UNLOCKING THE RIGHT AGAINST SELF-INCRIMINATION: A PREDICTIVE ANALYSIS OF 21ST CENTURY FIFTH AMENDMENT JURISPRUDENCE

MADELINE LEAMON†

I. INTRODUCTION

Long gone are the days of land-lines, flip-phones and chunky desktop computers. Today's technology penetrates every facet of individuals' personal, work and private lives. As technology has progressed to accommodate and simplify the lives of its users, product manufacturers, specifically Apple Inc., have strived to provide cutting-edge biometric security technology to their devices to protect user information from intrusion.[1]

With the advent of this cutting-edge biometric security technology, the necessary question that closely follows is whether, under the Fifth

† B.A., 2016, University of Michigan; Juris Doctor, expected 2019, Wayne State University Law School. I would like to thank Marcy Tayler, Tayler Leamon and Chris Struble for their unwavering love and support. In addition, I would like to thank Professor Peter Henning and the *Wayne Law Review* editors for their time and effort with this Note.

1. Rene Ritchie, *How Touch ID Works: Making Sense of Apple's Fingerprint Identity Sensor*, iMORE (Sept. 14, 2013), https://www.imore.com/how-touch-id-works.

Amendment, the content and information stored on people's devices is secure from forced compulsion. The self-incrimination clause of the Fifth Amendment effectively blocks a defendant from being forced to serve as a witness against himself.[2] As strong as this constitutional protection is, the Supreme Court has traditionally categorized a defendant's self-incriminating testimony as either physical or communicative in nature, with only communicative testimony entitled to Fifth Amendment protection.[3] In sum, the Fifth Amendment applies only when a defendant is compelled to make an incriminating testimonial statement.[4]

On its face, this seems like a simple line drawing scenario. However, the line that once distinguished physical and communicative compulsions has been eroded with the development of new technology that implicates both physical and communicative qualities. As this Note will discuss, biometric passwords do not fit neatly within physical or testimonial categories—instead falling somewhere in between.

This Note seeks to address the Fifth Amendment implications that would arise if a defendant in a criminal proceeding is compelled to unlock a digital device secured with biometric technology. The pertinent question is whether new password technology, although different in form from the traditional alphanumeric password, still carries with it the Fifth Amendment protections that the traditional alphanumeric password possesses.

Part II of this Note discusses the prominent Supreme Court case law developing the Fifth Amendment generally. Additionally, it explores the lower court case law pertaining to alphanumeric-password-protected devices, as well as the current framework that courts are operating in when it comes to the treatment of TouchID technology and the Fifth Amendment. Part III of this Note argues that courts currently misapply the Fifth Amendment privilege against self-incrimination to TouchID cases and specifically how the same analysis would logically apply to FaceID cases in the future. This Note argues that the current, formalistic approach to conceptualizing the Fifth Amendment privilege against self-incrimination is not expansive enough to protect defendants who choose to encrypt their devices with biometric security technology.

Part IV of this Note broadly examines how courts should rule when faced with the question of forced compulsion regarding TouchID and FaceID, particularly when a defendant invokes their Fifth Amendment right against self-incrimination. A biometric password is a password in the traditional sense. Because of the strong and direct link between the

2. Doe v. United States, 487 U.S. 201, 210 (1988).
3. Fisher v. United States, 425 U.S 391, 409 (1976).
4. *Id.* at 408.

device's content and the individual who unlocked it, the biometric password possesses meaningful testimonial qualities that should entitle it to Fifth Amendment protection. This Note suggests that compelling a defendant to provide their biometric password, namely a fingerprint passcode or using facial recognition technology to unlock their device, must receive the same constitutional protections afforded to any other form of testimonial evidence. This interpretation of the Fifth Amendment's protection not only gives credence to the underlying intent behind the privilege, but allows the privilege to be applied to modern day society with veracity and purpose.

II. BACKGROUND

As of 2017, there are an estimated 700 million iPhones in use worldwide.[5] As iPhone use grows, demand for the most convenient and easy-to-use security technology will continue to increase. In 2007, Apple launched its first iPhone with a classic four-digit password, eventually allowing for a stronger alphanumeric passcode to increase security for users.[6] Flash forward to 2013 with the release of the iPhone 5s, Apple introduced its first iteration of biometric security: TouchID.[7] This technology allowed the iPhone to capture high resolution photos of the user's fingerprint to serve as the password to unlock the device rather than an alphanumeric password.[8] If TouchID failed to recognize a person's fingerprint, the iPhone would prompt the four-digit password to unlock the device.[9] TouchID served as the predominant form of biometric security for several years, giving users what they thought was the most convenient, fast and secure method of protecting the contents of their devices.[10]

In November 2017, Apple introduced the iPhone X and FaceID, its latest biometric security technology, and effectively replaced TouchID on future Apple devices.[11] FaceID is currently the most cutting-edge biometric security paradigm, allowing users to utilize Apple's True

5. Don Reisinger, *Here's How Many iPhones Are Currently Being Used Worldwide*, FORTUNE (March 6, 2017), http://fortune.com/2017/03/06/apple-iphone-use-worldwide/.

