrime,[16] but it is estimated that its effects cost companies in the United States between $24 and $120 billion annually.[17] Furthermore, because cybercriminals are now better resourced and more sophisticated, tracking them down has proven to be more difficult and expensive.[18]

The growth of the Internet has also facilitated the rapid expansion of the child pornography industry.[19] Aside from providing a place for child pornographers to distribute abusive photos and videos, the Internet also allows pornographers to network, share tactics on how to evade law enforcement, and to just generally support each other.[20] Furthermore, it is now possible for an exploited child's picture to be shared with thousands of other individuals almost instantaneously.[21] The costs to society incurred by the growth of child pornography are difficult to measure, but the personal costs to the victims are vast.[22] Once pictures and videos of the abuse are on the Internet, they are nearly impossible to remove, and thus, victims describe being in a perpetual state of abuse and revictimization.[23] As will be discussed in greater detail later on in this article, not only has the growth of the Internet facilitated the spread of child pornography, but the growth of encryption has made it more difficult and time-consuming to arrest and prosecute child pornographers.[24]

[16] Pierluigi Paganini, *2013 - The Impact of CyberCrime*, INFOSEC INST., Nov. 1, 2013, http://resources.infosecinstitute.com/2013-impact-cybercrime/ (citing the loss of intellectual property, opportunity costs, job loss, insurance, penalties to customers, and damage to brand image as different factors in considering the cost of cybercrime).

[17] *Id.*

[18] Kerner, *supra* note 15.

[19] Dan Patterson, *Child Pornography and the Internet*, SUMALL FOUND., http://sumall.org/child-pornography-data/ (last visited Feb. 11, 2014) (indicating that the production and consumption of child pornography is still growing at an extremely high rate, despite efforts by law enforcement to curtail it). Between 2007 and 2011, the growth of the number of child porn images shared on the Internet quadrupled. *Id.*

[20] Richard Wortley & Stephen Smallbone, *Child Pornography on the Internet*, CMTY. ORIENTED POLICING SERVS. 2010, at 9–10 (U.S. Dep't of Justice Problem-Specific Guides Ser. No. 41, 2010) (noting that the Internet facilitates the cyber-stalking, procurement, and trafficking of children).

[21] Editorial, *Paying a Price for Child Pornography*, L.A. TIMES, Jan. 29, 2014, at A16 (describing Amy, an eight-year-old girl who was raped by her uncle, and whose photo has been found on more than 70,000 confiscated computers alone—and it is likely that is only the tip of the iceberg).

[22] *See* Arjun Sethi, *Who Should Pay for Child Porn Damages?*, WASH. POST, Jan. 24, 2014, http://www.washingtonpost.com/opinions/child-pornography-who-should-pay/2014/01/24/7be4d350-8449-11e3-9dd4-e7278db80d86_story.html.

[23] *Id.* One victim said of her experience, "Every day of my life I live in constant fear that someone will see my pictures and recognize me and that I will be humiliated all over again." *Id.*

[24] Wortley & Smallbone, *supra* note 20, at 22.

III. WHAT IS ENCRYPTION?

Simply put, encryption is a process of encoding electronic information in such a way that only parties who have the password can access the information.[25] In the early days of computing, encryption was a complex technique that only experienced computer users could employ. However, within the last ten years, powerful and free encryption software has become widely available on the Internet.[26] Some of this software is very simple to use, and now even users with minimal computer competence can utilize various encryption techniques.[27]

The spread of free encryption software has given many computer users the ability to protect their private and confidential data. However, it has also provided criminals with a potent tool to thwart law enforcement.[28] Child pornographers, forgers, drug dealers, white-collar criminals, and all manner of cybercriminals have used encryption to seriously hinder investigations into their wrongdoing. By hiding incriminating information behind encryption, criminals can make it nearly impossible for law enforcement to access the information unless they know the password.[29] Many times, the only way for law enforcement to get the password is by attempting to compel the defendant to divulge her password, usually through a court order. However, using governmental coercion to force suspected criminals to give up their passwords can conflict with the accused's Fifth Amendment right against self-incrimination.[30]

IV. PROLIFERATION OF ENCRYPTION TECHNOLOGY

Powerful encryption software is freely available over the Internet. One of the most popular encryption programs is called TrueCrypt, and not only is it free, but it is also one of the most highly regarded and easy-to-use encryption programs available.[31] TrueCrypt allows users to create "encrypted volumes" on their computers. These volumes are essentially virtual containers which users

[25] *See* Casey et al., *supra* note 1, at 130.

[26] *TrueCrypt*, CNET, http://download.cnet.com/TrueCrypt/3000-2092_4-10527243.html (last visited July 3, 2014).

[27] *See* Casey et al., *supra* note 1, at 130.

[28] Eoghan Casey & Gerasimos Stellatos, *The Impact of Full Disk Encryption on Digital Forensics*, 43 OPERATING SYS. REV. 93, 94 (2008).

[29] John Leyden, *Brazilian Banker's Crypto Baffles FBI*, REGISTER, June 28, 2010, http://www.theregister.co.uk/2010/06/28/brazil_banker_crypto_lock_out/.

[30] Marjorie A. Shields, Annotation, *Fifth Amendment Privilege Against Self-Incrimination as Applied to Compelled Disclosure of Password or Production of Otherwise Encrypted Electronically Stored Data*, 84 A.L.R. 6th 251, 258 (2013).

[31] Michael Kassner, *Encryption for the Paranoid: Verifying TrueCrypt Source Code and Binaries*, TECH REPUBLIC, Nov. 21, 2013, http://www.techrepublic.com/blog/it-security/encryption-for-the-paranoid-verifying-truecrypt-source-code-and-binaries/#.

can move documents, movies, and other digital files into, and once the files are moved into the volume they cannot be opened or viewed without using the correct password.[32] TrueCrypt also allows more advanced users to encrypt their computer's entire hard drive or computer system, which makes it impossible for anyone without the password to view any data at all on the computer.[33]

The original creators of TrueCrypt are anonymous[34] and have stated that they never created a "backdoor" for government agencies or law enforcement to use in order to circumvent TrueCrypt's protection. This means that the only way to recover files that are encrypted by TrueCrypt is to try to "crack" the password by using computer programs which attempt to guess various combinations of letters, numbers, and symbols. One method is to employ what is called a "brute force attack," which involves trying every key combination in an effort to find the correct password that will unlock the encryption.[35] However, a brute force attack can take anywhere from a few hours to a few years depending on how long and complex the user makes the password, and depending on how powerful the hardware is that is being used by the person or organization trying to guess the password.[36] If the TrueCrypt user creates a complex, twenty- to thirty-character password, then for all practical purposes his password will be uncrackable, regardless of how many resources the person or organization trying to crack the password has.[37] Even the FBI (Federal Bureau of Investigation) and Scotland Yard, which are agencies with very powerful hardware and decryption programs, have been thwarted by TrueCrypt.[38]

[32] TRUECRYPT FOUND., TRUECRYPT USER'S GUIDE 6 (Feb. 7, 2012), *available at* https://www.grc.com/misc/truecrypt/TrueCrypt%20User%20Guide.pdf.

[33] *Id.* at 33.

