WARNING—WEAK PASSWORD: THE COURTS' INDECIPHERABLE APPROACH TO ENCRYPTION AND THE FIFTH AMENDMENT

Matthew J. Weber[*]

TABLE OF CONTENTS

* J.D., University of Illinois College of Law, 2017; B.A., History, University of California, San Diego, 2011. For helpful conversations, musings, and guidance, I owe thanks to Professors Kurt T. Lash and Andrew D. Leipold. I would also like to thank the editors, members, and staff of the Journal of Law, Technology & Policy for their immense help and useful insight. Most of all, I thank my family and friends for their constant love and support.

I. INTRODUCTION

With the growing use of cell phones, computers, and the Internet in all aspects of life, from communicating with friends and colleagues to online banking and mobile payment, the need for data encryption is clear.[1] Technology companies respond to this need by allowing for easy encryption of devices and data.[2] More than simply allowing for encryption, some companies have made it the default for their devices or operating systems.[3] While powerful encryption is useful for most consumers, it has proven to be an issue for law enforcement.[4] The new ability of consumers to encrypt data in a way that almost no one without the encryption key can decrypt poses an issue for law enforcement because even if they can obtain a warrant requiring a third party (often the company that provided the software or hardware) to decrypt the device or data, that third party often does not have the will or technical ability to comply.[5] Leaving the person being investigated or charged with a crime as the only person able to decrypt his or her data creates an issue for law enforcement because it: (1) leaves a defendant the ability to argue that providing the data requested or the encryption key could be considered self incrimination—and possibly prohibited by the Constitution; and (2) allows a

1. *See Our Approach to Privacy*, APPLE, http://www.apple.com/privacy/approach-to-privacy/ (last visited Oct. 6, 2016) (describing Apple's use of encryption in connection with the multiple uses of its products, including electronic payment, messaging, health and fitness, Internet browsing, location services, and music, among others); *Android Pay*, GOOGLE ANDROID, https://www.android.com/pay/ (last visited Oct. 6, 2016) ("You already use your phone for just about everything. Now you can pay with it, too.").

2. *See generally, e.g.*, *macOS Security*, APPLE, http://www.apple.com/osx/what-is/security/ (last visited Oct. 6, 2016); *BitLocker Drive Encryption Overview*, MICROSOFT, https://technet.microsoft.com/en-us/library/cc732774(v=ws.11).aspx (last visited Oct. 6, 2016); *Disk Encryption Guide*, LINUX RED HAT, https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/5/html/Installation_Guide/Disk_Encryption_Guide.html#idp41010592/ (last visited Oct. 6, 2016); *Google Transparency Report: Email Encryption in Transit*, GOOGLE, http://www.google.com/transparencyreport/saferemail/?hl=en/ (last visited Oct. 6, 2016); *Online Banking: Security and Support FAQs*, BANK OF AM., https://www.bankofamerica.com/onlinebanking/online-banking-security-faqs.go/ (last visited Oct. 6, 2016); *Encryption: General Questions*, BBVA COMPASS, https://www.bbvacompass.com/online-banking/faq/encryption.jsp (last visited Oct. 6, 2016).

3. *See* APPLE, IOS SECURITY: IOS 9.3 OR LATER 12 (May 2016), https://www.apple.com/business/docs/iOS_Security_Guide.pdf ("By setting up a device passcode, the user automatically enables Data Protection.").

4. David Auerbach, *Why the U.S. Doesn't Deserve a Back Door to Your Data*, SLATE (Sept. 16, 2015, 4:54 PM), http://www.slate.com/articles/technology/bitwise/2015/09/fbi_cia_nsa_want_backdoor_access_to_data_yet_they_can_t_keep_their_own_data.html; Jeff Pegues, *Paris Terror Attacks Raise Questions over Privacy, Security*, CBS NEWS (Nov. 17, 2015, 7:32 AM), http://www.cbsnews.com/videos/paris-terror-attacks-raise-questions-over-privacy-security/ (reporting that law enforcement is confident that Paris attackers used encrypted communications).

5. *Legal Process Guidelines: U.S. Law Enforcement*, APPLE (Sept. 29, 2015), http://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf ("For all devices running iOS 8.0 and later versions, Apple will not perform iOS data extractions as data extraction tools are no longer effective. The files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess.").

defendant to simply refuse to divulge the encryption key regardless of a court order.[6]

The Fifth Amendment to the United States Constitution protects a defendant from self incrimination; it states: "No person . . . shall be compelled in any criminal case to be a witness against himself . . . ."[7] Courts have interpreted the amendment to prohibit a defendant from both testifying against himself and incriminating himself through the use of testimonial evidence.[8] This prohibition is difficult to implement with the changing role of technology in society because it can create a situation where the only person able to produce the evidence is the person against whom it will be used.

For example, if the police suspect John of running a Ponzi scheme, the police can go to a judge to obtain a search warrant for John's computer. If John, like many law students, owns a MacBook Air running Apple's latest operating system, El Capitan, he can encrypt his hard drive with a few clicks of the mouse, ensuring that no one without his specific encryption key can easily access his information—though, it might be possible to break the encryption using a method known as a brute-force attack (depending on password strength, that could take decades).[9] The people investigating John's possible Ponzi scheme would likely be forced to request that John decrypt his hard drive (or provide them with the encryption key), a request that John would likely challenge, claiming it was self-incrimination.

While courts have dealt with the idea of self-incrimination since the Bill of Rights was ratified, the idea of encryption and digital data is quite new, leaving individual courts to apply an outdated doctrine to cutting edge technology.[10] This Note will discuss the confusing and sometimes contrary ways courts have applied this protection when dealing with encrypted data. It will first provide background on encryption and its implementation/history with consumers. Second, it will summarize the current framework used by courts to determine whether specific testimony or evidence is considered self-incriminating testimony—thereby triggering Fifth Amendment protections. It will then analyze the haphazard application of current case law to the continually changing world of technology, specifically how courts interpret passwords/encryption keys when defendants refuse to divulge them, claiming Fifth Amendment protections. Third, it will look to future issues courts are likely to face due to the changing technologies available to consumers, specifically the new use of biometric security, and how the government hopes to deal with encryption moving forward. This Note will address the recent issue between Apple Inc. and the United States government related to the search of the phone of one of the suspects from the deadly San Bernardino

6. U.S. CONST. amend. V.

7. *Id.*

8. United States v. Hubbell, 530 U.S. 27, 43 (2000); Fisher v. United States, 425 U.S. 391, 409 (1976).

9. OMAR CHOUDARY ET AL., INFILTRATE THE VAULT: SECURITY ANALYSIS AND DECRYPTION OF LION FULL DISK ENCRYPTION 10 (2012), http://eprint.iacr.org/2012/374.pdf.

10. Amy Davidson, *The Dangerous All Writs Act Precedent in the Apple Encryption Case*, NEW YORKER (Feb. 19, 2016), http://www.newyorker.com/news/amy-davidson/a-dangerous-all-writ-precedent-in-the-apple-case.

shooting in December 2015,[11] and it will generally address the relationship between the technology industry and the government. Lastly, it will provide a recommendation for how courts should deal with encryption and the question of what should be considered testimonial in our digital world.

II. BACKGROUND

Traditionally, when Law Enforcement Officers (LEOs) wanted to conduct a search, they would apply for a search warrant, which, if granted, would give them the right to search, and require the LEOs be given the ability to conduct their search by whomever had the ability to give access (whether the search be of a person, place, or device).[12] As times changed and technology advanced, LEOs went from requesting search warrants for homes and businesses to requesting search warrants for telephone conversations (wiretaps) and electronic data.[13] This shift required a new step, the assistance of telecommunications companies in conducting the wiretaps or the assistance of technology companies in unlocking computers or devices. The companies often simply required court orders or search warrants before complying with search requests, but once served with search warrants the companies would comply.

A. The Rise of Encryption

More than ever before, due to the ubiquity of technology today, we have become increasingly reliant on technology; from paying bills, to checking bank accounts, to making purchases at the grocery store, much of our activities are conducted using our computers or cell phones. Because of this increase in use, technology companies have made it easier for their users to protect their data through the use of encryption.[14] Initially, users who wanted to encrypt their data needed to purchase cumbersome third-party software, but today most of the prominent operating systems and technology companies provide for such encryption.[15]

B. What Is Encryption?

At its most basic level, encryption is a process by which data can be hidden in plain view.[16] Many believe encryption is an antediluvian concept, with some examples recovered from the Old Kingdom of Egypt at around 1900

11. Mikey Campbell, *FBI Contacted Apple, Received Data Related to San Bernardino Case 3 Days After Shooting*, APPLEINSIDER (Feb. 26, 2016, 9:39 PM), http://appleinsider.com/articles/16/02/27/fbi-contacted-apple-received-data-related-to-san-bernardino-case-3-days-after-shooting-.

12. *Search Warrant*, CORNELL U. L. SCH.: LEGAL INFO. INST., www.law.cornell.edu/wex/search_warrant (last visited Oct. 6, 2016).

13. *Id.*

14. *See generally* sources cited *supra* note 2.

15. *Id.*

16. *A Brief History of Cryptography*, CYPHER RES. LABORATORIES, http://www.cypher.com.au/crypto_history.htm (last visited Oct. 6, 2016).

BC.[17] At the most basic level, encryption has remained the same, a method used to convert a readable message into a series of garbled letters and numbers—indecipherable to anyone without the cypher key.[18] During the First and Second World Wars, both sides used encryption for their military communications.[19] Germany's use of the Enigma encryption machine during World War II and its subsequent capture by the allied powers played a pivotal role in the war.[20] While still based on the same general concepts, nowadays, the encryption used by technology companies, banks, and governmental agencies is typically a stronger encryption (ranging from 128- to 2048-bit encryption keys), which according to most estimates would not be technically feasible to break by normal methods.[21]

While encryption does not have to involve a computer or advanced cryptography, these days, encryption involves hundreds of characters and mathematical algorithms to encrypt a given set of data.[22] Computer encryption takes a file or set of files and uses the decryption key to convert them into an unrecognizable jumble of characters that can typically only be decrypted using the original key or a key sent to the recipient in advance.[23] Current encryption is practically indecipherable, with even minimally encrypted files taking years to decrypt.[24]

C. Encryption and Tech Companies

Encryption has changed the relationship between the government and service providers (cell phone and Internet companies). This is because typically, when served with a search warrant, companies cooperate with law enforcement to provide the information requested—if they have access to it, and have no reason to object to it.[25] But now, when served with a search warrant, cell phone providers (such as AT&T and Verizon) might be willing to provide law enforcement with the data they request, but given the prevalence

17. *Id.*; *see also* NICHOLAS G. MCDONALD, UNIV. OF UTAH DEP'T OF ELEC. & COMPUT. ENG'G, PAST, PRESENT, AND FUTURE METHODS OF CRYPTOGRAPHY AND DATA ENCRYPTION 14 (2009), http://www.eng.utah.edu/~nmcdonal/Tutorials/EncryptionResearchReview.pdf (noting that Egyptians used a simple substitution cypher).

18. *See* MCDONALD, *supra* note 17.

19. *Id.* at 8–15 (pointing to the encryption in Germany's Zimmerman Telegram, the use of Native American code talkers, and Germany's use of the Enigma encryption machine during WWII).