6. *See* Ritchie, *supra* note 1.

7. *Id.*

8. *Id.*

9. *Id.*

10. Michael deAgonia, *What is Face ID? Apple's New Facial Recognition Tech Explained*, COMPUTERWORLD (Nov. 1, 2017, 2:57 AM), https://www.computerworld.com/article/3235140/apple-ios/what-is-face-id-apples-new-facial-recognition-tech-explained.html.

11. *Id.*

Depth infrared camera system to capture a depth map of the human face using 30,000 precise pin-points of light to serve as the password authentication of the device.[12] Unlike TouchID, FaceID is passive, simply requiring a person to glance at their iPhone to unlock it, regardless of changes in facial hair, sunglasses, hats or hoods.[13]

Security features such as TouchID and FaceID have increased the convenience and accessibility of Apple's devices for its users. Although the consumer-facing benefits of the sleek design and speed of the technology are appealing, the average consumer is blind to the alarming constitutional concerns that such technology inherently presents.[14] Both Fourth and Fifth Amendment jurisprudence pose intriguing and critical questions regarding whether the government can compel an individual to unlock their device using TouchID and FaceID. Although Apple is not the only company to utilize biometric security software on its devices, Apple's products are the most popular and current technology available on the market.[15]

Biometric security technology has caused far reaching legal dilemmas that the judicial system has been forced to answer in recent years.[16] One of the primary legal issues that surrounds the use of biometric security technology arises under the context of the Fifth Amendment, which protects a defendant from forced self-incrimination.[17] The courts have interpreted the Fifth Amendment to protect a defendant from being forced to testify against himself as well as incriminating himself through testimonial evidence.[18] With the recent introduction of biometric security technology on devices, the question of what qualifies as "testimonial" is heavily debated.[19] While the Fifth Amendment right against self-incrimination is not a new concept to courts, the idea of biometric security technology, which encrypts a

---

12. *Id.*

13. *Id.*

14. *See* Kara Goldman, *Biometric Passwords and the Privilege Against Self-Incrimination,* 33 CARDOZO ARTS & ENT. L.J. 211, 214 (2015).

15. *Technology & Telecommunications: Global Apple iPhone Sales from 3rd Quarter 2007 to 4th Quarter 2017*, STATISTA (Nov. 2017), https://www.statista.com/statistics/263401/global-apple-iphone-sales-since-3rd-quarter-2007/.

16. *See* NAT'L ACAD. OF SCI., BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES, 95–115 (Joseph N. Pato & Lynette I. Millett eds., 2010), https://www.ncbi.nlm.nih.gov/books/NBK219896/pdf/Bookshelf_NBK219896.pdf.

17. U.S. CONST. amend. V.

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

19. *In re* Single-Family Home & Attached Garage, No. 17 M 85, 2017 U.S. Dist. LEXIS 170184 at *7 (N.D. Ill. Feb. 21, 2017).

person's device by using the external human body, is new and unique to Fifth Amendment jurisprudence.

A. Background on the Fifth Amendment Case Law

The Fifth Amendment states, "No person . . . shall be compelled in any criminal case to be a witness against himself..."[20] Traditionally, a defendant may invoke his Fifth Amendment privilege against self-incrimination in any proceeding in which "testimony is legally required when his answer might be used against him in that proceeding or in a future criminal proceeding or when it might be exploited to uncover other evidence against him."[21] Specifically, the privilege protects against the compulsion of "testimonial disclosures."[22] Therefore, a witness may not invoke the privilege for "non-testimonial" compulsions.[23]

The Supreme Court delineated what qualifies as "non-testimonial" in a line of early, yet extremely influential cases.[24] Distinguishing "communicative" from "physical" or "bodily" evidence, the Court established through these cases that the latter does not receive Fifth Amendment protection.[25] In *Holt v. United States,*[26] the Court held that compelling a prisoner to put on a particular piece of clothing so a witness could identify him was not a "communication" protected by the Fifth Amendment privilege against self-incrimination.[27] In *Schmerber v. California,*[28] the Court held that the privilege could not be invoked because the compulsion of a blood sample was not communicative and, therefore, "non-testimonial" in nature.[29] In *United States v. Dionisio,*[30] the Court held that the production of a voice exemplar, which entails the characteristics of a person's voice and tone, is far different than the contents of a specific conversation, and is "non-testimonial" in nature, so