[34] *See* Paul Szoldra, *Snowden's Favorite Encryption Tool is "Not Secure"*, BUS. INSIDER, May 31, 2014, http://www.businessinsider.com/truecrypt-shuts-down-2014-5; OPEN CRYPTO AUDIT PROJECT, https://opencryptoaudit.org/ (last visited Aug. 4, 2014) (noting that while the original creators have, as of May 31, 2014, ceased supporting TrueCrypt, it is still available online, and a volunteer organization of computer experts continues to "audit" TrueCrypt in order to ensure the program's security).

[35] *Brute-force Attack*, COMPUTER HOPE, http://www.computerhope.com/jargon/b/brutforc.htm (last visited Jan. 11, 2014).

[36] Kevin Fogarty, *How many seconds would it take to break your password?*, IT WORLD, June 7, 2012, http://www.itworld.com/security/280486/how-long-would-it-take-crack-my-password?page=0,1.

[37] *See id.*

[38] *Not Even FBI was able to Decrypt Files of Daniel Dantas*, GLOBO, June 25, 2010, http://www.webcitation.org/query?url=g1.globo.com/English/noticia/2010/06/not-even-fbi-can-de-crypt-files-daniel-dantas.html; Mark Hosenball, *UK asked N.Y. Times to Destroy Snowden Material*, REUTERS, Aug. 30, 2013, http://www.reuters.com/article/2013/08/30/us-usa-security-snowden-nytimes-idUSBRE97T0RC20130830?feedType=RSS&feedName=domesticNews.

Other encryption programs have also become more prevalent in recent years. Many hard drives on the market now come with encryption programs already built into them by the manufacturer. Although the purpose of this encryption is mainly to protect a consumer's information if the hard drive is stolen, it has already caused serious problems for investigators in cybercrime investigations.[39]

V. MODERN FIFTH AMENDMENT CASE LAW

The Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself . . . ."[40] Defendants have successfully, and unsuccessfully, invoked their Fifth Amendment privilege against self-incrimination in cases where the government has attempted to compel them to give up the password to their encrypted files.

Because the Supreme Court has yet to make a ruling on whether, or in what circumstances, compelled decryption violates a defendant's right against self-incrimination, the lower courts have been left with little guidance on how to approach the issue of compelled decryption.[41] The lower courts must apply Supreme Court decisions relating to cases in which criminal defendants were compelled to produce incriminating paper documents, and it can be difficult and confusing to apply those cases to cases involving compelled decryption.[42] A brief summary of the terminology and doctrines relating to this area of law is important to understand the lower court decisions.

The Supreme Court has made it clear that the term "privilege against self-incrimination" is not an "entirely accurate description of a person's constitutional protection against being compelled in any criminal case to be a witness against himself."[43] A defendant's compelled act of producing incriminating documents before the court or a grand jury does not automatically trigger Fifth Amendment protection, even if the documents contain incriminating assertions of fact or belief on the part of the defendant.[44] The protection of the privilege extends only to compelled incriminating communications that are, what the Court calls, "testimonial" in character.[45] Testimonial means the government must have compelled the individual to use "the contents of his own mind" to communicate some statement of fact.[46] The

[39] Casey et al., *supra* note 1, at 130.

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

[41] Nicholas Soares, *The Right to Remain Encrypted: The Self-Incrimination Doctrine in the Digital Age*, 49 AM. CRIM. L. REV. 2001, 2008 (2012).

[42] *Id.*

[43] United States v. Hubbell, 530 U.S. 27, 34 (2000).

[44] *Id.* at 35–36.

[45] *Id.*

[46] Fruiterman, *supra* note 5, at 660 (citing Curcio v. United States, 354 U.S. 118, 128 (1957)).

production of a document may be testimonial if it conveys a statement of fact that certain documents are under the defendant's control or possession, or are authentic.[47] This is called the "act-of-production" doctrine.[48] However, even if the defendant's act of producing documents is testimonial, if the government can demonstrate that it had prior knowledge of the existence, possession, or authenticity of the documents, the testimonial protection of the documents will be destroyed.[49] This is what is known as the "foregone conclusion doctrine."[50]

A. United States v. Fisher *and the Act-of-Production Doctrine*

The Supreme Court case *United States v. Fisher* laid the foundation for the modern act-of-production and foregone conclusion doctrines.[51] In that case, attorneys representing clients under investigation for violating federal tax laws refused to hand over their clients' taxpayer documents to the IRS (Internal Revenue Service) and asserted their clients' Fifth Amendment privilege.[52] The Court found in favor of the IRS, and in doing so created the foregone conclusion doctrine.[53] The Court held that the Government can compel production where the "existence and location [of the documents] are a foregone conclusion and [defendant's act of production] adds little or nothing to the sum total of the Government's information."[54] The Court made it clear that the Fifth Amendment does not prohibit "the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a testimonial communication that is incriminating."[55] Because the subpoena only forced the defendants to hand over the documents, and did not force them to testify about the contents of the documents, the Court held that the act of producing the documents was not testimonial in nature.[56]

B. United States v. Doe *Narrows the Scope of the Act-of-Production Doctrine*

Eight years after the *Fisher* decision, the Supreme Court reexamined the act-of-production doctrine in *United States v. Doe*.[57] In that case, subpoenas

[47] *Id.* (citing *Hubbell*, 530 U.S. at 36).

[48] *Id.*

[49] *Id.*

[50] United States v. Fisher, 425 U.S. 391, 411 (1976).

[51] *Id.*

[52] Vivek Mohan & John Villasenor, *Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era*, 12 J. CONST. L. HEIGHTENED SCRUTINY 11, 14 (2012).

[53] *Id.*

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

[55] *Id.* at 408.

[56] Andrew J. Ungberg, *Protecting Privacy Through a Responsible Decryption Policy*, 22 HARVARD J.L. & TECH. 543 (2009) (citing *Fisher*, 425 U.S. at 409).

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

were served on the defendant for the production of certain business records during a grand jury investigation of alleged corruption on the part of the defendant.[58] However, the Government had little information about the documents themselves, including whether the documents were even in the defendant's possession.[59] The defendant filed a motion to quash the subpoenas, and the district court granted the motion, finding that "the act of producing the records would involve testimonial self-incrimination."[60] The court of appeals affirmed the district court's decision, and the case was appealed to the Supreme Court.[61]

In examining the issue of whether the defendant's act of producing the records was testimonial self-incrimination, the Court noted that the records in question were not themselves privileged, since the Government had not compelled the defendant to create them in the first place.[62] Yet, the Court recognized that "complying with the subpoena would concede the existence of the papers" and would demonstrate "their possession or control by the [defendant]."[63] The Court held that, in this case, the act of producing the documents would involve testimonial self-incrimination. In distinguishing its holding from *Fisher*, the Court deferred to the court of appeals's finding that the Government was "attempting to compensate for its lack of knowledge by requiring the appellee to become, in effect, the primary informant against himself."[64] The key factor in making this determination was that the Government had failed to produce evidence that possession, existence, and authentication of the document were a foregone conclusion, since the Government lacked substantial information about the records' whereabouts and even their existence.[65]

Finally, the Court held that the Government could have compelled the defendant to produce the business records if it had provided the defendant with "use immunity"[66] in regards to the potentially incriminating evidence.[67] The Court said that, on remand, if the Justice Department decided it needed to compel the defendant to produce his business records, the use immunity option

[58] *Id.*

[59] Fruiterman, *supra* note 5, at 667 (citing *Doe*, 465 U.S. at 612).

[60] *Doe*, 465 U.S. at 605.

[61] *Id.*

[62] *Id.* at 610.

[63] *Id.* at 613.