20. Andrew Lycett, *Breaking Germany's Enigma Code*, BBC HISTORY (Feb. 17, 2011), http://www.bbc.co.uk/history/worldwars/wwtwo/enigma_01.shtml; *The Enigma of Alan Turing*, CENT. INTELLIGENCE AGENCY (Apr. 10, 2015, 9:38 AM), https://www.cia.gov/news-information/featured-story-archive/2015-featured-story-archive/the-enigma-of-alan-turing.html; *see also* THE IMITATION GAME (Black Bear Pictures 2014).

21. Andrey Bogdanov et al., *Biclique Cryptanalysis of the Full AES*, *in* ADVANCES IN CRYPTOLOGY—ASIACRYPT 2011, at 344 (2011), http://research.microsoft.com/en-us/projects/cryptanalysis/aesbc.pdf; *see also* Numberphile, *Encryption and HUGE Numbers*, YOUTUBE (Dec. 9, 2012), https://www.youtube.com/watch?v=M7kEpw1tn50.

22. *A Brief History of Cryptography*, *supra* note 16.

23. Numberphile, *supra* note 21.

24. Mohit Arora, *How Secure Is AES Against Brute Force Attacks?*, EE TIMES (May 7, 2012, 5:29 PM), http://www.eetimes.com/document.asp?doc_id=1279619.

25. *Government Information Requests*, APPLE, http://www.apple.com/privacy/government-information-requests/ (last visited Oct. 6, 2016).

of encrypted messaging like iMessage and WhatsApp,[26] the cell phone providers often do not have access to the unencrypted data.[27] Even when messages, pictures, or phone calls are placed over the networks of the service providers, depending on the users' settings and usage, the data sent over the network can be encrypted, and therefore undecipherable to a party without the right encryption key.[28]

Messaging providers like Apple (iMessage) and WhatsApp[29] are similarly unhelpful if served with a search warrant because even though the messages are being sent over their servers, the messages are encrypted. Neither the providers nor the networks over which the messages are sent have access to the unencrypted versions of the messages, because they are encoded with end-to-end encryption (an encryption method that allows only the sender and recipient to view the message).[30] Similarly (albeit, slightly more secure), operating systems that allow their users to encrypt all or part of their disks create a situation where, even when served with a search warrant, companies (e.g., Microsoft and Apple) are unable to decrypt a hard drive without the encryption key the user selected when setting up the system.[31] These situations leave only the holder of the encryption key (likely the subject of the investigation) as the only person able to decrypt the computer.

Given that the only way to decrypt the data is by having the user enter the decryption key, law enforcement must typically get a search warrant requiring that the suspect decrypt his computer and provide an unencrypted version to law enforcement (because absent the encryption, the information is generally lawfully discoverable). This is problematic because such a search warrant would possibly violate the Fifth Amendment's protection against self-incrimination.[32] Courts that have faced this issue have differed on how to best deal with the possibility of providing law enforcement with a key that could potentially provide incriminating information when the suspect is the only source of said key.[33] For a defendant to successfully assert his protection against self-incrimination, he must show that he is being (1) compelled to provide (2) testimonial evidence that would (3) incriminate himself (as discussed in depth below).[34] The Supreme Court in *Doe v. United States* suggested that when determining if evidence is testimonial, courts can analogize to whether it is more similar to providing the combination to a wall

26. *See* APPLE, *supra* note 3 (stating that messages are encrypted by default once a user sets up a device passcode); *End-to-End Encryption*, WHATSAPP, https://www.whatsapp.com/faq/en/general/28030015 (last visited Oct. 6, 2016) (stating that messages are encrypted automatically).

27. AT&T, AT&T TRANSPARENCY REPORT (2014), http://about.att.com/content/dam/csr/transpreport/ATT_Transparency%20Report.pdf; VERIZON, TRANSPARENCY REPORT 1H 2016 (2016), http://www.verizon.com/about/portal/transparency-report/wp-content/uploads/2016/07/Transparency-Report-US-1H-2016.pdf.

28. Greg Kumparak, *Apple Explains Exactly How Secure iMessage Really Is*, TECHCRUNCH (Feb. 27, 2014), http://techcrunch.com/2014/02/27/apple-explains-exactly-how-secure-imessage-really-is/.

29. *WhatsApp Security*, WHATSAPP, https://www.whatsapp.com/security/ (last visited Oct. 6, 2016).

30. *See* Kumparak, *supra* note 28 (explaining how Apple encrypts iMessages).

31. *Use FileVault to Encrypt the Startup Disk on Your Mac*, APPLE, https://support.apple.com/en-us/HT204837 (last visited Oct. 6, 2016); *BitLocker Drive Encryption Overview*, *supra* note 2.

32. United States v. Hubbell, 530 U.S. 27 (2000); Fisher v. United States, 425 U.S. 391 (1976).

33. *Fisher*, 425 U.S. at 391.

34. *Id.* at 422.

safe or the key to a lock.[35] The Court later held in *United States v. Hubbell* that the assembly of documents could be seen as testimonial, noting that "[t]he assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox."[36] Now, courts are struggling to figure out how best to deal with encryption—is the encryption key more like a physical key or a combination? Can a court compel divulgence of a key? Can a court compel the turning over of a decrypted hard drive?

III. ANALYSIS

A. Existing Framework/Legal History

The Fifth Amendment of the Constitution protects a person from being "compelled in any criminal case to be a witness against himself . . . ."[37] This protection is one of the fundamental protections of the Bill of Rights, but for it to be invoked, a person must face being compelled to provide incriminating testimony.[38] In a typical testimonial self-incrimination case, it is often easy for the court to determine if the testimony being given is of an incriminating nature.[39] For example, a judge would likely not allow a prosecutor to force a witness to answer questions related to crimes that she is alleged to have committed, because it would clearly put the witness in danger of incriminating herself.

1. Fisher v. United States

Far more complicated, courts have to look to whether the action a person is being compelled to do is testimonial. In *Fisher v. United States*, the Supreme Court explored the testimonial nature of a compulsion to produce documents.[40] *Fisher* was a consolidation of two similar cases that had been decided inconsistently by the Third and Fifth Circuits.[41] In both cases, the Internal Revenue Service (IRS) was investigating and interviewing taxpayers regarding the preparation and filing of their tax returns.[42] Each taxpayer retained an attorney and gave them documents related to the investigation.[43] The IRS—upon learning the location of the documents it sought—served summonses on the attorneys for the documents.[44]

The attorneys in both cases fought the summonses, arguing that requiring their production would constitute a violation of their clients' Fifth Amendment

35. Doe v. United States, 487 U.S. 201, 210 n.9 (1988).
36. *Hubbell*, 530 U.S. at 43.
37. U.S. CONST. amend. V.
38. *Fisher*, 425 U.S. at 409.
39. *Id.*
40. *Id.* at 428–29.
41. *Id.* at 395–96.
42. *Id.* at 393–94.
43. *Id.*
44. *Id.*

rights.[45] The Court ultimately held that the attorneys must produce the documents because while their production might be communicative in nature (by producing the documents requested, the taxpayers are conceding that the documents exist and are in the possession of the attorneys), the message communicated is already a foregone conclusion.[46] Therefore, the Court found that producing the documents would not constitute a self-incriminating compulsion: "The existence and location of the papers are a foregone conclusion . . . . Under these circumstances by enforcement of the summons 'no constitutional rights are touched. The question is not of testimony but of surrender.'"[47]

The "foregone conclusion" rationale, first announced in *Fisher*, plays a large role in Fifth Amendment self-incrimination cases, specifically cases related to compelling the decryption of data.

2. Doe v. United States

Following the decision in *Fisher*, another case related to compelling production of possibly incriminating documents, *Doe v. United States*, came before the Supreme Court.[48] In this case, Doe, the target of a federal grand jury, was being compelled to give a foreign bank[49] permission to provide the grand jury access to certain records.[50] Doe argued that signing a document that could later be used to further an investigation against him constituted unconstitutional self-incriminating testimony.[51] The Court rejected Doe's argument, pointing out that accepting it would be too broad an interpretation of self-incriminating testimony.[52] Instead, the Court preferred a narrow interpretation of when a person is being compelled to be a witness against himself.[53]

The Court ultimately granted the grand jury order, which required Doe to sign a consent decree providing access to the Cayman Banks documents.[54] The Court rejected the argument that such an order required Doe to incriminate himself because the decree was drafted in such a way that avoided requiring Doe to admit anything.[55] The order required Doe to sign a "consent directive," which was "carefully drafted not to make reference to a specific account . . . [nor] acknowledge that an account in a foreign financial institution is in

45. *Id.* at 395.
46. *Id.* at 410–11.
47. *Id.* (quoting *In re* Harris, 221 U.S. 274, 279 (1911)).
48. Doe v. United States, 487 U.S. 201 (1988).
49. Banks in the Cayman Islands face criminal liability if they divulge customer confidential information without permission from that customer. *See* Cayman Is. Confidential Relationships (Preservation) Law No. 16 (1976), *amended by* Cayman Is. Confidential Relationships (Preservation) (Amendment) Law No. 26 (1979) §§ 3–4 (Cayman Islands bank-secrecy law).
50. *Doe*, 487 U.S. 201.
51. *Id.* at 208–09, 215–16.
52. *Id.* at 216–17.
53. *Id.*
54. *Id.* at 219.
55. *Id.* at 215–16.

existence or that it is controlled by petitioner."[56]

3. United States v. Hubbell

In a case related to the Whitewater investigation (the investigation included then President William Jefferson Clinton and his wife and now Presidential hopeful/Democratic Nominee Hillary Rodham Clinton), Webster Hubbell (a friend of the Clinton's) made a plea agreement to provide information to the special prosecutor in exchange for immunity on charges.[57] During the investigation, Hubbell was brought in front of a grand jury to verify that he was truthful and helpful as required by his plea agreement.[58] During the questioning in front of the grand jury in Arkansas, Hubbell, citing his Fifth Amendment protections, refused to answer when asked if he had documents that were covered under a served subpoena.[59] The prosecutor produced a court order requiring him to comply with the subpoena and "granting him immunity 'to the extent allowed by law.'"[60]

After being ordered by the court to produce the requested documents (subject to the immunity offered), Hubbell complied.[61] A grand jury in Washington D.C. later used the information from the documents he produced to the Arkansas court to indict him on charges unrelated to his plea agreement.[62] In reviewing his indictment, the Supreme Court noted that Hubbell's testimony was the first step in the chain of events that led to his prosecution, noting that the documents "did not magically appear in the prosecutor's office like 'manna from heaven.'"[63] The Court dismissed the indictment against Hubbell because the immunity it offered him did not include the derivative use of the information, and therefore was not the full immunity that must be offered a person being required to testify against himself.[64]

While there are sometimes easy cases for determining if a person is being compelled to give self-incriminating testimony, more often courts are needed to decide if a specific request is subject to self-incrimination protection. Courts often use the analysis from *Fisher*, *Doe*, and *Hubbell* when determining whether a person is being required to act as a witness against himself.[65] *Fisher* provides courts with the "foregone conclusion" framework—allowing prosecutors to establish that the contents of a production (as this is usually applied to production) are a foregone conclusion.[66] *Doe* provides a narrow view of what constitutes testimonial evidence, explaining that assisting in the

56. *Id.* at 215.
57. United States v. Hubbell, 530 U.S. 27, 30 (2000).
58. *Id.* at 30–31.
59. *Id.* at 31.
60. *Id.* (quoting *In re* Grand Jury Proceedings, No. GJ-96-3 (E.D. Ark., Nov. 14, 1996), App. 60–61).
61. *Id.*
62. *Id.* at 42.
63. *Id.*
64. *Id.* at 45.
65. *See, e.g.*, Commonwealth v. Gelfgatt, 11 N.E.3d 605 (Mass. 2014).
66. Fisher v. United States, 425 U.S. 391, 411 (1976).

production of evidence is not de facto testimonial.[67] *Hubbell* provides guidelines on the type of immunity required to defeat a self-incrimination challenge, suggesting that derivative-use immunity is often required.[68] As encryption is a relatively newly accessible technology,[69] courts have been slow to decide how to approach it.