20. U.S. CONST. amend. V.

21. CONG. RESEARCH SERV., S. Doc No. 108–17,THE CONSTITUTION OF THE UNITED STATES OF AMERICA ANALYSIS AND INTERPRETATION: ANALYSIS OF CASES DECIDED BY THE SUPREME COURT OF THE UNITED STATES TO JUNE 28, 2002, 1394–96, (2004), http://www.gpo.gov/fdsys/pkg/CDOC-108sdoc17/pdf/CDOC-108sdoc17.pdf.

22. *Id.* at 1396.

23. *Id.*

24. *See, e.g.,* Schmerber v. California, 384 U.S. 757 (1966); Holt v. United States, 218 U.S. 245 (1910).

25. *Schmerber,* 384 U.S. at 764.

26. 218 U.S. 245 (1910).

27. *Id.* at 252–53.

28. *Schmerber,* 384 U.S. at 757.

29. *Id.* at 761.

30. 410 U.S. 1 (1973).

the privilege could not be invoked.[31] In *United States v. Wade*,[32] the Court held that standing in a police line-up, like a voice exemplar, was not communicative, and was therefore "non-testimonial" in nature and beyond the scope of the privilege.[33] Lastly, in *Gilbert v. California*,[34] the Court held that the compulsion of a hand-writing exemplar did not violate the privilege against self-incrimination because the privilege only reaches compulsory communications, but a "mere handwriting exemplar, in contrast to the content of what is written... is an identifying physical characteristic outside its protection."[35]

As demonstrated by this line of cases, the Fifth Amendment privilege against self-incrimination applies to any *communication* of the accused, whether that is physical or vocal.[36] However, the privilege does not protect against the compulsion of physical or bodily evidence such as blood samples, appearing in court wearing a particular item of clothing, producing a writing or voice exemplar, or standing in a police lineup.[37] Each of these activities are considered "non-testimonial" and are beyond the scope of the privilege.[38] On the other hand, to be considered testimonial, an accused's communication "must itself, explicitly or implicitly, relate a factual assertion or disclose information."[39]

B. When The Lines Are Unclear—Is The Evidence Testimonial? Non-testimonial? Both?

Although the Supreme Court identified specific examples of physical and bodily evidence in its early line of cases, the door of interpretation was left open where the line distinguishing testimonial versus non-testimonial evidence was less clear. In the following cases, the Supreme Court confronted the hard question of deciding whether the compulsion of a piece of evidence is considered testimonial when the line is blurry.[40] Moreover, the Court dealt with what is considered a major limitation on

---

31. *Id.* at 14.
32. 388 U.S. 218 (1967).
33. *Id.* at 223.
34. 388 U.S. 263 (1967).
35. *Id.* at 266–67.
36. *Wade*, 388 U.S. at 223.
37. *See, e.g.,* Schmerber v. California, 384 U.S. 757 (1966); Holt v. United States, 218 U.S. 245 (1910); *Wade*, 388 U.S. at 223.
38. *See, e.g., Schmerber*, 384 U.S. at 764.
39. Doe v. United States, 487 U.S. 201 (1988) (citing Fisher v. United States, 425 U.S 391 (1976)).
40. *See, e.g.*, Fisher v. United States, 425 U.S. 391 (1976).

an individual's right against self-incrimination—the Foregone Conclusion Doctrine.[41]

In *Fisher v. United States*,[42] the Supreme Court touched on the difficult issue of compelling documents at trial.[43] Specifically, documents of taxpayers being investigated for civil and criminal liability under federal tax laws, which they supplied to their private accountants and lawyers.[44] The defense attorneys argued that it would violate their client's Fifth Amendment right against self-incrimination if they were required to disclose the documents to the Internal Revenue Service.[45] The Court held that the attorneys were required to produce all of the requested documents because the information within, and the existence of the documents themselves, was a "foregone conclusion."[46] The Court found that the admission of the existence of the documents did not rise to the level of testimony which demands Fifth Amendment protection.[47] The Court stated that the compulsion of the documents "does not compel oral testimony; nor would it ordinarily compel the taxpayer to restate, repeat, or affirm the truth of the contents of the documents sought."[48]