[64] *Id.* (quoting Matter of Grand Jury Empanelled Mar. 19, 1980, 680 F.2d 327, 335 (3d Cir. 1982)).

[65] Fruiterman, *supra* note 5, at 666–67.

[66] *Doe*, 465 U.S. at 615 ("Sections 6002 and 6003 of Title 18 provide for the granting of use immunity with respect to potentially incriminating evidence.").

[67] *Id.*

would be available,[68] although information directly or indirectly derived from defendant's act of producing the records would not be able to be used in a criminal case against the defendant.[69]

C. United States v. Hubbell *Limits the Foregone Conclusion Doctrine*

The 2000 case *United States v. Hubbell* is the most recent Supreme Court case dealing with the act-of-production and foregone conclusion doctrines. In *Hubbell*, the defendant pled guilty to mail fraud and tax evasion, and had agreed to fully cooperate with the Government in a separate ongoing investigation as part of his plea deal.[70] However, the Government became suspicious that the defendant had violated his promise to fully cooperate,[71] and a second prosecution was brought against the defendant in order to ascertain whether he had broken the terms of his plea bargain. Hubbell was served with a subpoena *duces tecum* ordering him to produce any documents that he possessed within eleven different categories of business, personal, and income-related documents.[72]

Hubbell invoked his Fifth Amendment right against self-incrimination, but the district court ordered him to comply with the subpoena and granted him immunity over his act of producing the documents.[73] Hubbell then turned over 13,120 pages of documents and records, and responded to a series of questions from the Government which established that all of the documents had been in his custody and control.[74] The Government then used the information it had obtained from Hubbell in its case against him, and in 1998 a grand jury returned a ten-count indictment charging him with various fraud- and tax-related crimes.[75]

By the time the case was appealed to the Supreme Court, the main issue before the Court was whether the indictment should be dismissed because the subpoena and subsequent questioning by the Government had violated Hubbell's Fifth Amendment privilege.[76] The Government argued that the

[68] *Id.* at 617.

[69] Kastigar v. United States, 406 U.S. 441, 455 (1972) (holding that derivative use immunity "does not mean that one who invokes it cannot be subsequently prosecuted. Its sole concern is to afford protection against being forced to give testimony leading to the infliction of penalties affixed to . . . criminal acts.").

[70] United States v. Hubbell, 530 U.S. 27, 30 (2000).

[71] The Government had evidence that the defendant Hubbell had received "hush money" in exchange for not telling the Government the full truth. United States v. Hubbell, 167 F.3d 553, 555–56 (D.C. Cir. 1999).

[72] *Id.* at 565.

[73] *Hubbell*, 530 U.S. at 31.

[74] *Id.*

[75] *Id.*

[76] *See id.* at 41–43.

existence of such documents was a foregone conclusion because all businessmen keep such papers.[77] In responding to this argument, the Court noted that the Government "had not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents . . . and the Government cannot cure this deficiency through the overbroad argument that a business man . . . will always possess general business and tax records."[78] The Court thus found that the facts of the case fell outside of the "foregone conclusion" doctrine and upheld the dismissal of the indictment.

One commentator succinctly described the Court's decision in *Hubbell* thusly:

> *Hubbell* shows that the foregone conclusion doctrine does not apply when the prosecuting authority merely presumes that the defendant has incriminating documents, no matter how strong that presumption. At bottom, the Fifth Amendment does not permit the Government to conduct "fishing expeditions" for documents based on mere conjecture.[79]

As a final note on the Supreme Court's interpretation of the Fifth Amendment, the Court has suggested that compelling a defendant to produce the key to his safe would have a different testimonial nature than if he were compelled to produce the combination to the safe.[80] The Court has indicated that producing the key to the safe would not be a testimonial act, but the production of the combination from memory would be protected under the act-of-production doctrine since it is an "expression of the contents of an individual's mind."[81] This distinction made by the Court has led some scholars and lawyers to argue that Fifth Amendment protection would therefore extend to a defendant in a compelled decryption case from being forced to produce his password from his own memory.[82]

VI. COMPELLED DECRYPTION CASE LAW

Applying Supreme Court's Fifth Amendment analyses in *Fisher*, *Doe*, and *Hubbel*, which involved the Government trying to compel the defendant to produce paper documents, to cases where the government is trying to compel the defendant to give up the password to his encrypted data has been a difficult

[77] *Id.* at 44.

[78] *Id.*

[79] Soares, *supra* note 41, at 2007.

[80] David Colarusso, *Heads in the Cloud, a Coming Storm the Interplay of Cloud Computing, Encryption, and the Fifth Amendment*, 17 B.U. J. SCI. & TECH. L. 69, 84 (2011) (citing *Hubbell*, 530 U.S. at 34–36; Doe v. United States, 487 U.S. 201, 210 (1988)).

[81] *Id.*

[82] *Id.* (citing *Doe*, 487 U.S. at 210 n.9). For examples of such arguments, *see* Clemens, *supra* note 7, at 24–27; Bonin, *supra* note 7, at 514; *see also* Brief for Leon Gelfgatt at 1, Commonwealth v. Gelfgatt, 11 N.E.3d 605 (2013) No. 2012-P-0737.

task for the lower courts. The courts struggle with how to apply the foregone conclusion and act-of-production doctrines, which were originally created to deal with the production of physical documents, to this modern, high-tech dilemma.

Therefore, using governmental coercion to force a defendant to give up his password has been used by the government with only mixed success. Typically, the prosecution will petition the court for an order which commands the defendant to decrypt his data under the threat of contempt if he fails to do so.[83] Compelled decryption is a relatively recent tactic that was first used by the government in late 2006. Although the government was initially successful in obtaining these court orders, more recent cases have demonstrated that courts are becoming increasingly reluctant in granting such orders, with many refusing to do so to protect the defendant's Fifth Amendment right against self-incrimination. By protecting defendants from being compelled to decrypt their data, the courts have further exacerbated the difficulties already faced by law enforcement when investigating cybercrimes.[84]

A. In re Boucher *and the Beginning of Compelled Decryption*

The case law surrounding compelled decryption is relatively sparse, and many of the holdings are contradictory. Cases involving compelled decryption are becoming more common however, as law enforcement officials are increasingly encountering encrypted data during investigations. The earliest reported case involving the issue of compelled decryption is *In re Boucher*.[85] On December 17, 2006, Sebastian Boucher was pulled over and inspected by a Customs and Border Protection agent named Chris Pike while crossing the border from Canada into the United States. During the inspection, Officer Pike opened up Boucher's laptop, and was able to examine the contents of the laptop's hard drive without entering a password.[86] After doing a quick search of the hard drive, Officer Pike located thousands of images that appeared to be pornographic based on the filenames of the images.[87] Upon further inspection, officers found a file named "2yo getting raped during diaper change," but were unable to open the file to view it.[88] Agents asked Boucher where the "2yo getting raped during diaper change" file was stored on the hard drive, and

[83] *In re* Boucher, 2:06-MJ-91, 2009 WL 424718, at *1 (D. Vt. Feb. 19, 2009).

[84] This is not to say that the courts which have protected defendants from disclosing their passwords have necessarily been incorrect in their application of Fifth Amendment case law. For scholarly arguments for—and against—extending Fifth Amendment protection to compelled password disclosure, *see* Fruiterman, *supra* note 5; Ungberg, *supra* note 56; Soares, *supra* note 41.