B. Applying the Existing Framework to Encryption Cases

When courts look to apply the self-incrimination doctrine to encrypted devices, they start their analysis with *Fisher*,[70] *Doe*,[71] and *Hubbell*.[72] The case law and the United States Constitution suggest that a defendant cannot be compelled to testify against himself.[73] The protection against self-incrimination is triggered when evidence is: (1) compelled of a defendant, (2) testimonial, and (3) incriminating.[74] The courts have carved out an exception for evidence or testimony of which there is already a foregone conclusion—that is to say that when the "existence and location" of evidence are a foregone conclusion, a defendant can be required to turn it over, as he adds little nor concedes that he has the evidence.[75] Courts typically do not spend much time deciding if evidence is being compelled or is incriminating, but they face a more difficult time deciding whether the evidence is testimonial. A defendant can be compelled to try on clothing and give samples of blood, handwriting, or voice without it being considered testimonial.[76]

Courts have held that such examples are not testimonial because they are not either "express[ly] or implied[ly] assertion[s] of fact or belief."[77] Applying this rationale to compelled decryption is difficult because an encryption key falls somewhere between a physical item, like papers or a sample of some kind, and something more mental, like a location of possible evidence.

Courts have decided few cases dealing with compelled decryption, and cases that have been decided have not always been decided using the same analysis. Even when courts have used the same analysis, they have sometimes

67. Doe v. United States, 487 U.S. 201, 214–15 (1988).

68. United States v. Hubbell, 530 U.S. 27, 45 (2000).

69. Encryption has been around for hundreds or even thousands of years in one manner or another—but not as easy to implement or ubiquitous as it is now. *See generally* MCDONALD, *supra* note 17, at 4, 11 (noting that the earliest components of cryptography originated nearly four thousand years ago in the Egyptian town Menet Khufu but that the first unbreakable encryption algorithm was not invented until the early 1900s).

70. *Fisher*, 425 U.S. 391.

71. *Doe*, 487 U.S. 201.

72. *Hubbell*, 530 U.S. 27.

73. *See* U.S. CONST. amend. V; *Hubbell*, 530 U.S. 27; *Doe*, 487 U.S. 201; *Fisher*, 425 U.S. 391.

74. *Fisher*, 425 U.S. at 408 ("[T]he Fifth Amendment does not independently proscribe 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.").

75. *Id.* at 411.

76. United States v. Wade, 388 U.S. 218, 222–23 (1967); Gilbert v. United States, 388 U.S. 263, 266 (1967); Schmerber v. California, 384 U.S. 757, 771–72 (1966); Holt v. United States, 218 U.S. 245, 252–53 (1910).

77. Pennsylvania v. Muniz, 496 U.S. 582, 597 (1990); Nicholas Soares, Note, *The Right to Remain Encrypted: The Self-Incrimination Doctrine in the Digital Age*, 49 AM. CRIM. L. REV. 2001, 2005 (2012).

come to surprisingly different results.[78] A federal magistrate judge for the district court in Vermont held in *In re Grand Jury Subpoena to Sebastien Boucher* ("*Boucher I*") that compelling a defendant to enter a password to decrypt files on his computer without offering the necessary immunity would force the defendant to self-incriminate himself, and therefore the magistrate judge quashed the subpoena.[79] The Government appealed ("*Boucher II*") the magistrate's decision from *Boucher I*, changing its request from requiring that the defendant reveal the password to simply "requir[ing] Boucher to produce the contents of his encrypted hard drive in an unencrypted format by opening the drive before the grand jury."[80] This slight change in request was made to convince the district court that the defendant would not be forced to testify against himself but instead simply provide the information requested.[81] The court denied Boucher's motion to quash the subpoena, finding that the contents of the drive were a foregone conclusion because Boucher had already incriminated himself when he showed the computer in an unencrypted format to a border control official.[82]

Three years later, a district court in Colorado ordered a defendant to decrypt her computer in *United States v. Friscosu*.[83] In *Friscosu*, the Government prevailed because the court found that the knowledge of the existence of files located on the defendant's computer was enough to satisfy the forgone conclusion exception.[84] Most recently, the Court of Appeals for the Eleventh Circuit rejected the Government's argument that a defendant should be compelled to decrypt a drive, because it was testimonial and the Government did not meet the foregone conclusion exception and failed to provide adequate immunity (offering immunity for the act of producing the evidence, but not for its derivative use).[85]

While each of the above examples contains somewhat different facts (except the *Boucher* cases), each of the fact patterns was more or less the same. Nonetheless, the courts came to starkly different outcomes in each case—proving an issue with the standards by which a defendant can be compelled to decrypt her drive.

1. Boucher I *and* II

When Sebastien Boucher ("Boucher") and his father crossed the border into the United States from Canada, a border agent pulled them aside for a secondary screening.[86] During the screening, the agent opened Boucher's

78. *Compare Muniz*, 496 U.S. at 582, *with In re* Boucher, No. 2:06-MJ-91, 2007 WL 4246473 (D. Vt. Nov. 29, 2007).

79. *In re Boucher*, 2007 WL 4246473, at *6.

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

81. *Id.* at *4.

82. *Id.*

83. United States v. Friscosu, 841 F. Supp. 2d. 1232, 1238 (D. Colo. 2012).

84. *Id.* at 1237.

85. United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011), 670 F.3d 1335, 1338 (11th Cir. 2012).

86. *In re* Boucher, No. 2:06-MJ-91, 2007 WL 4246473 (D. Vt. Nov. 29, 2007).

laptop and, without entering a password, came across files that led him to believe that the drive contained child pornography.[87] The agent read Boucher his *Miranda*[88] rights (which Boucher immediately waived) and proceeded to question Boucher about the contents of the drive.[89] Boucher then unlocked the encrypted drive and allowed the agent to look through it.[90] Then, after consulting with a United States attorney, the agent arrested Boucher.[91] Upon Boucher's arrest, his computer was confiscated and hard drive copied—but without the password (previously entered by the Defendant), the investigators were unable to access the files previously viewed by the border agents.[92]

Without the ability to access the drive, the grand jury issued a subpoena requesting Boucher's encryption key.[93] The subpoena directed Boucher to "provide all documents, whether in electronic or paper form, reflecting any passwords used or associated with the Alienware Notebook Computer, Model D9T, Serial No. NKD900TA5L00859, seized from Sebastien Boucher at the Port of Entry at Derby Line, Vermont on December 17, 2006."[94] Boucher responded to the subpoena requesting that the magistrate judge quash the order to provide his encryption key, as it was a violation of his privilege against self-incrimination.[95] The court's analysis looked to *Fisher* for guidance, recognizing that for the Fifth Amendment to protect Boucher, the evidence must be compelled, testimonial, and incriminating in nature.[96] The court quickly pointed out that the evidence was compelled, noting that subpoenas inherently require compliance, "therefore constitu[ting] compulsion."[97] Next, the court answered in the affirmative when looking to whether the subpoena requested incriminating evidence, concluding that because "the files sought by the [G]overnment allegedly contain child pornography, the entry of the password would be incriminating."[98] The court spent the majority of its decision analyzing whether the act of entering the password should be considered testimonial.[99]

In determining whether the act of entering a password is inherently testimonial, the court attempted to analogize the facts of prior case law with the new idea of compelled decryption.[100] The court looked to whether the entering or disclosing of a password would disclose knowledge the defendant has or speaks of his guilt.[101] The court concluded that the defendant would at

87. *Id.*
88. *See* Miranda v. Arizona, 384 U.S. 436, 471 (1966) (establishing that a warning must be given to criminal suspects of their right to remain silent).
89. *In re Boucher*, 2007 WL 4246473, at *1.
90. *Id.*
91. *Id.*
92. *Id.* at *2.
93. *Id.*
94. *Id.*
95. *Id.*
96. Fisher v. United States, 425 U.S. 391, 409 (1976).
97. *In re Boucher*, 2007 WL 4246473, at *2.
98. *Id.*
99. *Id.* at *3–4.
100. *Id.* at *3.
101. *Id.*

least be forced to confirm ownership of the computer and knowledge of the encryption key, thereby forcing him into "the 'cruel trilemma' of choosing between self-accusation, perjury, or contempt."[102] The court rejected the Government's argument that decrypting his computer is similar to signing a form allowing the Government access to a bank account.[103] Finally, the court found that the Government's foregone conclusion argument failed because the Government had not seen all or even most of the contents of the drive (assuming the Government was requesting the decrypted files) nor did the Government already know the encryption key (assuming the Government was requesting the password).[104] Ultimately, the court quashed the Government's subpoena because it found that decrypting the drive would incriminate Boucher, and the Government did not meet the foregone conclusion exception.[105]

Following the magistrate's quashing of the subpoena, the Government appealed the decision.[106] In *Boucher II*, the Government argued that instead of requesting the encryption key, it would only request a decrypted drive.[107] The Government also offered more proof of prior knowledge in an effort to bolster the foregone conclusion argument.[108] The court noted that the subpoena requests "have been narrowed to requiring Boucher to produce an unencrypted version of the Z drive."[109] The court focused its analysis on the foregone conclusion exception.[110] The court noted that because the border agent had seen at least some of the documents, it met the foregone conclusion requirements: "[W]here the existence and location of the documents are known to the [G]overnment, 'no constitutional rights are touched,' because these matters are a 'foregone conclusion.'"[111] The court looked to Boucher's interaction with the border control agents, noting that the agents viewed files and "ascertained that they may consist of images or videos of child pornography," which it later determined met "Second Circuit precedent[, which only] requires the [G]overnment to demonstrate 'with reasonable particularity that it knows of the existence and location of subpoenaed documents.'"[112] The court, on appeal, held that Boucher decrypting the drive did not violate his constitutional rights because the Government met the foregone conclusion exception.[113]

102. *Id.* (quoting Doe v. United States, 487 U.S. 201, 212 (1988)).
103. *Id.* at *3–4 (referring to the decision in *Doe*, 487 U.S. at 209).
104. *Id.* at *6.
105. *Id.*
106. *In re* Boucher, No. 2:06-MJ-91, 2009 WL 424718, at *1 (D. Vt. Feb. 19, 2009).
107. *Id.*
108. *Id.*
109. *Id.* at *2.
110. *Id.* at *3.
111. *Id.*
112. *Id.*
113. *Id.* at *4.