In *Fisher*, the Court announced the "Foregone Conclusion Doctrine," on which many lower courts have relied on when compelling individuals to unlock their devices.[49] Under the "Foregone Conclusion Doctrine," if the government already knows the substantive information that is contained in the testimony it seeks to compel, then the content of the testimony can be compelled because the content is considered a "foregone conclusion."[50] Because the defendant's testimony adds little or nothing to the government's case against him, the Foregone Conclusion doctrine is viewed as a limitation on one's Fifth Amendment rights because one may be forced to compel information or documents in some situations even if it is self-incriminating.[51]

---

41. *Id.*
42. *Id.*
43. *Id.* at 428–29.
44. *Id.* at 394.
45. Fisher, 425 U.S. at 395.
46. *Id.* at 411.
47. *Id.*
48. *Id.* at 409.
49. *See* United States v. Hubbell, 530 U.S. 27, 44–45 (2000); *see, e.g.*, *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012); United States v. Fricosu, 841 F. Supp. 2d 1232, 1235 (D. Colo. 2012).
50. Fisher, 425 U.S. at 409–11.
51. *Id.* (citing *In re* Harris, 221 U.S. 274, 279 (1911)).

A critical detail to note is that *Fisher* was a fact-specific case.[52] Had the government not already known the substantive information contained in the compelled testimony, the compulsion of such documents by the defendant could have represented an implicit admission of guilt.[53] For example, the disclosure of such documents could have shown that Fisher possessed the incriminating documents used to prosecute him.[54] Simply stated, the Court looked beyond the incriminating information contained in the documents and reasoned that the production of documents was physical, rather than communicative, in nature because the defendant was merely handing over information that was already voluntarily produced and known about.[55] As a result, the taxpayers could not avoid the subpoena and had to produce the documents.[56]

Following *Fisher* came *Doe v. United States,*[57] which also dealt with the government compelling the production of possibly incriminating documents.[58] This was a Supreme Court case in which the defendant, who was being indicted by a federal grand jury, was being compelled to release foreign bank records from the Cayman Islands in the form of a consent decree.[59] Doe invoked his Fifth Amendment privilege and argued that the decree releasing the documents could later be used against him if he were to sign it.[60] The Court rejected the defendant's argument and required him to release the records by signing the consent decree.[61] The Court found that the act of signing the decree was non-testimonial because, although it allowed the government "access to a potential source of evidence, the directive itself [did] not point the government toward hidden accounts or otherwise provide information that [would] assist the prosecution in uncovering evidence."[62] The defendant's Fifth Amendment rights were not violated.[63] The Court

52. *Id.* at 411. The court held that the attorneys were required to produce the documents. *Id.* at 412–14. The court recognized that, although their production might be communicative in nature, compliance with the subpoena would concede that the documents exist and are in the possession of the attorneys. *Id.* For that reason, the message communicated within the documents was already a foregone conclusion, therefore not implicating the protection against testimonial self-incrimination. *Id.*

53. *Id.* at 411.

54. *Id.* at 409–410.

55. *Id.* at 409–11.

56. *Id.* at 410.

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

58. *Id.*

59. *Id.* at 201.

60. *Id.* at 214.

61. *Id.* at 215.

62. *Id.*

63. *Id.*

stated, "in order to be testimonial, [a criminal defendant's] communication must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a 'witness' against himself."[64] Essentially, the *Doe* Court ruled that the defendant's signature had no testimonial significance because the signature itself did not communicate any information to the government.[65]

In his dissent in *Doe*, Justice Stevens advocated for a different outcome that courts could apply when deciding whether the government can compel an individual to decrypt a secured device.[66] Justice Stevens argued that, although it may not have directly communicated testimony, forcing Doe to sign the consent decree implicitly communicated to the jury that Doe had the power and authority to release the records and, thus, anything found after would be directly related to him.[67] Justice Stevens claimed that forcing Doe to sign the consent decree was comparable to forcing Doe to help the government establish their case against him, thereby violating his privilege against self-incrimination.[68]

Although *Fisher* essentially found that the compelled production of documents was a "forgone conclusion," the Court in both *Fisher* and *Doe* held that, even if the compelled testimony revealed implicit "communicative" information incriminating the defendant, the Fifth Amendment privilege against self-incrimination does not protect such testimony.[69] To arrive at this conclusion, the Court in both cases engaged in analysis that weighed the testimonial and non-testimonial nature of the compulsion in a way that departed from *Schmerber*.[70] The clear-cut method of categorizing testimonial and non-testimonial evidence eroded in these cases, especially with the development of the "Foregone Conclusion Doctrine" into the analysis.[71]