[85] *Boucher*, 2009 WL 424718, at *1.

[86] *Id.*

[87] *Id.* at *2.

[88] *Id.*

Boucher directed the agents to drive Z, which at the time was not protected by the encryption program Boucher had on his computer.[89] Agents located more videos and photos of child pornography in drive Z, and Boucher was subsequently arrested.[90]

Two weeks later, investigators tried to access drive Z again, but were unable to do so because it had been encrypted using an encryption program called Pretty Good Privacy (PGP),[91] which required a password to access drive Z.[92] By restarting Boucher's laptop, agents had apparently inadvertently activated the encryption program.[93] Investigators were unable to view any of the files on drive Z, and consequently could not obtain the evidence of child pornography. The Government attempted to gain access, but could not find any "backdoors" or secret entrances to access the file, and admitted that it would be "nearly impossible to access the encrypted files without knowing the password."[94] In order to gain access to the incriminating files, the Government sought and obtained a grand jury subpoena for the production of "any passwords used or associated with the computer seized from Sebastien Boucher on December 17, 2006." Boucher made a motion to quash the subpoena, claiming that the subpoena violated his Fifth Amendment right against self-incrimination. The District Court of Vermont agreed with Boucher and granted his motion.[95]

The Government was granted an appeal, and on appeal the decision was reversed. The court quoted the Supreme Court in *Fisher v. United States*, saying that "where the existence and location of the documents are known to the government, no constitutional rights are touched, because these matters are a foregone conclusion."[96] The court held that the foregone conclusion doctrine applied because Boucher had already admitted that the laptop was his, and because the government agents had been able to view the files before they were encrypted.[97] Accordingly, the court denied Boucher's motion to quash and ordered Boucher to provide the Government with an unencrypted version of the Z drive.

[89] *Id.*

[90] *Id.*

[91] *Boucher*, 2009 WL 424718, at *2. For more information on PGP software, *see* Margaret Rouse, *Pretty Good Privacy (PGP)*, SEARCHSECURITY, Sept. 2005, http://searchsecurity.techtarget.com/definition/Pretty-Good-Privacy.

[92] *Boucher*, 2009 WL 424718, at *2.

[93] *Id.*

[94] *Id.*

[95] *Id.*

[96] *Id.* at *3 (quoting United States v. Fisher, 425 U.S. 391, 410–11 (1976)).

[97] *Id.*

B. United States v. Kirschner*: A Court Sides with the Defendant*

After *Boucher*, the next case involving compelled decryption is *United States v. Kirschner*.[98] The facts surrounding the case are sparse, but from the record it can be established the defendant was charged with three counts of receiving child pornography.[99] The Government had issued a subpoena ordering the defendant to provide all the passwords associated with his computer and any files on it.[100] Specifically, the Government wanted to gain access to an "encryption file" located on the computer.[101] Although the record does not specify what kind of encryption program was being employed by the defendant, it is possible the "encryption file" that the court is referring to was some sort of encrypted volume that allows the user to store multiple files within it.[102]

The defendant filed a motion to quash the order, and like the defendant in *Boucher*, argued that providing the government with access to his encrypted files would violate his privilege against self-incrimination.[103] The court agreed and quashed the subpoena, holding that even if the defendant were to be granted immunity with regard to the *act* of producing the password to the grand jury, the immunity would not suffice to protect his Fifth Amendment privilege in response to questioning requiring him to reveal his password.[104] The court reasoned that the defendant's act of producing the password would be specific testimony asserting a fact, and held "compelled testimony that communicates information that may lead to incriminating evidence is privileged even if the information itself is not inculpatory."[105] The court noted that the case was not about producing specific documents—it was about producing specific testimony asserting a fact,[106] and therefore the Fifth Amendment privilege against compelled self-incrimination protected the defendant.

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

[99] *Id.* at 666.

[100] *Id.*

[101] *Id.*

[102] *See How to Create an Encrypted Volume*, VIRGINIA TECH, http://www.ahnrit.vt.edu/OnlineTutorials/TrueCrypt/tipsheet-how_to_create_an_encrypted_volume.html (last visited Jan. 29, 2014).

[103] *Kirschner*, 823 F. Supp. 2d at 669.

[104] *Id.*

[105] *Id.* (quoting Doe v. United States, 487 U.S. 201, 208 (1988)).

[106] *Id.*

C. Fricosu and Doe*: Two Courts with Similar Approaches but Differing Results*

In early 2012, two cases involving compelled decryption were decided in the Tenth and Eleventh Circuits, respectively, and in both cases the court utilized similar reasoning but reached different conclusions. The first case, *United States v. Fricosu*, was decided on January 23, 2012.[107] That case involved a defendant, Ramona Fricosu, who was indicted on charges arising from alleged fraudulent real estate transactions.[108] The government executed search warrants at her home, and seized multiple computers and digital storage devices.[109] One of the items seized was a Toshiba Satellite M305 laptop, for which the Government obtained an additional warrant to search its contents.[110] However, the laptop's entire hard drive was encrypted by a program called PGP Desktop, and federal agents' attempts at decrypting the hard drive failed.[111] The Government said it would allow Fricosu to enter the password without being observed by the Government, or otherwise provide the unencrypted contents of the laptop by whatever means she chose.[112] Fricosu declined to produce the unencrypted contents of the laptop and asserted her privilege against self-incrimination under the Fifth Amendment.[113]

The court held that the Fifth Amendment privilege was not applicable to the case, since the contents of the laptop, and any facts communicated by the production of those contents, were foregone conclusions.[114] The court held "there is little question here but that the Government knows of the existence and location of the computer's files. The fact that it does not know the specific contents of any specific documents is not a barrier to production."[115] This decision by the court to apply the foregone conclusion doctrine in a case where the Government did not have specific knowledge of even one incriminating document has been criticized in academia,[116] and the only reported case which

[107] United States v. Fricosu, 841 F. Supp. 2d 1232, 1232 (D. Colo. 2012).

[108] Brief of Amicus Curiae Electronic Frontier Foundation in Support of Defendant Fricosu's Opposition to Government's Application Under the All Writs Act Requiring Defendant to Assist in the Execution of Previously Issued Search Warrants at 2, *Fricosu*, 841 F. Supp. 2d at 1232 (No. 1:10-cr-00509-REB) [hereinafter Brief of Amicus Curiae Electronic Frontier Foundation].

[109] *Id.*

[110] *Id.*

[111] *Id.*; *Symantec Encryption Desktop Professional: Products & Solutions*, SYMANTEC, http://www.symantec.com/encryption-desktop-pro (last visited February 19, 2014).

[112] Brief of Amicus Curiae Electronic Frontier Foundation, *supra* note 108, at 2.

[113] *Id.*

[114] United States v. Fricosu, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012).