2. United States v. Friscosu

The next case to deal with compelled decryption was *United States v. Friscosu*, which centers on Ramona Friscosu ("Friscosu"), who was under investigation when a search warrant was served to search her home.[114] During the search, investigators located (and confiscated) six computers.[115] One of the confiscated computers, the Toshiba Satellite M305 laptop ("Toshiba"), was encrypted.[116] After overhearing Friscosu and her (now estranged) husband talking about the Toshiba, and referring to it as belonging to Friscosu, the Government applied for a warrant to require her to provide the unencrypted contents of the computer.[117] Friscosu made a motion to quash the warrant, claiming that producing an unencrypted copy of the drive would violate her constitutional privilege against self-incrimination.[118]

Again, the court quickly skipped passed the questions of whether the defendant was being compelled and whether the evidence would be incriminating, dealing mostly with whether the evidence would be testimonial and if either of the exceptions applied.[119] The court did not actually address the question of whether the evidence was testimonial, because it decided that the Government met the requirements of foregone conclusion as to ownership or authenticity.[120]

The court looked to the name of the computer (RS.WORKGROUP. Ramona) to determine that Friscosu was the owner of the Toshiba, and therefore someone who would know the encryption key.[121] Because Friscosu was likely the owner of the Toshiba, which likely had the incriminating files, the court determined that the evidence was but a foregone conclusion, noting that "the fact that [the Government] does not know the specific content of any specific documents is not a barrier to production."[122] The court held that the contents of Friscosu's computer were a foregone conclusion and that because it was clear Friscosu was the owner of the Toshiba, her providing the password would similarly provide no additional testimonial evidence.[123]

3. United States v. Doe (In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011)

The most recent case to address compelled decryption was *United States v. Doe*, where the defendant ("Doe") was being investigated for charges related to child pornography.[124] Law enforcement officers began an investigation

114. United States v. Fricosu, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012).
115. *Id.*
116. *Id.*
117. *Id.*
118. *Id.*
119. *Id.*
120. *Id.*
121. *Id.*
122. *Id.* (citing *In re* Boucher, No. 2:06-MJ-91, 2009 WL 424718, at *3 (D. Vt. Feb. 19, 2009)).
123. *Id.* at 1237–38.
124. United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011), 670 F.3d 1335, 1339 (11th Cir. 2012).

when they began to suspect that a specific YouTube.com ("YouTube") account was being used to send and receive child pornography.[125] In an effort to find the person behind the YouTube account, officers used the account to find a number of IP addresses.[126] They discovered that these IP addresses were assigned to a number of hotels, which the officers then used to obtain a list of guests.[127] The officers found that Doe was the only guest each hotel had in common during the prescribed time period.[128] Officers applied for and received a warrant to "seize all digital media, as well as any encryption devices or codes necessary to access such media."[129] The officers seized two laptops and five external hard drives, some of which were encrypted.[130] Because of the encryption, forensic investigators were unable to access the drives.[131] A grand jury, though, subsequently issued a warrant requiring Doe to produce the "unencrypted contents" of the drives and "any and all containers or folders thereon."[132]

Doe refused to comply with the subpoena, citing a violation of his Fifth Amendment protections.[133] The United States attorney requested that the court grant act-of-production immunity (but notably not derivative-use immunity) to protect Doe from giving up his Fifth Amendment protections.[134] Doe refused to comply with the subpoena, resulting in Doe's incarceration for civil contempt.[135] On appeal, without much analysis, the court found that the subpoena would compel testimony (ignoring the question of whether the evidence would be incriminating), therefore triggering Fifth Amendment protections.[136]

The court spent the rest of the decision addressing whether the immunity offered by the court (act-of-production immunity without derivative-use immunity) was sufficient to meet the immunity exception of the Fifth Amendment.[137] The court held that Doe's immunity was insufficient because it only protected Doe against being prosecuted based on his production.[138] The

125. *Id.*

126. *Id.*; *see* Kathleen Hickey, *How an IP Address Can Reveal Your Location*, GCN (Apr. 26, 2011), https://gcn.com/articles/2011/04/26/ip-address-gives-location-within-half-mile.aspx (explaining that unique Internet addresses are provided to computers when they connect to the Internet). IP addresses can be used to narrow down the location of Internet traffic; in this case, the addresses were used to narrow the location down to specific hotels. *Doe*, 670 F.3d at 1339.

127. *Doe*, 670 F.3d at 1339.

128. *Id.*

129. *Id.*

130. *Id.*

131. *Id.*

132. *Id.*

133. *Id.* at 1337.

134. *Id.*

135. *Id.* at 1338.

136. *Id.* at 1341 ("An individual must show three things to fall within the ambit of the Fifth Amendment: (1) compulsion, (2) a testimonial communication or act, and (3) incrimination."); *see also* United States v. Ghidoni, 732 F.2d 814, 816 (11th Cir. 1984); United States v. Authement, 607 F.2d 1129, 1131 (5th Cir. 1979).

137. *Doe*, 670 F.3d at 1341, 1349–50 ("The district court still could have compelled Doe to turn over the unencrypted contents—and held him in contempt if he refused to do so—had the Government offered and the district court granted Doe constitutionally sufficient immunity.").

138. *Id.* at 1351.

court chose not to limit its analysis to the type of immunity the Government was offering but instead chose to look deeper into the Government's intended use of the evidence.[139] To get to this point, the court looked to the Supreme Court's decision in *Kastigar v. United States*,[140] where the Court (in a similar Fifth Amendment case, but unrelated to compelled encryption[141]) held, "If . . . the immunity granted is not as comprehensive as the protection afforded by the [Fifth Amendment] privilege, petitioners were justified in refusing to answer, and the judgments of contempt must be vacated."[142] Using *Kastigar*, the court in *Doe* rejected the use of only act-of-production immunity, noting "Supreme Court precedent is clear: *Use and derivative-use immunity establishes the critical threshold* to overcome an individual's invocation of the Fifth Amendment privilege against self-incrimination. No more protection is necessary; *no less protection is sufficient*."[143] The court reversed the district court's ruling, holding that the Government failed to provide Doe the immunities required under the Fifth Amendment.[144]

C. Encryption Law in the Future/Current Events

As technology continues to progress, courts will be faced with new and different issues related to the right to privacy and self-incrimination. With most Americans owning smartphones, we now store (and have quick access to) more information (bank information, credit cards, pictures, geolocations, schedules, text communications, etc.) than ever before on our phones.[145] Because of this change, courts will have to decide how best to apply the current law to the changing technology. Two examples of issues brought up by current technologies that have not yet been fully dealt with by the courts are: (1) biometric identification and security—which allows phones to identify users by their biometric identifiers;[146] and (2) the Government's issues with encryption and requests for less secure encryption to facilitate law enforcement.[147]

---

139. *Id.* at 1350 ("The Government stated in its letter served on Doe on April 7, 2011, and before the district court on April 19, 2011, that it would not use Doe's act of production against him in a future prosecution; but it would use the contents of the unencrypted drives against him.").

140. Kastigar v. United States, 406 U.S. 441 (1972).

141. Petitioners were held in contempt for refusing to answer questions in front of a grand jury. *Id.* at 442. The petitioners were given immunity, but contended that the immunity was not as broad as the privilege protected. *Id.* The Court held that immunity was sufficiently broad; therefore, the petitioners could be compelled to testify. *Id.* at 462. The Court noted, "Immunity from the use of compelled testimony, as well as evidence derived directly and indirectly therefrom, affords this protection. *It prohibits the prosecutorial authorities from using the compelled testimony in any respect*, and it therefore insures that the testimony cannot lead to the infliction of criminal penalties on the witness." *Id.* at 453 (emphasis added).

142. *Id.* at 449.

143. *Doe*, 670 F.3d at 1351 (emphasis added).

144. *Id.* at 1352–53.

145. Aaron Smith, *U.S. Smartphone Use in 2015*, PEW RESEARCH CTR. (Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.

146. *See* Dan Nosowitz, *The Future of Smartphone Security*, POPULAR SCI. (Sept. 10, 2013), http://www.popsci.com/gadgets/article/2013-09/future-smartphone-security (noting features that are unique to each person's body such as fingerprint and retina).

147. MANHATTAN DIST. ATTORNEY'S OFFICE, REPORT OF THE MANHATTAN DISTRICT ATTORNEY'S OFFICE ON SMARTPHONE ENCRYPTION AND PUBLIC SAFETY 13 (Nov. 2015), https://cyber.harvard.edu/

1. Biometrics and Self-Incrimination

When Apple announced the release of its then newest phone, the iPhone 5s on September 10, 2013, it also announced that the United States' most popular smartphone would for the first time implement biometric security.[148] Apple's introduction of TouchID allowed iPhone users to unlock their phones simply using a preselected fingerprint.[149] Apple included the biometric security because it combined convenience and security.[150] As Dan Riccio, a senior vice president at Apple, explained, "Your fingerprint is one of the best passwords in the world, it's always with you, and no two are exactly alike."[151] While both convenient and unique, this seemingly more secure method of unlocking a device could expose its users to unprotected self-incrimination. Using the key versus combination framework for deciding if a compulsory act is testimonial (described above), the fingerprint would seem to act much more like a key than a combination, and likely result in an iPhone owner being compelled to unlock his device.

Smartphone manufacturers implemented biometric security as a quick and seamless way for users to unlock their devices without the cumbersome traditional password.[152] Unfortunately for owners of devices that use biometric security, courts do not treat a fingerprint the same as a password. Recently, courts have ruled that biometrics are not the same as passwords when used to lock devices, and are not considered testimonial (and can therefore be compelled).[153] In 2014, a court in Virginia compelled a defendant to produce his fingerprint to unlock his smartphone, holding that such production would not be testimonial because it would not "require the witness to divulge anything through his mental process."[154] The court looked to *Hubbell* and *Fisher* when trying to determine whether to compel the defendant's fingerprint, noting that "the Defendant cannot be compelled to produce his passcode to access his smartphone but he can be compelled to produce his fingerprint to do the same."[155]

The Virginia court correctly applied the case law from *Hubbell* and *Fisher* but applied it blindly.[156] Instead of looking to the purpose of the fingerprint (a type of password), it simply looked at the physical act it was

---

pubrelease/dont-panic/DA_Report_Smartphone_Encryption_Public_Safety_11182015.pdf.

148. *Who's Winning the U.S. SmartPhone Market?*, NIELSEN, http://www.nielsen.com/us/en/insights/news/2013/whos-winning-the-u-s-smartphone-market-.html (Aug. 6, 2013); *Apple Special Event*, APPLE, at 59:55 (Sept. 10, 2013), http://www.apple.com/apple-events/september-2013/ (unveiling of iPhone 5S by Dan Riccio, Senior Vice President, Hardware Engineering).

149. *Apple Special Event*, *supra* note 148.

150. *Id.*

151. *Id.*

152. Mehedi Hassan, *How Biometrics on Smartphones Is Changing Our Lives*, M2SYS BLOG ON BIOMETRIC TECH. (July 13, 2016), http://blog.m2sys.com/biometric-resources/biometrics-on-smartphones/.

153. Commonwealth v. Baust, 89 Va. Cir. 267, 271 (2014).

154. *Id.*

155. United States v. Hubbell, 530 U.S. 27, 35–36 (2000); Fisher v. United States, 425 U.S. 391 (1976); *Baust*, 89 Va. Cir. at 271.

156. *See* Lauren Walker, *Virginia Judge Says Fifth Amendment Protects Passwords Not Fingerprints*, NEWSWEEK (Nov. 3, 2014, 4:16 PM), http://www.newsweek.com/virginia-judge-says-fifth-amendment-protects-passwords-not-fingerprints-281856 (explaining the holding in *Commonwealth v. Baust*).

requiring the defendant to do. The court analogized compelling the defendant's fingerprint (to unlock his phone) to compelling a defendant to provide a writing exemplar or blood sample but rejected the comparison between a fingerprint and a password.[157] The difference, the court found, was the lack of communication required—a defendant need not "communicate 'knowledge'" when using his fingerprint to unlock his phone.[158] Not only did the court ignore the similar purpose of the fingerprint and the password, but it also rejected the motion to compel the password, while granting the motion to compel the fingerprint.[159]

As it is such a new technology, it is still unclear if other courts will interpret fingerprints or other biometrics as testimonial; or follow the lead of the Virginia court and liken it to providing other non-testimonial evidence.