C. Case Law on Password Protected Devices

As discussed above, the Supreme Court has slowly transitioned away from a strict, categorical approach to an adaptable framework that allows courts to weigh the fact of a specific case when deciding whether a compelled act is testimonial and within the scope of the Fifth

64. *Id.* at 210.
65. *Id.* at 201.
66. *Id.* at 219–21 (Stevens, J., dissenting).
67. *Id.* at 219 (Stevens, J., dissenting).
68. *Id.* at 220 (Stevens, J., dissenting).
69. *Id.* at 219. Fisher v. United States, 425 U.S. 391, 414 (1976).
70. Schmerber v. California, 384 U.S. 757, 764 (1966).
71. *See* Goldman, *supra* note 14, at 224–225.

Amendment privilege.[72] Moving beyond compelled testimony in general to compelled decryption of password protected devices, lower courts must look to the Supreme Court decisions in *Fisher* and *Doe* to determine the scope of the Fifth Amendment privilege against self-incrimination in the modern context of password protection.

In *In re Grand Jury Subpoena to Sebastien Boucher* (hereinafter referred to as *Boucher I & Boucher II*),[73] Boucher was pulled aside while in a security clearing line at the United States border with Canada.[74] He was directed to a secondary inspection, during which his laptop was found.[75] The officer conducting the security check opened up his laptop, and without entering a password, searched the laptop's files and found approximately 40,000 pornographic images, several of which he believed contained child pornography.[76] Boucher waived his Miranda rights and allowed the security guard to view his laptop files in private.[77] This led to the discovery of several child pornographic images and videos.[78] He was arrested, but when the officers confiscated his laptop, it was shut down.[79] Weeks later, when the officers attempted to search the laptop's hard drive for more evidence, they found that the files were password protected, which hindered their access to the hard drive containing the incriminating evidence.[80]

In *Boucher I*, the magistrate judge had to decide whether the act of entering a password ought to be considered testimonial, as Boucher invoked his Fifth Amendment right when subpoenaed to unlock his laptop with the password only he knew.[81] The magistrate recognized that "for the privilege to apply, the communication must be compelled, testimonial, and incriminating in nature."[82] Consequently, the magistrate court found that forcing Boucher to either disclose the password or enter it into the computer itself would require him to produce self-incriminating evidence.[83] The magistrate determined that a password, because it is in the witness's mind, is testimonial and beyond the reach of

72. *See supra* section II.B.

73. *In re* Grand Jury Subpoena (Boucher), No. 2:06-mj-91, 2007 U.S. Dist. LEXIS 87951 (D. Vt. Nov. 29, 2007).

74. *Id.* at *2.

75. *Id.*

76. *Id.*

77. *Id.* at *4.

78. *Id.*

79. *Id.*

80. *Id.*

81. *Id.* at *5.

82. *Id.* at *6 (citing Fisher v. United States, 425 U.S. 391, 408 (1976)).

83. *Id.* at *7.

a grand jury subpoena.[84] Essentially, the compulsion of the password would be the functional equivalent to claiming ownership of whatever was on the laptop, as Boucher was the only one who knew the password.[85]

In *Boucher II*, the district court reversed the magistrate's decision.[86] The government made a "forgone conclusion" argument, claiming that they already knew what was on the encrypted files, so therefore no privilege applied.[87] The magistrate court had found that the government's foregone conclusion argument failed on the basic premise that, while the government saw *some* of the files on Boucher's laptop, it did not view *all* or even *most* of them, neither did it know "of the existence of other files on drive Z that may [have] contain[ed] incriminating material."[88] Despite this finding, the district court analyzed this question under a different lens and held that "[w]here the existence and location of the documents are known to the government, 'no constitutional rights are touched' because these matters are a 'foregone conclusion.'"[89]

Although the magistrate decision was reversed, the district court's opinion would have likely come out differently had the officers not had the opportunity to view the hard-drive with such particularity when the laptop was confiscated the first time.[90] The district court reasoned that because Boucher had admitted that the laptop was his, and had provided the officers with access to the hard drive at a prior time, he was compelled to provide an unencrypted version of the hard drive to the officers.[91] Had these events not occurred, it can be presumed that the district court would have affirmed the magistrate court's decision and found that the password could not be compelled.[92]

In *United States v. Kirschner*,[93] the defendant was indicted by a grand jury on three felony counts of receipt of child pornography.[94] The government issued subpoenas regarding the defendant's computers and also ordered that he provide all passwords associated with each computer

84. *Id.* at *10.