[115] *Id.*

[116] *See* Fruiterman, *supra* note 5, at 676.

has cited the *Fricosu* court's application of the foregone conclusion doctrine made a point to distinguish its holding from the *Fricosu* court's holding.[117]

The second case decided in 2012 that dealt with compelled decryption was *United States v. Doe*.[118] In *Doe*, law enforcement officials had been investigating an individual who had been maintaining a YouTube.com account that the Government suspected of sharing explicit materials involving underage girls.[119] Law enforcement officials tracked the suspect, identified as "Doe," to a hotel in California, and applied for a warrant to search his room.[120] Agents executed the warrant and seized seven different hard drives from the room where Doe was staying. Upon inspection, it became clear to the FBI examiners that Doe had used a free and powerful encryption program called TrueCrypt to encrypt portions of his hard drives.[121] Doe had used TrueCrypt's "Encrypt Non-System Partition" feature,[122] which meant that although it was possible for investigators to access some of the contents of the hard drives, other parts (called "partitions") were completely inaccessible without a password.[123] It was on these inaccessible partitions that the FBI suspected Doe had stored child pornography.[124] Doe was then issued a subpoena requiring him to appear before a grand jury and produce the unencrypted contents of his hard drives.[125] The Government offered him limited immunity regarding the disclosure of the password, but not the contents of the hard drive that were protected by the password.[126] Doe refused and invoked his Fifth Amendment privilege.[127] He was held in contempt of court and incarcerated while he awaited his appeal.[128]

On appeal, the Eleventh Circuit reversed the lower court's decision and released Doe from jail, holding that Doe's act of decrypting and producing the hard drives' contents would be sufficiently testimonial to trigger Fifth Amendment protection.[129] The court also held that the district court erred in limiting Doe's immunity to the Government's use of his act of decryption, while still allowing the Government derivative use of the evidence that the act disclosed.[130] The court noted that "even if the decryption and production of the

[117] *Id.*

[118] United States v. Doe, 670 F.3d 1335 (11th Cir. 2012).

[119] *Id.* at 1339.

[120] *Id.*

[121] *Id.*; TRUECRYPT FOUND., *supra* note 32, at 6.

[122] TRUECRYPT FOUND., *supra* note 32, at 50.

[123] *Id.*

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

[125] *Id.*

[126] *Id.* at 1338.

[127] *Id.*

[128] *Id.*

[129] *Id.* at 1344.

[130] *Doe*, 670 F.3d at 1350.

contents of the hard drives themselves are not incriminatory, they are a link in the chain of evidence that is designed to lead to incriminating evidence; this is sufficient to invoke the Fifth Amendment privilege."[131]

The court also rejected the Government's foregone conclusion argument. The court held that just because the Government was in physical possession of the hard drives did not mean that it knew of the existence and location of the electronic files stored there.[132] Seizure and possession thus did not constitute sufficient knowledge of the existence and location of the electronic files.[133] Also, because the Government's expert could not say whether the encrypted drives even contained any files,[134] the Government's prior knowledge was insufficient to meet the existence and location elements of the foregone conclusion standard.[135]

The Eleventh Circuit's broad ruling on the issue of compelled decryption was received enthusiastically by digital rights activists,[136] although it remains to be seen how much influence the decision will have on courts outside of the Eleventh Circuit. The Eleventh Circuit is the only federal court of appeals to make a ruling on the issue of compelled decryption, and therefore its holding may have a greater persuasive effect on the other circuits.[137]

D. Ongoing Encryption Cases

There are two compelled decryption cases currently making their way through the courts which have garnered national attention. In each case, a lower court judge has, at least initially, ruled in favor of the defendant, indicating that the courts may be shifting toward granting defendants in compelled decryption cases greater protection.[138]

[131] *Id.* at 1342 n.15.

[132] *Id.* at 1346.

[133] *See id.* at 1347.

[134] *See* TRUECRYPT FOUND., *supra* note 32 (explaining that TrueCrypt partitions not only make any files that are hidden within them inaccessible, they also completely conceal their presence from users who do not have an authorized passcode).

[135] *Doe*, 670 F.3d at 1347.

[136] *See* Hanni Fakhoury, *EFF to Court: Forced Decryption Unconstitutional*, ELECTRONIC FRONTIER FOUND., July 23, 2013, https://www.eff.org/deeplinks/2013/07/new-eff-amicus-forced-decryption-unconstitutional.

[137] A district court judge in Milwaukee, which is within the Eighth Circuit, has cited the Eleventh Circuit's ruling as very persuasive in his own decision in a compelled decryption case. Bruce Vielmetti, *West Allis Encryption Case Delves into Fifth Amendment Debate*, J. SENTINEL, Apr. 25, 2013, http://www.jsonline.com/news/crime/west-allis-encryption-case-delves-into-fifth-amendment-debate-gi9mrag-204772741.html.

[138] *See* Kade Crockford, *Massachusetts High Court Set to Rule on Whether State can Force You to Decrypt Your Drive*, ACLU, Oct. 31, 2013, https://www.aclu.org/blog/technology-and-liberty-national-security/massachusetts-high-court-set-rule-whether-state-can.

In *United States v. Decryption of a Seized Data Storage System*, FBI agents executed a search warrant for the home of Mr. Feldman and seized sixteen electronic storage devices or hard drives.[139] Nine of the drives were encrypted, and the FBI was unable to break the encryption.[140] As a result, Feldman was not arrested or charged with a crime. The Government sought to compel Feldman to decrypt his drives, but the magistrate judge overseeing the case denied the Government's request.[141] The court ruled that the act of producing the decrypted contents of the computer triggered Fifth Amendment scrutiny, and it also rejected the forgone conclusion doctrine that the courts in *Fricosu* and *Kirchner* had followed.[142]

After the court denied the request, the Government continued to attempt to decrypt the drives, and eventually succeeded in decrypting one of the drives.[143] Although investigators found child pornography, Feldman still was not charged with a crime. When the Government asked the magistrate judge to reconsider his earlier decision, the court changed its mind. The defendant appealed to the federal district court, and the court granted a temporary stay on the lower court's ruling, pending its own review. During the pendency of that decision, Feldman was arrested and charged with possession of child pornography, based on the files found in the drive which the FBI was able to decrypt. As of now, seven out of the nine drives are still encrypted, and it is uncertain if the court will compel the defendant to decrypt the remaining drives.[144]

Massachusetts v. Gelfgatt is the second pending case involving compelled decryption.[145] The defendant is an attorney accused of forging residential mortgage assignments.[146] During a search of his home, the Government seized encrypted computers that the Government suspects contain incriminating

[139] Amicus Brief of Real Party in Interest Jeffrey Feldman's Opposition to Decryption at 1, United States v. Feldman, No. 13-MJ-449-RTR (E.D. Wis. July 23, 2013). Mr. Feldman was suspected of possessing child pornography. *Id.*

[140] *Id.*

[141] *Id.*

[142] *See* Order Denying Application to Compel Decryption, No. 13-M-449 (E.D. Wisc. April 19, 2013), *available at* http://ia601700.us.archive.org/6/items/gov.uscourts.wied.63043/gov.uscourts.wied.63043.3.0.pdf ("This is a close call, but I conclude that Feldman's Act of production, which would necessarily require his using a password of some type to decrypt the storage device, would be tantamount to telling the government something it does not already know with "reasonable particularity" . . . and ordering Feldman to decrypt the storage devices would be in violation of his Fifth Amendment right.").

[143] Jeffrey Brown, *Feds Decrypt Two Hard Drives in Wisconsin Case, Defendant Arrested on CP charges*, CYBERCRIME REV., Aug. 19, 2013, http://www.cybercrimereview.com/2013/08/feds-decrypt-two-hard-drives-in.html.

[144] *Id.*

[145] Brief for Leon Gelfgatt, *supra* note 82, at 1.