What is clear, however, is that courts will begin to answer this question more and more, with two of the most popular smartphone manufacturers[160] featuring some sort of fingerprint security—and future plans to expand the use of biometrics (Samsung is reportedly looking into retina scanners as an extra layer of security).[161] If courts continue to compel fingerprints to unlock phones, Apple vice president Dan Riccio will no longer be able to make the claim that "[y]our fingerprint is one of the best passwords in the world."[162]

2. Encryption Backdoors and the Need for Assisting Law Enforcement

The rise of encryption introduced a new set of challenges for law enforcement—whereas prior to built-in encryption, police with a search warrant could often search a suspect's phone or computer with ease, now most phones and computers come with the ability to encrypt in a way that only the suspect can decrypt.[163] With the current level of encryption available for consumers, users can very easily encrypt their phones and computers in a way that even the manufacturer cannot decrypt—effectively allowing a potential suspect to decide whether he wants to comply with a search warrant.[164] While it could be argued that most common criminals would comply (even when that might result in providing the police with incriminating evidence) because the alternative would likely be a contempt charge, many argue that an advanced level of encryption has and will continue to hamper the war on terror.[165]

Currently, it is not only possible, but easy, for people to communicate

157. *Baust*, 89 Va. Cir. at 269.

158. *Id.* at 270 (quoting United States v. Kirschner, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010)).

159. *Id.* at 271.

160. NIELSEN, *supra* note 148.

161. Lance Whitney, *Galaxy S7 May Sport Retina Scanner with Pressure Sensitive Display*, CNET (Dec. 14, 2015, 7:28 AM), http://www.cnet.com/news/samsung-galaxy-s7-might-sport-pressure-sensitive-display/.

162. *Apple Special Event*, *supra* note 148.

163. *See, e.g.*, Devlin Barrett et al., *Apple and Others Encrypt Phones, Fueling Government Standoff*, WALL ST. J. (Nov. 18, 2014, 10:30 PM), http://www.wsj.com/articles/apple-and-others-encrypt-phones-fueling-government-standoff-1416367801 ("New encryption technology that renders locked iPhones impervious to law enforcement would lead to tragedy.").

164. *See generally* MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 147 (explaining the issues encryption poses to general law enforcement).

165. *See, e.g.*, Barrett et al., *supra* note 163.

through encrypted lines in a way that authorities armed with court orders cannot access.[166] While there are many third party apps that can be used for encrypted messaging, many users need not download a special app, as any iPhone user has that ability built into iMessage (Apple's proprietary text messaging system)—by default.[167] Since the fall of 2014, Apple and Google (the makers of the software that powers over 95% of smartphones worldwide) have, by default, encrypted the disks of smartphones in a way that only the user can decrypt.[168] Many saw the approach to security by Apple and Google as direct responses to the revelations of National Security Agency spying, as exposed by Edward Snowden in 2012 and 2013.[169]

After the recent terrorist attacks in Paris,[170] San Bernardino,[171] and Nice,[172] politicians and law enforcement agencies around the world began talking about encryption and how it is aiding terrorists in planning and executing attacks.[173] This fear of encryption led to calls for the companies that write the software to include backdoors[174] for law enforcement, a suggestion

166. Darlene Storm, *The Best Secure Messaging Apps That Protect You from Surveillance*, COMPUTERWORLD (Nov. 5, 2014, 10:46 AM), http://www.computerworld.com/article/2843682/application-security/the-best-secure-messaging-apps-that-protect-you-from-surveillance.html (evaluating thirty-nine messaging products that "protect you from surveillance").

167. *See, e.g.*, Russell Brandom, *Apple Overhauls Messages with New Emoji Features and App Drawer*, VERGE (June 13, 2016, 2:54 PM), http://www.theverge.com/2016/6/13/11923988/apple-overhauls-messages-with-new-emoji-features-and-app-drawer (detailing features of iMessage, "Apple's proprietary messaging system").

168. *See Government Information Requests*, APPLE, https://www.apple.com/privacy/government-information-requests/ (last visited Oct. 6, 2016) ("On devices running iOS 8 and later versions, your personal data is placed under the protection of your passcode. For all devices running iOS 8 and later versions, Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess."); *see also* Craig Timberg, *Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police*, WASH. POST (Sept. 18, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/ (quoting Google spokesperson Niki Christoff, "For over three years Android has offered encryption, and keys are not stored off of the device, so they cannot be shared with law enforcement.").

169. Timberg, *supra* note 168.

170. Mary Brophy Marcus, *Injuries from Paris Attacks Will Take Long to Heal*, CBSNEWS (Nov. 19, 2015, 5:57 AM), http://www.cbsnews.com/news/injuries-from-paris-attacks-will-take-long-to-heal/ (noting that on November 13, 2015, terrorists committed a coordinated series of attacks in and around Paris, France, which killed 129 people and injured well over 300).

171. Sarah Parvini, *San Bernardino Shooting Victims: Who They Were*, L.A. TIMES (Dec. 17, 2015, 9:10 AM), http://www.latimes.com/local/lanow/la-me-ln-san-bernardino-shooting-victims-htmlstory.html (noting that on December 2, 2015, a couple shot and killed fourteen civilians, while seriously injuring an additional twenty-one in San Bernardino, California).

172. *Nice Attack: Who Were the Victims?*, BBC NEWS (Aug. 19, 2016), http://www.bbc.com/news/world-europe-36805164 (noting that on July 14, 2016, a group of Bastille Day celebrators were attacked by a man using a cargo truck as a weapon, killing eighty-six people and injuring over three hundred others).

173. Danny Yadron et al., *Paris Attacks Fan Encryption Debate*, WALL ST. J. (Nov. 19, 2015, 9:43 PM), http://www.wsj.com/articles/paris-attacks-fan-encryption-debate-1447987407; Seung Lee, *Did the San Bernardino Shooters Use Advanced Encryption or Not?*, NEWSWEEK (Dec. 21, 2015, 6:35 PM), http://www.newsweek.com/san-bernardino-shooters-encryption-fbi-407938.

174. A "backdoor" is a mechanism by which a third party (likely the government) can bypass the encryption and access the encrypted device. *See, e.g.*, *Encryption Backdoors*, STANFORD U. COMPUTER SCI. DEP'T, https://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/tech_encryptionbackdoors.html (last visited Oct. 8, 2016) (discussing the functionality of backdoor encryption); *see also* Joseph Lorenzo Hall, *Issue Brief: A "Backdoor" to Encryption for Government Surveillance*, CDT (Mar. 3, 2016), https://cdt.org/insight/issue-brief-a-backdoor-to-encryption-for-government-surveillance/ (discussing the

that the security experts and tech companies have resoundingly rejected. Some states have gone further and introduced bills outright banning smartphones that feature Full Disk Encryption (FDE).[175]

New York assemblymember Matthew Titone proposed a bill, A08093,[176] that would require all phones sold in the state of New York to be able to be decrypted by the manufacturer/software provider.[177] Assemblymember Titone explained in his memorandum in support of the legislation that he was introducing the bill to combat crime generally, and terrorism specifically, noting that "terrorists will use these encrypted devices to plot their next attack over FaceTime. . . . Enacting this bill would penalize those who would sell smart-phones that are beyond the reach of law enforcement."[178] California assemblymember Jim Cooper introduced a bill, AB 1681, that is nearly identical to Titone's bill.[179] Assemblymember Cooper announced the law in a press conference, explaining that he was introducing it in an effort to combat human trafficking—he noted that cell phones are now being used by pimps to communicate with and exert control over their prostitutes.[180] These proposed laws would end the current ability of criminals to refuse to unlock their devices (when served with a proper court order) because it would require the manufacturer/software provider to retain the ability to unlock the phone.[181]

The proposed laws have been received with mixed reactions, with law enforcement groups supporting them, and privacy and technology groups against them.[182] While security experts have been critical of both the New

functionality of backdoor encryption).

175. Full Disk Encryption is a technique of encrypting an entire hard disk rather than specific files on the disk. *See, e.g.*, Chris Hoffman, *What's the Difference Between BitLocker and EFS (Encrypting File System) on Windows?*, HOW-TO GEEK (Dec. 22, 2015), http://www.howtogeek.com/236719/whats-the-difference-between-bitlocker-and-efs-encrypting-file-system-on-windows/ (discussing full disk encryption). FDE is thought to be more secure than other forms of encryption because the drive (including the unused portions) is encrypted—and all new files are automatically encrypted, rather than the user manually selecting which files to encrypt. *Id.*

176. A08093, 2015–2016 Gen. Assemb., Reg. Sess. (N.Y. 2015) ("Any smartphone that is manufactured on or after January first, two thousand sixteen, and sold or leased in New York, shall be capable of being decrypted and unlocked by its manufacturer or its operating system provider.").

177. *Id.* While the legislation does not explicitly ban the sale of encrypted phones, it does so implicitly because an encrypted device that can be decrypted by a third party is hardly encrypted at all. *Id.*

178. N.Y. State Assemb., Memorandum in Support of Legislation, http://assembly.state.ny.us/leg/?default_fld=&leg_video=&bn=A08093&term=2015&Memo=Y (last visited Oct. 8, 2016).

179. AB-1681, 2015–2016 Gen Assemb., Reg. Sess. (Cal. 2016) ("This bill would require a smartphone that is manufactured on or after January 1, 2017, and sold in California, to be capable of being decrypted and unlocked by its manufacturer or its operating system provider. The bill would, except as provided, subject a seller or lessor that knowingly failed to comply with that requirement to a civil penalty of $2,500 for each smartphone sold or leased. The bill would prohibit a seller or lessor who has paid this civil penalty from passing any portion of the penalty on to purchasers of smartphones.").

180. *See* Assemb. Jim Cooper, *Cooper Introduces Human Trafficking Investigation Legislation*, CAL. STATE ASSEMB. DEMOCRATIC CAUCUS (Jan. 20, 2016, 9:17 AM), http://asmdc.org/members/a09/news-room/video-gallery/cooper-introduces-human-trafficking-investigation-legislation (explaining the purpose of the new bill he is introducing and noting the prevalent use of smartphones in the human trafficking world, specifically by pimps and prostitutes—many of whom are being kept against their will).