85. *Id.*

86. *In re* Grand Jury Subpoena (Boucher), No. 2:06-mj-91, 2009 U.S. Dist. LEXIS 13006 at *10 (D. Vt. Feb. 19, 2009).

87. *In re Boucher*, 2007 U.S. Dist. LEXIS 87951, at *13–14.

88. *Id.* at *15.

89. *In re* Grand Jury Subpoena (Boucher), No. 2:06-mj-91, 2009 U.S. Dist. LEXIS 13006 at *8 (D. Vt. Feb. 19, 2009) (citing Fisher v. United States, 425 U.S. 391, 411 (1976)).

90. *Id.* at *10.

91. *Id.*

92. *Id.*

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

94. *Id.* at 666.

and its files to obtain the evidence needed to prove that he was in possession of child pornography.[95] The defendant filed a motion to quash the grand jury subpoena, asserting his Fifth Amendment privilege against self-incrimination.[96] The court held that compelling the defendant to reveal the password for the computer, ". . . requires Defendant to communicate 'knowledge,' unlike the production of a handwriting sample or a voice exemplar" and that such a compulsion would require him to make a "testimonial" communication, and thus violated his right against self-incrimination.[97] Simply stated, the act of producing his passwords was deemed to be "testimonial" because the defendant would be forced to disclose the knowledge he possessed mentally, regarding the password, which was the foundation of his indictment.[98]

III. ANALYSIS

While Apple's TouchID is innovative, convenient, and allows for high security in the practical sense, the reality is that it could expose iPhone users to self-incrimination without Fifth Amendment protection.[99] As *Boucher I*, *Boucher II*, and *Kirschner* demonstrate, when a device is password protected, the password itself is considered "testimonial" and, therefore, cannot be compelled, unless considered a foregone conclusion.[100] Although alphanumeric passwords and TouchID passwords are essentially identical, courts are currently granting different Fifth Amendment protections for each as the cases below demonstrate.

A. Current Case Law Pertaining To TouchID—What Are The Courts Saying?

With the relatively recent implementation of this technology into the iPhone, case law pertaining to TouchID is limited. Despite the limited number of cases, the courts that have heard this issue have ruled that devices secured with TouchID are not functionally as secure as devices

95. *Id.*
96. *Id.*
97. *Id.* at 669.
98. *Id.* at 668–69.
99. *See* Goldman, *supra* note 14, at 224–225.
100. *In re* Grand Jury Subpoena (Boucher), No. 2:06-mj-91, 2007 U.S. Dist. LEXIS 87951, at *7 (D. Vt. Nov. 29, 2007); *In re* Grand Jury Subpoena (Boucher), No. 2:06-mj-91, 2009 U.S. Dist. LEXIS 13006, at *7 (D. Vt. Feb. 19, 2009); Kirschner, 823 F. Supp. 2d at 668–69.

secured with an alphanumeric password.[101] More importantly, the use of TouchID on a device is not considered a testimonial act and can therefore be compelled, falling beyond the scope of Fifth Amendment protection.[102]

In *Commonwealth v. Baust,*[103] a Virginia Circuit Court required a defendant to produce his fingerprint to unlock his smartphone.[104] The defendant was charged with strangling a victim and causing injury.[105] The defendant purportedly recorded the assault.[106] There was a question of whether the recording device used to record the assault transferred the video onto the defendant's phone.[107] Officers obtained a warrant to seize the phone, however the phone was locked by fingerprint and a passcode preventing them access to see the phone's contents.[108] The court concluded that the production of one's fingerprint was non-testimonial because it would not "require the witness to divulge anything through his mental processes."[109] Therefore, a fingerprint is not protected by the defendant's Fifth Amendment privilege against self-incrimination like the compulsion of an alphanumeric passcode would be.[110]

In arriving at its conclusion, the court looked to prior Supreme Court precedent, including *Kirschner*, holding that the ". . . defendant cannot be compelled to 'divulge through his mental processes' the passcode for entry. The fingerprint like a key, however, does not require Defendant to 'communicate any knowledge' at all."[111] In sum, requiring the defendant to produce the passcode would force him to disclose "the contents of his own mind" whereas the fingerprint was just "physical characteristic" evidence requiring no disclosure of knowledge.[112]

Similarly, in *State v. Diamond,*[113] the Court of Appeals of Minnesota held that the defendant's Fifth Amendment rights were not violated when he was required to provide his fingerprint so the police could search his phone.[114] In *Diamond*, there was a reported burglary at the house of

101. Commonwealth v. Baust, 89 Va. Cir. 267, 271 (2014); State v. Diamond, 890 N.W.2d 143, 151 (Minn. Ct. App. 2017).
102. *Baust,* 89 Va. Cir. at 271; *Diamond,* 890 N.W.2d at 151.
103. *Baust*, 89 Va. Cir. at 271.
104. *Id.*
105. *Id.* at 267
106. *Id.* at 268.
107. *Id.*
108. *Id.*
109. *Id.* at 270.
110. *Id.* at 271.
111. *Id.*
112. *Id.*
113. State v. Diamond, 890 N.W.2d 143 (Minn. Ct. App. 2017).
114. *Id.* at 151.