[146] *Id.*

information. The court denied a motion by the Government to compel the defendant to decrypt his computers, but the motion was appealed to Massachusetts's appeals court. On appeal, the lower court's decision was reversed,[147] and it is expected to be appealed yet again.[148]

VII. EFFECTS OF THE ENCRYPTION PROBLEM

The proliferation of encryption technology is clearly causing, and will continue to cause, significant problems for law enforcement. The problems for law enforcement have further been exacerbated by the recent court holdings protecting defendants from being compelled to decrypt their encrypted data. Because different jurisdictions have reached different conclusions about the constitutionality of compelled decryption, it is uncertain if the government will be able to compel decryption in the future. Digital forensic investigators and law enforcement officers must adapt to counter the proliferation of encryption technology, and must find new ways to circumvent suspects' encryption protection.

A. Digital Forensic Investigators

Digital forensics is a branch of forensic science covering the investigation and recovery of data found in computers, mobile phones, and other digital devices. Digital forensics has grown from a relatively obscure field to an important part of many investigations.[149] The field has existed less than forty years, and initially forensics was performed only by skilled computer professionals who worked with law enforcement on an *ad hoc*, case-by-case basis.[150] However, beginning in 1999 the field entered into what some experts have called a "Golden Age" for digital forensics.[151] Forensic tools were developed that allowed users with limited training to recover deleted data and search for email messages and other incriminating files. There was also growth

[147] Commonwealth v. Gelfgatt, 11 N.E.3d 605, 605 (2013) (finding the defendant's disclosure to police during questioning that he had encrypted his data destroyed the testimonial nature of producing his password under the foregone conclusion doctrine).

[148] Chris Reidy, *SJC: Defendant May be Compelled to Give Investigators Access to his Computer Files*, BOS. GLOBE, June 25, 2014, http://www.bostonglobe.com/business/2014/06/25/sjc-defendant-may-compelled-give-investigators-access-his-computer-files/PANzWVKdCB2LRgeutZNhQI/story.html.

[149] Simson L. Garfinkel, *Digital Forensics Research: The Next 10 Years*, 7 DIGITAL INVESTIGATION 64, 64 (2010).

[150] *Id.* at 66.

[151] *Id.* The widespread use of personal computers and the Microsoft Windows operating system was one of the main factors behind the growth in the field of digital forensics. Because the vast majority of the public used the Microsoft Windows operating system, examiners only had to learn one system. The failure of the market to adopt encryption technology was also cited as a major reason behind the "Golden Age" of digital forensics. *Id.*

in digital forensic research and professionalization, and national standards for investigators were adopted for the first time.[152]

Still, experts in the field are predicting that digital forensics is facing an imminent crisis.[153] Simson Garfinkel, a leading academic and inventor in the field of digital forensics, has cited pervasive encryption and new legal challenges as the main reasons behind the coming crisis.[154] According to Simson, the proliferation of TrueCrypt presents a major problem for investigators because of how difficult it is to crack.[155] TrueCrypt's "hidden volume" feature is particularly troublesome for investigators.[156] This feature allows users to create a hidden volume within a standard TrueCrypt volume, and each volume has its own password.[157] If a user is compelled to give up the password to his encrypted data, he can give the investigators the password to the standard volume, but not the hidden volume.[158] Investigators will then be able to access the data in the standard volume, but they will have no way of knowing about the hidden volume's existence. A savvy user will put private or mildly embarrassing files in the standard volume, but hide the actual incriminating data in the hidden volume.[159] Because the user will appear to be cooperating with law enforcement by divulging his password, investigators may not realize that additional evidence is still concealed in the volume.[160]

TrueCrypt is not the only encryption software causing problems for digital investigators.[161] Well-known software developers such as McAfee and Symantec have released encryption products that support Full-Disk Encryption (FDE).[162] FDE provides encryption for the entire hard drive, making it

[152] *Id.*

[153] Forte, *supra* note 4, at 19; Garfinkel, *supra* note 149, at 67.

[154] Garfinkel, *supra* note 149, at 67. Garfinkel also cites the proliferation of "cloud" computing (i.e., using files and applications over the Internet), the increased use by the public of operating systems other than Microsoft Windows, and growth in the memory capacity of hard drives and other storage devices as major problems for digital forensic investigators. *Id.*

[155] *Id.* Garfinkel states that although TrueCrypt technology is not completely impervious to an attack by a skilled digital forensic examiner, circumventing the technology requires both luck and time on the part of the examiner. *Id.*

[156] Casey et al., *supra* note 1, at 130.

[157] "The principle is that a TrueCrypt volume is created within [the free space of] another [already existing] TrueCrypt volume. Even when the outer volume is mounted, it should be 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 hidden volume can be distinguished from random data." TRUECRYPT FOUND., *supra* note 32, at 38–39.

[158] *Id.* at 37–39.

[159] *See id.* at 38–39.

[160] Casey et al., *supra* note 1, at 131.

[161] *Id.*

[162] Paul Rubens, *Buyer's Guide to Full Disk Encryption*, ESECURITY PLANET, May 9, 2012, http://www.esecurityplanet.com/mobile-security/buyers-guide-to-full-disk-encryption.html.

impossible to access any files on the hard drive without the password.[163] This is a serious problem for investigators, because until recently offenders who used encryption rarely protected every piece of data on their hard drive, and would often leave at least some incriminating digital evidence in unencrypted form (for example, their internet history or files in their browser cache).[164] However, if a hard drive is protected with full disk encryption, investigators will be barred from examining this evidence without the password.[165] Not only are there a growing number of FDE software products, but hard drive manufacturers are building full disk encryption protection directly into some of the hard drives that they sell.[166] Some analysts have predicted that such encryption may become standard for all hard drives in the future.[167] The increasing use of Full Disk Encryption can considerably impede digital investigations, potentially precluding access to all the digital evidence in a case.[168] Hard drive manufacturers are also hesitant to install any kind of "backdoor" into the encryption software that could allow law enforcement to circumvent the encryption protection.[169] This means that investigators are forced to employ time-consuming and often unsuccessful brute-force techniques in the hopes of guessing the correct password.[170]

Full disk encryption presents other difficulties for investigators as well. If investigators or police turn off a suspect's computer during a search without realizing it is encrypted, the encryption software may activate and the investigators will no longer be able to access any of the data on the drive without the password, as was the case in *Boucher*.[171] Furthermore, some encrypted hard drives have a safety feature in which the hard drive essentially self-destructs and destroys any data stored on it if it detects tampering.[172]

A number of experts in the field of digital forensics have suggested different approaches and procedures for investigators to adopt in order to counter the encryption problem, which will be discussed below. However, as one researcher concluded, "[r]esearch is needed to develop new techniques and technology for breaking or bypassing full disk encryption," and without such further developments, digital forensics runs the risk of becoming obsolete in the years to come.[173]

[163] Casey & Stellatos, *supra* note 28, at 93.

[164] *Id.* at 94.

[165] *Id.* at 93.

[166] Casey et al., *supra* note 1, at 130.

[167] *Id.*

[168] *Id.* at 129.

[169] *Id.* at 130.

[170] Forte, *supra* note 4, at 19.

[171] Casey et al., *supra* note 1, at 130.

[172] *Id.*

[173] *Id.* at 134.