181. A08093, *supra* note 176; AB-1681, *supra* note 179.

182. Tom Risen, *New York Bill Aims to Ban Encrypted Phones*, U.S. NEWS (Jan. 15, 2016, 5:46 PM), http://www.usnews.com/news/articles/2016-01-15/new-york-bill-aims-to-ban-encrypted-phones; Cyrus R. Vance, Jr., *Apple and Google Threaten Public Safety with Default Smartphone Encryption*, WASH. POST (Sept. 26, 2014), https://www.washingtonpost.com/opinions/apple-and-google-threaten-public-safety-with-default-

York and California bills, pointing to the near impossibility of providing both a secure device and a backdoor for law enforcement, the fact remains that if passed, these laws would have a large impact (New York and California represent two of the three most populous states in the Union, and combined comprise more than fifty-six million people).[183] It is unclear if a state-by-state implementation of encryption plan is constitutional. If either or both laws are passed, they will likely face opposition from technology companies on the basis of their interfering with interstate commerce.[184]

3. San Bernardino Shooting and the All Writs Act

On December 2, 2015, a San Bernardino County Department of Health employee and his wife perpetrated the deadliest mass shooting since Newtown—killing fourteen of his co-workers and injuring twenty-one.[185] Following the shooting, police investigated and pursued the suspects, eventually engaging in a firefight, killing both shooters.[186] In the days and weeks following the shooting, law enforcement investigated the shooting, both to find the motive behind the shooting and to find any possible co-conspirators.[187]

On December 3, 2015, U.S. Magistrate Judge David Bristow issued a search warrant, giving law enforcement the power to search the shooters' home and car.[188] In the ensuing search, law enforcement officers found, among other things, an Apple iPhone 5c, which they later found to have been issued to one of the shooters by his San Bernardino County employer.[189] Like they had done many times before, the FBI approached Apple with the iPhone it found in the suspect's car, requesting that Apple extract the data from the seized iPhone—

---

smartphone-encryption/2014/09/25/43af9bf0-44ab-11e4-b437-1a7368204804_story.html; Cyrus Farivar, *Yet Another Bill Seeks to Weaken Encryption-by-Default on Smartphones*, ARS TECHNICA (Jan. 21, 2016, 4:00 AM), http://arstechnica.com/tech-policy/2016/01/yet-another-bill-seeks-to-weaken-encryption-by-default-on-smartphones/; Andy Greenberg, *Proposed State Bans on Phone Encryption Make Zero Sense*, WIRED (Jan. 27, 2016), http://www.wired.com/2016/01/proposed-state-bans-on-phone-encryption-make-zero-sense/; HAROLD ABELSON ET AL., KEYS UNDER DOORMATS: MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS (July 7, 2015), https://internetpolicy.mit.edu/sites/default/files/documents/MIT-CSAIL-TR-2015-026.pdf.

183. *2010 Census Data: Resident Population Data*, U.S. CENSUS BUREAU, http://www.census.gov/2010census/data/apportionment-pop-text.php (last visited Oct. 6, 2016). The 2010 Census reported that New York had a population of 19,378,102 people, and California had a population of 37,253,956 people; compared to the total American population of 308,745,538 people. *Id.*

184. *See, e.g.*, Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970) (establishing balancing test for dormant Commerce Clause jurisprudence). Selling phones with different hardware/software depending on the state the phone would be sold in would likely be a burden for smartphone makers.

185. Erik Ortiz, *San Bernardino Shooting: Timeline of How the Rampage Unfolded*, NBC NEWS (Dec. 3, 2015, 11:28 PM), http://www.nbcnews.com/storyline/san-bernardino-shooting/san-bernardino-shooting-timeline-how-rampage-unfolded-n473501.

186. *Id.*

187. *Id.*

188. Elliot Hannon, *Judge Orders Apple to Help FBI Hack San Bernardino Shooter's Phone*, SLATE (Feb. 16, 2016, 8:43 PM), http://www.slate.com/blogs/the_slatest/2016/02/16/judge_orders_apple_to_help_fbi_unlock_san_bernardino_shooter_s_phone.html.

189. *Id.*; Fred Kaplan, *How Apple's Stand Against the FBI Could Backfire*, SLATE (Feb. 19, 2016, 6:26 PM), http://www.slate.com/articles/technology/future_tense/2016/02/how_apple_ceo_tim_cook_s_stand_against_the_fbi_could_backfire.html.

except this time, Apple could not comply with the request.[190] Apple was able to provide *some* information to the FBI, but was unable to decrypt the device.[191] Apple was unable to comply with the FBI's request due to changes it had made to the iPhone Operating System (iOS) a year before, positioning Apple and the Federal Government for a clash that both had been preparing for since 2014.[192]

On February 16, 2016, the United States attorney requested an order (that was later granted[193]) compelling Apple to *assist* in the unlocking of the San Bernardino shooter's phone.[194] Instead of obtaining an order for Apple to break its encryption (an order the FBI understood Apple would be technically incapable of complying with), the FBI requested an order requiring Apple to assist in the unlocking of the phone.[195] The court order compelled Apple to write software that bypasses two of the iPhone's security features: (1) a delay introduced when an incorrect passcode is entered;[196] and (2) a self-destruct feature by which an iPhone destroys its data after ten incorrect passcode attempts.[197] This order—if complied with—would have allowed the FBI to connect the shooter's updated[198] iPhone to a computer, which has a program capable of guessing all the possible passcode combinations,[199] without the delay or possibility of wiping.[200]

Apple decided to fight the order, though it should be noted that Apple has assisted the FBI's investigation, providing the Bureau with all the data the

190. Will Oremus, *Apple vs. the FBI*, SLATE (Feb. 17, 2016, 7:44 PM), http://www.slate.com/articles/technology/future_tense/2016/02/apple_s_stand_against_the_fbi_is_courageous_it_s_also_good_for_apple.html; Ben Thompson, *Apple Versus the FBI, Understanding iPhone Encryption, the Risks for Apple and Encryption*, STRATECHERY (Feb. 17, 2016), https://stratechery.com/2016/apple-versus-the-fbi-understanding-iphone-encryption-the-risks-for-apple-and-encryption.

191. Campbell, *supra* note 11.

192. Marcy Wheeler, *Why This iPhone?*, SLATE (Feb. 19, 2016, 1:26 PM), http://www.slate.com/articles/technology/future_tense/2016/02/the_apple_fbi_encryption_battle_is_over_an_iphone_unlikely_to_yield_critical.html.

193. Order Compelling Apple, Inc. to Assist Agents in Search, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. ED 15-0451M, 2016 WL 618401 (C.D. Cal. Feb. 16, 2016) [hereinafter Order Compelling Apple, Inc.].

194. Government's *Ex Parte* Application for Order Compelling Apple Inc. to Assist Agents in Search, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. ED 15-0451M (C.D. Cal. Feb. 16, 2016) [hereinafter Government's *Ex Parte* Application], https://www.wired.com/wp-content/uploads/2016/02/SB-shooter-MOTION-seeking-asst-iPhone.pdf.

195. *Id.*

196. *See* APPLE, *supra* note 3 (explaining key security features: the delay, triggered after four incorrect passcode attempts imposes a one-minute delay after the fifth incorrect attempt, a five-minute delay after the sixth incorrect attempt, a fifteen-minute delay after the seventh and eighth incorrect attempts, and a one-hour delay after the ninth incorrect attempt).

197. *See id.* (explaining key security features such as that the iPhone can be set to *wipe* all its data after the tenth incorrect passcode attempt; this wipe is achieved by discarding the encryption key from accessible memory, making the entire hard disk unintelligible).

198. *See* Order Compelling Apple, Inc., *supra* note 193 (indicating that Apple would upload a custom operating system to the shooter's phone modifying security settings—though not specifically decrypting).

199. There are ten thousand possible combinations for a four-digit numeric passcode, or one million possible combinations for a six-digit numeric passcode. APPLE, *supra* note 3.

200. *See id.* (explaining that even without the delay, the iteration counter imposes an eighty millisecond delay, and therefore, all the possible combinations could theoretically be guessed in under five hours).

shooter backed up to the iCloud[201] prior to turning off the iPhone's auto-backup to the cloud.[202]

The order compelling Apple to write the above-referenced software was based primarily on the 1789 All Writs Act ("Act"), which allows courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[203] In this case, the Government requested that the court compel Apple to assist in satisfying a lawful search warrant, by which the court gave the Government the power to search the suspect's iPhone 5c.[204] This order—which Apple CEO Tim Cook has argued to be unprecedented in a statement released on the company's website[205]—set the Government and Apple on a collision course, in a battle that both the tech industry and law enforcement community had been expecting since tech companies began offering relatively unbreakable encryption on consumer devices.[206] Ultimately, this question was not answered because the FBI was able to use other means to unlock the device in question.[207]

a. The All Writs Act

Historically, courts use the Act to effectuate their lawful orders when there has been no statutory framework to follow.[208] The Government's motion cited cases in which the Act was used by courts to compel parties to assist in effecting court orders—suggesting that Apple be similarly required to assist technically in the search of the phone, pursuant to the court's order.[209] Unlike the cases cited by the Government, Apple in this case was being ordered to create a new operating system, pursuant to the Government's unique specifications.[210] The Government argued that because Apple's devices cannot be updated without a unique "digital signature,"[211] it has ensured that it cannot

201. Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. ED 16-10CM (SP) (C.D. Cal. Feb. 16, 2016) [hereinafter Apple Inc.'s Motion to Vacate Order], https://epic.org/ amicus/crypto/apple/In-re-Apple-Motion-to-Vacate.pdf; Amy Davidson, *The Dangerous All Writs Act Precedent in the Apple Encryption Case*, NEW YORKER (Feb. 19, 2016), http://www.newyorker.com/news/amy-davidson/a-dangerous-all-writ-precedent-in-the-apple-case.

202. *Id.*

203. 28 U.S.C. § 1651 (2012).

204. Government's *Ex Parte* Application, *supra* note 194.

205. Letter from Tim Cook, CEO, Apple. Inc., to Customers (Feb. 16, 2016), http://www.apple.com/customer-letter/ ("The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand.").

206. Danny Yadron et al., *Inside the FBI's Encryption Battle with Apple*, GUARDIAN (Feb. 18, 2016, 1:00 PM), http://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple.

207. *See* Kim Zetter, *The FBI Drops Its Case Against Apple After Finding a Way into That iPhone*, WIRED (Mar. 28, 2016, 6:18 PM), https://www.wired.com/2016/03/fbi-drops-case-apple-finding-way-iphone/ (explaining how the FBI ultimately gained access to the suspect's phone).

208. Andrew Crocker, *Judge to DOJ: Not All Writs*, ELEC. FRONTIER FOUND. (Oct. 12, 2015), https://www.eff.org/deeplinks/2015/10/judge-doj-not-all-writs.

209. Government's *Ex Parte* Application, *supra* note 194.

210. *Id.*

211. The "digital signature" is Apple's unique encryption key—without which, a phone cannot be

be seen as "far removed"[212] from the matter. The Government noted in the memorandum of points and authority to its motion to compel, that Apple's assistance was necessary at the time based on its unique ability to "cryptographically sign code,"[213] leading the Government to request that Apple write the specific code and upload it onto the iPhone in question.

b. Department of Justice Argument

In its application for an order compelling Apple's assistance in unlocking the seized iPhone, the Government argued that the Act gave the court the power to mandate Apple's assistance.[214] The Government argued that the Act can require "a third party to provide non-burdensome technical assistance," citing the Supreme Court in *New York Telephone Co*.[215] The Court in that case created a three-factor test for determining whether it could compel action by a third party using the Act: (1) whether a party is far removed from the controversy; (2) whether requiring action would impose an undue burden on the party; and (3) whether the assistance from the party was necessary for the successful fulfilling of the underlying court order (in this case a search warrant for the iPhone).[216]

The Government argued that it met the three-factor test imposed by the Court in *New York Telephone Co.*, first arguing that Apple was not far removed from the unlocking of the iPhone.[217] The Government argued that because Apple "designed, manufactured and sold the [iPhone] and wrote and owns the [operating system]," it cannot be seen as far removed from the controversy.[218] The Government further argued that Apple cannot be far removed because it is the only party able to update the software[219] in a way that would comply with the court's order.[220] The Government's argument was supported by the Supreme Court's decision in *New York Telephone Co.*, which held that a non-governmental third party can be compelled to act when its "facilities were being employed to facilitate a criminal enterprise."[221]

The Government next argued that the order is not unduly burdensome for

updated. *Id.*

212. *Id.* (pointing to United States v. N.Y. Tel. Co., 434 U.S. 159, 174 (1977)).