M.H.[115] Upon arriving at and assessing the home, police found footprints around the outside of the garage.[116] The following day, the defendant was arrested on an outstanding warrant unrelated to the burglary, and pursuant to the arrest, police collected his property, which included his shoes and phone.[117] The police officers, upon completing an inventory of the items collected when the defendant was arrested, noticed that the footprints found outside M.H.'s home were similar to the tread of the defendant's shoes.[118] After obtaining a warrant to search the defendant's property more thoroughly, the officers found that they could not unlock his phone because it was protected by a fingerprint passcode.[119]

The Minnesota Court of Appeals found that the trial court's ordering of Diamond to produce his fingerprint to unlock the phone was not a violation of his Fifth Amendment rights because he was "not required to disclose any knowledge he might have or to speak his guilt."[120] In its analysis, the court emphasized distinctions between *Kirschner* and *Diamond*.[121] In particular, it rested its reasoning on the notion that Diamond was not required to use any form of knowledge or mental capacity in placing his fingerprint on the phone, as opposed to compelling someone to hand over a passcode of which only he or she has knowledge.[122] Moreover, the court concluded that compelling Diamond to provide his fingerprint, "is no more testimonial than furnishing a blood sample, providing handwriting or voice exemplars, standing in a lineup, or wearing particular clothing."[123] Here, the court directly analogized the concept of a fingerprint to the original line of Supreme Court cases which delineated specific categories of acts of production which were found to be explicitly non-testimonial.[124]

Unlike *Baust* and *Diamond*, the District Court for the Northern District of Illinois in *In re Single-Family Home & Attached Garage* held that the Fifth Amendment "prohibits the forced unlocking of a device by

115. *Id.* at 145.
116. *Id.*
117. *Id.* at 146.
118. *Id.*
119. *Id.*
120. *Id.* at 150; *see also* Doe v. United States, 487 U.S. 201, 211 (1988).
121. *Diamond*, 890 N.W.2d. at 151.
122. *Id.*
123. *Id.*; *see also Doe*, 487 U.S. at 210.
124. *See, e.g.*, United States v. Dionisio, 410 U.S. 1 (1973) (finding that the production of a voice exemplar was non-testimonial in nature); Schmerber v. California, 384 U.S. 757, 764 (1966) (finding that the compulsion of a blood sample was non-testimonial in nature); Gilbert v. California, 388 U.S. 263 (1967) (finding that the compulsion of a hand-writing exemplar was non-testimonial in nature).

finger touch."[125] In this case, the FBI suspected that an individual on a specific, identified premises had been using Apple technology to access and store child pornography.[126] Additionally, the FBI concluded that the child pornography was being accessed from an iPhone 5, as well as an iPad 2.[127] There were four identified individuals living at the recognized premises, but the individual or individuals accessing the child pornography were unidentified.[128] The government sought authority to "force their fingers or thumbs to any Apple devices" that were found on the premises to determine who was using the devices.[129]

The court found that compelling an individual to unlock a phone using his fingerprint would "implicitly communicate potentially incriminating information . . ." and is therefore a violation of their Fifth Amendment rights.[130] It reasoned that if an individual succeeds at unlocking a device, "there is no divorcing the compelled act of production from the resulting implicit testimony that he possesses and controls the device and any contraband or evidence stored on it."[131] Further, the court emphasized the fact that the device is automatically unlocked when the correct fingerprint touches the sensor, so the connection is "direct and powerful"[132] and warrants distinction from prior Fifth Amendment precedent which mechanically differentiated between "physical" and "testimonial" acts.[133] Further, the court recognized how potent and dangerous such a forced compulsion could be for the person who successfully unlocked the device.[134] Not only would the device be unlocked and at the government's disposal, but the person who unlocked it would be inextricably tied to the incriminating contents inside the device without recourse.[135] The court found that compelling the defendant's fingerprint password is testimonial in nature because it

125. *In re* Single-Family Home & Attached Garage, No. 17 M 85, 2017, U.S. Dist. LEXIS 170184, at *25 (N.D. Ill. Feb. 21, 2017), *rev'd in part*, *In re* Search Warrant Application for [Redacted Text], 279 F. Supp. 3d. 800 (N.D. Ill. 2017). Note that although the district court reversed the magistrate's opinion in *In Re* Single Family Home & Attached Garage, the case is being used in this Note for the magistrate's analysis on the issue of TouchID only. Should a higher court reverse the district court, the cited analysis of the magistrate will likely be proper.