B. Law Enforcement Officials

Police officers and other government agents must also adapt the way in which they collect evidence when there is a possibility that the suspect used encryption. There have been numerous documented cases in which valuable evidence was lost because law enforcement officials mishandled hard drives or devices with encryption protection.[174] Law enforcement officials investigating a cybercrime are often unaware that cutting off the power on a computer before a forensic duplicate[175] of the computer's hard drive has been made can cause any encrypted volumes on the hard drive to automatically lock up, making the data within it inaccessible.[176] Not only can the mishandling of digital evidence prevent investigators from regaining access to the encrypted data, it may even prevent investigators from realizing that there is encrypted data on the hard drive in the first place.[177]

VIII. POTENTIAL SOLUTIONS TO THE ENCRYPTION PROBLEM

Since the encryption problem is not going away, and the courts have sent, at best, mixed signals about the constitutionality of compelling a defendant to give up the password to her encrypted data, it is imperative that other solutions to the problem be explored. Three solutions this article will explore are the development and invention of new tools and techniques for digital forensic investigators, improved training for law enforcement, and various legislative solutions.

A. Improved Tools and Techniques for Digital Forensic Investigators

Although encryption programs such as TrueCrypt are very difficult to crack if used with a strong password, that does not mean that there are not potential weaknesses. Exploiting mistakes made by the user can provide investigators with hints as to what the password may be, information about the files that are encrypted, and potentially even access to the encrypted data.[178] For example, if a user encrypts her data with the same or similar password she uses for her email, social media profile, or any other online website account, an investigator will likely be able to obtain the passwords to her accounts either through finding the saved passwords on her computer, or by obtaining a

[174] *Id.* at 129–130.

[175] A forensic duplicate is an exact copy of the hard drive used by forensic investigators. Investigators examine the copy instead of the original hard drive in order to avoid altering the original media. *What is a Forensic Hard Drive Imaging?*, FORENSICON, http://www.forensicon.com/resources/articles/what-is-forensic-hard-drive-imaging/ (last visited Feb. 5, 2014).

[176] Casey & Stellatos, *supra* note 28, at 95.

[177] *Id.*

[178] *See* TRUECRYPT FOUND., *supra* note 32, at 50, 83, 87.

subpoena ordering the websites to produce the user's password.[179] Obviously, the investigator will not know ahead of time whether the online account password matches the encryption password, but it will save considerable time if it does, and it is therefore worthwhile to make the effort. Furthermore, even if the passwords do not match, the investigator may still be able to enter the password into a program that runs what is called a "dictionary attack," which will attempt to guess variations of the password using different characters and numbers.[180]

A more insidious way for an investigator to obtain a user's password is to attempt to implant key-logging software onto the suspect's computer without her knowledge and before she is arrested or her home searched.[181] The software can record every keystroke the user makes, including when the user enters her encryption password. However, this can potentially raise wiretapping and invasion of privacy issues, and so far has only been utilized by the government in special circumstances.[182]

There is also some indication that powerful encryption cracking tools may be available to digital forensic investigators in the near future. Due to the Snowden leaks, it has been revealed that the National Security Agency (NSA) has been able to crack or circumvent the encryption that guards global commerce and banking systems.[183] Of course, the resources available to the NSA are not going to be available to the average digital forensic investigator.[184] Nevertheless, technological breakthroughs made by the NSA may one day trickle down to traditional investigators, such as the development

[179] DEBRA L. SHINDER, SCENE OF THE CYBERCRIME: COMPUTER FORENSICS HANDBOOK 306–315 (Ed Tittel ed., 2002); *see also* Declan McCullagh, *Feds Seek New Ways to Bypass Encryption*, CNET, Feb. 23, 2011, http://news.cnet.com/8301-31921_3-20035168-281.html.

[180] SHINDER, *supra* note 179, at 307; Margaret Rouse, *Dictionary Attack*, http://searchsecurity.techtarget.com/definition/dictionary-attack (last visited Feb. 19, 2014).

[181] *See* Kevin Poulsen, *FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats*, WIRED MAG., July 18, 2007, http://www.wired.com/politics/law/news/2007/07/fbi_spyware?currentPage=all (explaining the FBI used this technique to steal data from former crime boss Nicodemo S. Scarfo).

[182] *Id.*; *See also* Andrew D. Salek-Raham, *Carrier IQ, Pre-Transit Keystroke Logging, and the Federal Wiretap Act*, 13 N.C. J.L. & TECH. 417, 431–38 (2012) (explaining the different ways courts have interpreted the Federal Wiretapping Act in regards to key-logging).

[183] Nicole Perloth, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES, Sept. 5, 2013, http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all.

[184] Dan Goodin, *Feds Plow Resources into "Groundbreaking" Crypto-Cracking Program*, ARS TECHNICA, Aug. 30, 2013, http://arstechnica.com/security/2013/08/feds-plow-10-billion-into-groundbreaking-crypto-cracking-program/ (reporting that the NSA spends $11 billion a year on various encryption-breaking programs).

of the futuristic-sounding "quantum computer."[185] Both the NSA and civilian laboratories have been developing this revolutionary type of computer which would be "exponentially faster"[186] than any current computer, and would be capable of breaking nearly every current form of encryption.[187] Although a functioning version of the computer is still, at best, a long way off,[188] it could prove to be a potent weapon in a digital investigator's arsenal if its development is successful.

B. Improved Training for Law Enforcement

As discussed earlier, law enforcement officers are frequently unaware of how to handle digital devices that contain encryption technology, and sometimes mishandling an encrypted device can cause valuable evidence to be lost. An obvious solution to this problem is to train law enforcement officers on how to appropriately collect sources of digital evidence.[189] Proper preparation and education can dramatically increase the chances of investigators and law enforcement recovering incriminating data during a search.[190]

The Secret Service is a good example of how proper training can greatly aid in the collection of digital evidence and prevent the government from ever even needing the defendant to disclose his password. Every new agent goes through a week of training in computer forensics at the Secret Service Academy.[191] In order to avoid having to attempt to crack a suspect's encryption, the Secret Service began trying to seize suspects' computers while they are still turned on and while the encrypted volume is unlocked.[192] One technique employed by the Secret Service to ensure that the suspect is logged onto his computer when agents arrive to execute the search warrant is to attempt to initiate an online chat with the suspect and then send an agent dressed as a United Parcel Service driver to the door.[193] As Secret Service agent Stuart Van Buren explained during a computer security conference, "Traditional forensics always said pull the plug. . . . That's changing. Because

[185] Steven Rich & Barton Gellman, *NSA Seeks to Build Quantum Computer that Could Crack Most Types of Encryption*, WASH. POST, Jan. 2, 2014, http://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html.

[186] *Id.* (explaining that the computer would utilize the theory of quantum mechanics and allow the computer to do multiple calculations at a single instant).

[187] *Id.*

[188] *Id.* (explaining estimates range from less than a decade to multiple decades).

[189] Casey & Stellatos, *supra* note 28, at 96.

[190] *Id.*

[191] McCullagh, *supra* note 179.

[192] *Id.*

[193] *Id.*

of encryption . . . we need to make sure we do not power the system down before we know what's actually on it."[194]

In 2009, the Secret Service planned a raid on a notorious hacker named Albert Gonzalez, who was suspected of gaining access to around 180 million payment-card accounts from the customer databases of corporations such as OfficeMax, Target, and JCPenney.[195] Because of the expectation that the hacker would be hiding evidence inside of encrypted volumes, the agents crafted preraid and on-scene search strategies in order to maximize the opportunity to retrieve the data running on the computers before the computers were taken to a forensics lab.[196] As a result of the careful planning, the Secret Service was able to capture critical evidence at the scene of the search, even though the system was protected by powerful encryption.[197] Had the agents simply raided the home, unplugged the computers, and taken them to a forensics lab, it is likely much of the evidence would have been lost.[198]

C. Legislative Solutions

Attempts have been made in the past to solve the encryption problem with legislative action. For the most part, the legislative solutions in the United States have failed,[199] although they have had success in other countries.[200] This article will explore two possible legislative solutions that have been proposed.