213. Government's Motion to Compel Apple Inc. to Comply with This Court's February 16, 2016 Order Compelling Assistance in Search, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. ED 16-10CM (SP) (C.D. Cal. Feb. 16, 2016) [hereinafter Government's Motion to Compel Apple Inc.], https://www.justice.gov/usao-cdca/file/826836/download.

214. *Id.*

215. *Id.* at 11–12.

216. *N.Y. Tel. Co.*, 434 U.S. at 174.

217. Government's *Ex Parte* Application, *supra* note 194, at 13.

218. *Id.*

219. *Id.* ("The same software Apple is uniquely able to modify . . . . Especially but not only because iPhones will only run software cryptographically signed by Apple . . . there is no other party that has the ability to assist the government in preventing these features from obstructing the search ordered by the court pursuant to the warrant.").

220. *Id.*

221. *Id.* at 13–14 (quoting *N.Y. Tel. Co.*, 434 U.S. at 174); Government's Motion to Compel Apple Inc., *supra* note 213, at 8.

Apple. The Government pointed to Apple's regular business of writing software code to suggest that it could not claim that writing a specific code would impose an undue burden.[222]

Lastly, the Government argued that it met the necessity requirement because Apple created a situation whereby it is the only entity that can write software to update its iOS.[223] Because iPhones require Apple's crypto-signature,[224] Apple's assistance would have been required to effectuate the search warrant had the Government not found an alternative way to unlock the phone. The Government noted that it was not requesting that Apple provide the unencrypted contents of the phone, but instead that it simply assist in the Government's testing of passcodes to unlock the phone.[225]

c. Apple's Argument

Apple responded to the Government's motion to compel by arguing that it should not be required to further comply with the Governments request.[226] The reason, Apple argued, was because the Government's request (1) relied on a misapplication of the Act, (2) violated the First Amendment by compelling speech by Apple, and (3) violated the Fifth Amendment's due process clause.[227]

Apple's argument was generally centered on the Government's improper application of the Act. When deciding whether to apply the Act, the Supreme Court held that when a statute addresses an underlying issue specifically, that statute, and not the Act, is "controlling."[228] Apple first argued that the Act cannot require the action requested by the Government, suggesting that the Act allows courts to "fill in gaps in the law" to exercise the power they already have, but not the "free-wheeling" ability to change existing law.[229] Apple argued that the court lacked the authority to compel it to comply with the order because Congress contemplated (when passing the Communications Assistance for Law Enforcement Act) bestowing upon courts the power to require such a compulsion, but ultimately chose to exempt manufacturers of telecommunications equipment[230] from implementing "any specific design of equipment . . . features, or system configurations . . . ."[231]

---

222. Government's *Ex Parte* Application, *supra* note 194, at 14–16.

223. *Id.* at 16.

224. *Id.* at 7.

225. *Id.*

226. Campbell, *supra* note 11.

227. Apple Inc.'s Motion to Vacate Order, *supra* note 201; *see also* Campbell, *supra* note 11.

228. "The All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute. Where a statute specifically addresses the particular issue at hand, it is that authority, and not the All Writs Act, that is controlling. Although that Act empowers federal courts to fashion extraordinary remedies when the need arises, it does not authorize them to issue ad hoc writs whenever compliance with statutory procedures appears inconvenient or less appropriate." Pa. Bureau of Corr. v. U.S. Marshals Serv., 474 U.S. 34, 43 (1985).

229. Apple Inc.'s Motion to Vacate Order, *supra* note 201, at 14.

230. *Id.* at 16.

231. In the section of CALEA entitled, "Design of features and systemes configurations," the statute states:

This subchapter does not authorize any law enforcement agency or officer—

Facing new challenges to law enforcement's ability to fight crime, Congress, in 1994, passed the Communications Assistance for Law Enforcement Act (CALEA). CALEA grants law enforcement investigative powers but also limits what can be required from manufacturers and service providers.[232] When passing CALEA, Congress had the chance to address whether it would require companies to assist law enforcement in the manner being requested by the FBI—but ultimately chose not to make any such requirement. In fact, CALEA provides that telecommunications carriers (which Apple points out it is not) are not required to decrypt or "ensur[e] the government's ability to decrypt" unless the communication was encrypted by the carrier (and even then the carrier must "possesses the information necessary to decrypt"—which Apple does not).[233] Congress's inclusion of some language related to encryption, but omission of requirements to compel assistance in decryption, shows that it considered such a compulsion but ultimately rejected it.

Apple argued that CALEA specifically addresses whether to require manufacturers and service providers to aid decryption.[234] Because CALEA speaks on the specific matter, the Act should not be the statute to rule, but instead should be trumped by CALEA's provisions. The Supreme Court held in *Pennsylvania Bureau of Corrections v. U.S. Marshall Service* that the Act does not allow courts to issue writs when compliance with existing statutes would be simply "inconvenient or less appropriate,"[235] as compliance with CALEA would be in this situation.

Apple next addressed the Government's use of *United States v. New York Telephone Co.*, ultimately drawing distinctions between the Government's requests and those of the telephone company in *New York Telephone Co.*[236] Apple argued that the Government did not show that it satisfied the three-factor test provided by the Court in that case.[237]

First, Apple is too far removed from the underlying case. Unlike the telephone company, which owned the lines being allegedly used to "facilitate a criminal enterprise on a continuing basis,"[238] Apple contended that it is a private company that does not own the phones or have any connection to the data on the phone.[239] Second, the Government's request would have imposed

---

(A) *to require any specific design of equipment, facilities, services, features, or system configurations to be adopted* by any provider of a wire or electronic communication service, *any manufacturer of telecommunications equipment*, or any provider of telecommunications support services; or

(B) to prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services.

47 U.S.C § 1002(b)(1) (emphasis added).

232. *Id.* § 1002(b).

233. *Id.* § 1002(b)(3).

234. Apple Inc.'s Motion to Vacate Order, *supra* note 201, at 6–8.

235. Pa. Bureau of Corr. v. U.S. Marshals Serv., 474 U.S. 34, 43 (1985).

236. United States v. N.Y. Tel. Co., 434 U.S. 159 (1977).

237. Apple Inc.'s Motion to Vacate Order, *supra* note 201, at 20.

238. *N.Y. Tel. Co.*, 434 U.S. at 174.

239. Apple Inc.'s Motion to Vacate Order, *supra* note 201, at 21.

an "unprecedented and oppressive burden" on Apple.[240] While the telephone company was required to assist the Government in installing pen registers[241]—a device that telephone companies used frequently in conducting their normal business[242]—in the instant case, the Government was asking Apple to create an entirely new operating system in an effort to assist the Government's attempts to unlock the phone.[243] Apple asserted that such an undertaking violated the Act's prohibition against adversely affecting the third party or imposing an undue burden.[244] Third, Apple contended that its assistance was only necessary because of the actions of the FBI earlier in its investigation.[245] While the court suggested in *New York Telephone Co.* that there was "no conceivable way" for the FBI to successfully carry out its court-ordered investigation,[246] Apple argued that the FBI did not face such a situation, but instead, through its own actions, created a need to turn to the Act.[247]

d. Outcome

It seems that both Apple and the Government foresaw this potential clash coming since Apple (and other tech companies) began encrypting devices sold to consumers and/or offering end-to-end encrypted messaging. Many in the media have questioned whether this was the right test case for either side.[248] For the Government, it seems to be a good test case because the crime in question is terrorism-related, and the underlying crime was well reported and remains in the minds of the American public.[249] Unfortunately for the Government's case, the case was not time-sensitive.[250] While the phone might help in the investigation of a crime, there does not seem to be a pressing need for the phone to be unlocked immediately.[251] For Apple, the case does not seem to the best test case for whether it should be required to assist in the unlocking of one of its devices because the suspect is widely assumed to be

240. *Id.* at 23.

241. A "pen register" is a device used to record phone numbers dialed on specific phone lines. *Pen Register*, CORNELL U. L. SCH.: LEGAL INFO. INST., https://www.law.cornell.edu/wex/pen_register (last visited Oct. 6, 2016).

242. *N.Y. Tel. Co.*, 434 U.S. at 174–75 (noting that the phone company regularly used pen registers in normal operations).

243. Apple Inc.'s Motion to Vacate Order, *supra* note 201, at 23–28.

244. *Id.*

245. *Id.* at 11. The FBI has acknowledged that it worked with the phone's owner (San Bernardino County) to reset the iCloud password in an effort to unlock the iCloud backup. *Id.* at 11 n.21. Apple argued that had the county and the FBI not reset the password, "this litigation may not have been necessary," as it could have initiated a remote backup of the phone and subsequently produced an updated backup to investigators. *Id.* at 11.

246. *N.Y. Tel. Co.*, 434 U.S. at 175.

247. Apple Inc.'s Motion to Vacate Order, *supra* note 201, at 29–30.

248. Kaplan, *supra* note 189; Wheeler, *supra* note 192.

249. Kaplan, *supra* note 189; Will Oremus, *Irate DOJ Dismisses Apple's Fight with the FBI as a "Brand Marketing Strategy"*, SLATE (Feb. 19, 2016, 6:02 PM), http://www.slate.com/blogs/future_tense/2016/02/19/department_of_justice_motion_mocks_apple_s_fbi_fight_as_a_brand_marketing.html; Kaveh Waddell, *The Optics of Apple's Encryption Fight*, ATLANTIC (Feb. 17, 2016), http://www.theatlantic.com/technology/archive/2016/02/why-apple-is-fighting-the-fbi/463260.

250. Wheeler, *supra* note 192.

251. *Id.*; Letter from Tim Cook to Customers, *supra* note 205.

guilty of the heinous murder of fourteen co-workers.[252] It has also been noted that this particular iPhone model (an iPhone 5c) is not one which Apple should be fighting over as it is not the most up-to-date phone or software, and the government-requested solution would not work on future iPhone models.[253] At least in public opinion, Apple may benefit from standing by its customers, claiming that writing the software requested by the Government would unnecessarily put all iOS users at risk.[254] Tim Cook noted in his open letter to customers that "[t]hey have asked us to build a backdoor to the iPhone."[255]

On March 21, 2016 (the day before the hearing on the order), the Government submitted an ex parte application for a continuance, requesting that the court continue the hearing to April 5, 2016.[256] The Government requested the continuance because, since initially requesting the hearing, a third party approached the FBI suggesting that the party had a different method to unlock the phone.[257] Some experts have suggested that the FBI paid over $1 million to unlock the phone in question.[258] This new method, if successful, would not only make Apple's assistance unnecessary, but also destroy the Government's argument under the Act. The Government requested additional time to test the new method before deciding whether it has eliminated the need for Apple's assistance.[259] Ultimately, the court vacated the original order, rendering both Apple and the Government's motions moot.[260]

While this might appear to be an opportunity for both sides to take a step back and devise a procedure moving forward, it is likely only pushing this issue down the road. Apple's newest phones are not as easy to break into (at least not using this type of method),[261] which might lead the Government to move towards mandating backdoors. While it is unclear where either party goes moving forward, it is clear that this fight is far from over; it is all but certain that the Government will come back with another request for Apple to build, as Tim Cook described it, "something . . . too dangerous to create."[262]

252. Kaplan, *supra* note 189; Oremus, *supra* note 249; Waddell, *supra* note 249.

253. Dan Guido, *Apple Can Comply with the FBI Court Order*, TRAIL OF BITS BLOG (Feb. 17, 2016), http://blog.trailofbits.com/2016/02/17/apple-can-comply-with-the-fbi-court-order; Thompson, *supra* note 190.

254. Letter from Tim Cook to Customers, *supra* note 205; Oremus, *supra* note 190.

255. Letter from Tim Cook to Customers, *supra* note 205.

256. Government's *Ex Parte* Application for a Continuance, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexis IS300, California License Plate 35KG203, No. ED 16-10CM (C.D. Cal. 2016), https://cryptome.org/2016/03/usg-apple-191.pdf.

257. *Id.*

258. Lily Hay Newman, *The FBI Paid More than $1.3 Million to Unlock the San Bernardino iPhone. Is That a Good Deal?*, SLATE (Apr. 21, 2016, 6:10 PM), http://www.slate.com/blogs/future_tense/2016/04/21/the_fbi_paid_more_than_1_3_million_to_unlock_the_san_bernardino_iphone.html.

259. Government's *Ex Parte* Application for a Continuance, *supra* note 256.

260. Order Vacating February 16, 2016 Order, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. ED 16-10CM (SP) (C.D. Cal. Mar. 29, 2016), https://www.justsecurity.org/wp-content/uploads/2016/03/FBI-Apple-CDCal-Order-Vacating-Previous-Order.pdf.

261. *See* APPLE, *supra* note 3, at 7–9 (describing the "Secure Enclave" on newer iOS devices).

262. Letter from Tim Cook to Customers, *supra* note 205.

IV. RECOMMENDATIONS

A. Compelled Decryption

In the four cases summarized above, it is clear that while the case law has largely remained the same, the courts have interpreted relatively similar sets of facts in very different ways.[263] The courts should update the case law to reflect the realities of the digital age. Doing so would make for a more uniform standard provided to defendants, regardless of forum. Courts should look to specific standards for:

- What makes evidence testimonial?
- What makes something a foregone conclusion?
- What level of immunity is sufficient to compel production?

When analyzing similar sets of facts in *Friscosu* and *Doe*, different courts came to starkly different conclusions regarding the foregone conclusion exemption.[264] Looking forward, courts should adequately define what constitutes a foregone conclusion (simply knowledge that a specific *type* of information *would* be on a computer or knowledge that *specific files* are on a computer). The courts should also determine what level of immunity is sufficient—though there is precedent from the Supreme Court on the subject, it is not uniformly followed.

More generally, courts should understand that encryption and new technology do not easily fit in the existing framework of the Fifth Amendment. It has been difficult to determine whether a password should be compelled because it fails to fall under the antiquated framework (is it more like a key to a strongbox or a combination?). Instead of attempting to make the existing framework apply to the newest technology, courts should move toward a new framework that takes into account the changing technology and what it represents. The Framers never could have imagined that citizens could walk around with devices that provided them access to all of their most sensitive information—and because of that, we should look to change how we interpret access to that information.

B. Current Events and Looking Forward

Technology companies and criminals have been in an ever-increasing arms race when it comes to encryption. The technology companies continually strive to make the best products for their customers (which often include a combination of ease of use and security), while wrongdoers seek to access consumer data. This situation leads the technology companies to attempt to make more secure devices in an effort to protect their consumers. Unfortunately, this leads to a conflict with law enforcement because the security offered to protect consumers against criminals can also be used to hide

263. *See supra* Section III.B.

264. *Compare* United States v. Friscosu, 841 F. Supp. 2d. 1232 (D. Colo. 2012), *with* Doe v. United States, 487 U.S. 201 (1988) (coming to starkly different conclusions).

consumer data from legitimate legal searches.[265] Courts have been slow to address this quickly changing industry.

The rise of biometric security on consumer devices (mostly fingerprint scanners on smartphones) seemed for most consumers to be a perfect combination of ease of use and security, but ultimately it has been found to be less secure (against a search warrant) than a typical alphanumeric password.[266] This is unfortunate for consumers because it is far more convenient to use a fingerprint scan to unlock a device than enter a password (which someone might be able to find out); but, a fingerprint can be compelled under the Fifth Amendment—and a password (typically) cannot be.[267] Courts should move to interpret all unlocking methods (password, fingerprint, retina scan, etc.) the same when deciding whether they are protected under the Fifth Amendment. This would be a better system because ultimately, when used as a password, a fingerprint scan is equally testimonial to an alphanumeric password—instead of having to enter a complex password, a user simply uses her biologic password—her fingerprint.[268]

While mandating encryption backdoors for the government is not a question for the courts to answer (at least not yet), it is an idea that has recently received a lot of attention. It is difficult to strike a balance between consumer privacy and national security. On one hand, technology companies argue that implementing any sort of backdoor would inherently render their devices less secure; on the other, the Government has argued that such strong encryption limits its ability to keep the United States safe against terrorism.[269] It is unlikely—at least as of now—that the bills being brought up in New York and California prohibiting encryption on smartphones will pass, but with the rising fear of terrorism, it is not inconceivable that the United States Congress will begin to look at the idea.

Congress should not limit the ability for technology companies (i.e., phone manufacturers) to allow encryption on their devices. This would harm millions of law abiding citizens, making their personal data accessible more easily, while only forcing criminals and terrorists to download apps (often

265. Russell Brandom, *In the Apple Encryption Fight, the FBI Is Now on China's Side*, VERGE (Mar. 16, 2016, 10:02 AM), http://www.theverge.com/2016/3/16/11244396/apple-vs-fbi-encryption-china-source-code-backdoor.

266. Elliot Williams, *Your Unhashable Fingerprints Secure Nothing*, HACKADAY (Nov. 10, 2015), http://hackaday.com/2015/11/10/your-unhashable-fingerprints-secure-nothing/.

267. *See generally* United States v. Friscosu, 841 F. Supp. 2d. 1232 (D. Colo. 2012) (discussing whether a person is required to divulge encrypted password); *see also* Jack Linshi, *Why the Constitution Can Protect Passwords but Not Fingerprint Scans*, TIME (Nov. 6, 2014), http://time.com/3558936/fingerprint-password-fifth-amendment/ (discussing why the Constitution protects passwords but not fingerprints); Reed Albergotti, *Judge Rules Suspect Can Be Required to Unlock Phone with Fingerprint*, WALL ST. J. (Oct. 31, 2014, 5:07 PM), http://blogs.wsj.com/digits/2014/10/31/judge-rules-suspect-can-be-required-to-unlock-phone-with-finger print/ (discussing a Virginia court ruling that allows police to compel fingerprints but not passwords).

268. *See* Commonwealth v. Baust, 89 Va. Cir. 267 (2014) (holding that compelling defendant to produce *password* to his encrypted cell phone would violate his Fifth Amendment privilege against self-incrimination but compelling defendant to produce *fingerprint* to his encrypted cell phone did not implicate defendant's Fifth Amendment privilege against self-incrimination).

269. *See* Mark Surman, *Mozilla Chief: FBI Snooping at Apple "Back Door" Makes You Less Safe*, CNN (Feb. 18, 2016, 4:34 PM), http://www.cnn.com/2016/02/18/opinions/apple-encryption-backdoor-fbi-surman/ (discussing the dangers of the state decoding citizens' encrypted data).

made by foreign-based companies) that allow for such encryption.[270] There is little (if any) evidence that terrorists are using the encryption offered by phone manufacturers when planning and implementing their attacks,[271] and even if they were, prohibiting such technology would only have them use third party apps. The importance of the fight on terror cannot be minimized, but this is not the solution.

C. Apple and the All Writs Act

The fight between Apple and the Government was long coming, and though it is on hold for now, it will continue to be an issue until the Supreme Court rules on whether the All Writs Act can be used to mandate assistance from a third party in the way requested. Unlike most of the cases discussed in this Note, this case had nothing to do with the Fifth Amendment, but instead revolved around whether a third party company can be made to assist in the unlocking (or decryption) of a device it manufactured.[272] The courts should rule that companies like Apple and Google cannot be made to provide this type of assistance, because they are too far removed and it would be an undue burden.

While it is likely that a very similar case will come back to the courts, though with a newer iPhone or an iPhone running a more up-to-date software, it could be that Apple is not technically able to provide even the assistance requested in this case. Tech pundits have speculated that Apple has a number of options to tie its hands further when it comes to assisting the Government.[273] It is unclear whether such strong encryption for consumer devices is a good idea, but what is clear is that technology companies plan to continue to provide it,[274] and this will continue to be an issue between those companies and governments that want lawful access.

V. CONCLUSION

Well before computers were in consumer households or cell phones in the pockets of most Americans, the courts came up with a framework by which they could determine whether defendants could be compelled to provide

270. Andrew Crocker, *The California Bill to Undermine Smartphone Encryption Actually Got Worse*, ELEC. FRONTIER FOUND. (Apr. 8, 2016), https://www.eff.org/deeplinks/2016/04/california-bill-undermine-smartphone-encryption-actually-got-worse.

271. *But see* Matt Hamblen, *Paris Attacks Demand "Wake-up Call" on Smartphone Encryption*, COMPUTERWORLD (Nov. 16, 2015, 12:51 PM), http://www.computerworld.com/article/3005426/mobile-security/paris-attacks-demand-wake-up-call-on-smartphone-encryption.html (expressing the concern of the growth of cheap or free smartphone apps like WhatsApp or Chatsource that encrypt messages, which kept security agencies from any advance warning of what was being planned).

272. *See* Kevin Johnson et al., *FBI Hacks into Terrorist's iPhone Without Apple*, USA TODAY (Mar. 29, 2016, 1:51 PM), http://www.usatoday.com/story/news/nation/2016/03/28/apple-justice-department-farook/82354040/ (discussing that the Justice Department had withdrawn its legal action against Apple).

273. Nathaniel Mott, *Take That, FBI: Apple Goes All in on Encryption*, GUARDIAN (June 15, 2016, 6:42 AM), https://www.theguardian.com/technology/2016/jun/15/apple-fbi-file-encryption-wwdc ("Since its battle with the FBI, Apple has made a number of important changes to increase security and tighten encryption.").

274. *Id.*

certain information, while still invoking their Fifth Amendment protections.[275] The framework has worked well in many aspects, as it has been applied to situations the judges in *Fisher*, *Doe*, and *Hubbell* could never have contemplated.

Applying the compelling-of-documents framework provided by the above-referenced cases to encryption keys and decryption has forced courts to messily apply non-technical ideas to the digital world. Courts must at the very least update some of these frameworks to apply to an increasingly digital world. The foregone conclusion doctrine, for example, can become overbroad in a society where most consumers have access to their most sensitive and important documents on their smartphone or laptop. It is a foregone conclusion that most readers of this Note could access their bank records and intimate conversations with friends and family on both their smartphones and computers—but is this what the *Fisher* court had in mind when it laid out the doctrine? Probably not, because it was 1976.

Looking forward, the courts must find a way to deal with the current and future technology that law enforcement will face. As it stands now, certain types of security are not protected by the Fifth Amendment and other types are[276]—while this might make sense by applying strict Fifth Amendment case law, it does not make sense when applying rational thinking. One way of unlocking a device should receive the same protection (or lack of protection) as others. Instead of looking at the method of the security, courts should look at the purpose.

275. *See* Fisher v. United States, 425 U.S. 391 (1976).
276. Linshi, *supra* note 267.