1. Key Disclosure

Key disclosure statutes are currently in effect around the world.[201] Key disclosure legislation makes it a crime for a suspect or defendant to refuse to disclose his password to law enforcement.[202] Many common law countries

[194] *Id.*

[195] James Verini, *The Great Cyberheist*, N.Y. TIMES MAG., Nov. 10, 2010, http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html?ref=magazine.

[196] Casey & Stellatos, *supra* note 28, at 96.

[197] *Id.*

[198] *Id.*

[199] S*ee* Hillary Victor, *Big Brother is at Your Back Door: An Examination of the Effect of Encryption Regulation on Privacy and Crime*, 18 J. MARSHALL J. COMPUTER & INFO. L. 825 (2000) (discussing in-depth the failed legislative attempts to regulate encryption during the mid–1990s and early 2000s).

[200] *Canada Digital Policy Branch: Canada's Policy on Cryptography*, GOV'T OF CAN., http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00118.html (last modified Feb. 2, 2013); *Cybercrime Act 2001*, ELEC. FRONTIERS AUSTL., https://www.efa.org.au/Issues/Privacy/cybercrimeact.html (last visited Feb. 15, 2014).

[201] Among the list of nations that have key disclosure laws on the books are Australia, the United Kingdom, and South Africa. John Matonis, *Key Disclosure Laws Can be Used to Confiscate Bitcoin Assets*, FORBES, Sept. 12, 2012, http://www.forbes.com/sites/jonmatonis/2012/09/12/key-disclosure-laws-can-be-used-to-confiscate-bitcoin-assets/.

[202] *Id.*

have adopted the mandatory key disclosure legislation as an exception to the privilege against self-incrimination.[203]

For example, the United Kingdom's version of key disclosure, passed as part of the Regulation of Investigatory Powers Act (RIPA), allows for sentences of "up to two years for cases not involving national security or five years for those that do."[204] Since its implementation in 2007, multiple suspected terrorists have been convicted of violating RIPA, as well as suspects in less serious cases.[205]

If the United States were to implement key disclosure legislation similar to that in the United Kingdom, it would provide the lower courts with explicit instruction on how to handle the issue of compelled disclosure. Of course, passing the legislation would not permanently end the debate on compelled disclosure, as the courts could still overturn the statute if it was found to violate the Constitution.[206] However, if Congress or a state legislature were to pass a key disclosure law, it would, at the very least, bring publicity to the issue of compelled decryption and possibly spur the Supreme Court to action in deciding how to handle the issue.

2. Key Escrow Laws

Key escrow[207] systems are arrangements between a user of an encryption program and a trusted third party, approved by the government, to hold a backup of the user's password.[208] The user can contact the third party if she forgets her password, but more importantly, at least for the purposes of this article, the government could subpoena the third party for the password if there was probable cause to believe she was hiding illegal or incriminating information with her encryption.[209] This would get around any issue of self-

[203] *Id.*

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

[205] John Leyden, *Clink! Terrorist Jailed for Refusing to Tell Police his Encryption Password*, REGISTER, Jan. 16, 2014, http://www.theregister.co.uk/2014/01/16/password_refusal_earns_terror_suspect_extra_jail_time/; *Teenager Jailed for Refusing to give Police his Computer Password*, DAILY MAIL, Oct. 6, 2010, http://www.dailymail.co.uk/news/article-1318103/Teenager-jailed-refusing-police-password.html.

[206] Marbury v. Madison, 5 U.S. (1 Cranch) 137, 177–78 (1803). For further discussion of judicial review, *see* Saikrishna B. Prakash & John C. Yoo, *The Origins of Judicial Review*, 70 U. CHI. L. REV. 887 (2003).

[207] Sometimes known as "key recovery" or "trusted third-party encryption." HAL ABELSON ET AL., THE RISKS OF KEY RECOVERY, KEY ESCROW, AND TRUSTED THIRD-PARTY ENCRYPTION 1 (1997).

[208] *Id.* at 1–5.

[209] *Id.*

incrimination, since it would not be the suspect who was disclosing the password, but the third party.[210]

However, one major hurdle for implementing a key escrow system is that the idea has proven to be unpopular.[211] In the early 1990s the Clinton administration proposed a version of a key escrow system called the "Clipper Chip" initiative, which would have "offered the public high-quality [encryption] protection embedded in hardware in exchange for the government's ability to read the underlying text . . . in certain legally authorized circumstances."[212] Yet the initiative was met with harsh criticism as well as strong public mistrust, and was eventually discarded.[213] Given that American citizens' overall trust in the federal government has hit an all-time low,[214] it seems unlikely that the idea of a key escrow system will be more palatable to the public anytime soon.

IX. CONCLUSIONS

It should now be clear that the proliferation of encryption technology is causing, and will continue to cause, significant problems for law enforcement and investigators involved in investigating cybercrime. The lower courts' recent holdings protecting defendants from being compelled to decrypt their encrypted data are further exacerbating the problem. However, while the courts, prosecutors, and law enforcement officials wait for the Supreme Court to weigh in on the issue of compelled decryption, steps can be taken in the present and near future to assist in the investigation of cybercrime. Investing in new technologies and tactics for digital forensic investigators, and providing law enforcement officials with digital forensic training, can prevent valuable evidence from being lost. Legislative solutions to the encryption problem are also possible, but if enacted will likely face constitutional challenges and

[210] David B. Walker, *Privacy in the Digital Age: Encryption Policy—A Call for Congressional Action*, 1999 STAN. TECH. L. REV. 3, 40–45 (1999) (discussing how the elements of compulsion, self-incrimination, and testimonial aspects seem to be lacking).

[211] *Key Escrow*, ELEC. PRIVACY INFO. CTR., http://epic.org/crypto/key_escrow/ (last visited Feb. 1, 2014) (discussing how computer scientists, various international groups, and the European Union have all criticized key escrow).

[212] CAROLYN W. PUMPHREY, TRANSNATIONAL THREATS: BLENDING LAW ENFORCEMENT AND MILITARY STRATEGIES 73 (2000), *available at* http://www.strategicstudiesinstitute.army.mil/pdffiles/00217.pdf.

[213] *Id.*

[214] COUNCIL OF PROF'L ASS'NS ON FED. STATISTICS, TRUST IN GOVERNMENT AND GOVERNMENT STATISTICS: A SUMMARY OF PRESENTATIONS FROM COPAFS' DEC. 6, 2013 QUARTERLY MEETING 1 (2013), *available at* http://www.copafs.org/UserFiles/file/presentations/2013Dec/TrustinGovernmentandGovernmentStatisticsSummaryV2.pdf (reporting that only 19% of the public say that they trust the government in Washington "most of the time" or "just about always," which are the lowest levels since 1958).

protests from the public. However, regardless of the solutions that are adopted to combat the present encryption problem, the larger problem of technology outpacing society's ability to adapt to it will still remain. Criminals will not simply sit back and allow law enforcement and the courts to catch up. The challenge for the legal system will be how do deal with it.

J. RILEY ATWOOD*

* *Juris Doctor*, Saint Louis University School of Law, expected May 2015.