126. *Id.* at *5.

127. *Id.*

128. *Id.* at *6.

129. *Id.*

130. *Id.* at *23.

131. *Id.*at *19.

132. *Id.*

133. *Id.* at *21–23.

134. *Id.*

135. *Id.*

implicitly communicates "that the device and its contents are in his 'possession and control,'" entitling it to the protection under the Fifth Amendment.[136] Because of the nature of this new technology, the fingerprint held with it a communicative nature of ownership of the device and the information held on the device, which the court found was deserving of constitutional protection.[137]

B. Baust and Diamond Misapplied The Fifth Amendment Privilege Against Self-Incrimination

Although the Virginia Court in *Baust* and the Minnesota Court of Appeals in *Diamond* correctly applied the prior Supreme Court case law pertaining to what constitutes a testimonial act of production, they applied the Supreme Court case law blindly to the issue of TouchID. Both of these decisions depict the result when a court chooses the formalism of a legal rule over the substance and purpose of why the rule was created to begin with. It appears that both courts were turning a blind eye by refusing to acknowledge the distinction between what kind of protection a fingerprint deserves in the identification sense of the law, (i.e. the traditional function of the fingerprint) from its function as a password on a phone in the modern context.

In *Baust,* the court looked to *Kirschner* and *Fisher* in attempting to determine whether it was proper under the Fifth Amendment to compel the defendant's fingerprint to unlock his phone.[138] In reaching its decision, the court relied on a hollow and formalistic distinction between the type of alphanumeric password seen in *Kirschner,* which was found to be protected from compulsion under the Fifth Amendment, and the fingerprint password used by Baust.[139] Instead of paying attention to the purpose of the fingerprint, which was to serve as a high-security password, the court erroneously looked at the physical act that the defendant was required to do to unlock the device.[140] Because the fingerprint was merely physical evidence obtained from the body, analogous to a handwriting sample or a voice exemplar, it held there was no constitutional protection against forced compulsion.[141]

---

136. *Id.* at *18 (citing Fisher v. United States, 425 U.S. 391, 410 (1976)).

137. *Id.*

138. *Fisher*, 425 U.S. 391; Commonwealth v. Baust, 89 Va. Cir. 267, 271 (Va. Cir. Ct. 2014).

139. *Baust*, 89 Va. Cir. at 271 (stating "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.").

140. *Id.*

141. *Id.*

Because the fingerprint password did not require the defendant to use his own knowledge or mind, the fingerprint was deemed non-testimonial, physical evidence and was therefore excluded from Fifth Amendment protection.[142] Simply stated, all this court accomplished in its holding was successfully putting form over substance. The court expressly ignored the fact that the compulsion of a fingerprint password revealed far more, both explicitly and implicitly about the person unlocking the device and their presumed ownership of the contraband held on the device, than merely providing a fingerprint to the government.[143] When a defendant is forced to provide their fingerprint to unlock a device, that defendant becomes exposed as the owner and possessor of a slew of evidence on that device, that can and likely will be used against him or her in a criminal proceeding.[144] This is exactly what the right against self-incrimination is designed to protect against—to protect defendants from being forced to testify against themselves.[145] The *Baust* court blissfully ignores this critical fact.

Similar to *Baust,* the court in *Diamond* engaged in the same erroneous legal formalism and reasoning. The *Diamond* court arrived at its conclusion, to require the compulsion of the defendant's fingerprint password, stating, "Diamond was not required to disclose any knowledge he might have or to speak his guilt."[146] The court, very similarly to the court in *Baust,* stressed the flawed distinction between producing an alphanumeric password, versus compelling one's fingerprint to unlock a device, despite serving the exact same function.[147] By ordering Diamond to place his fingerprint on his phone to unlock it, the action communicated very clearly and directly to the government that Diamond was the owner or possessor of the phone and the incriminating contents held inside. From any common-sense standard, this is a testimonial act of production, regardless of the level of knowledge required to do the act.

The *Baust* and *Diamond* courts both seem to ignore the fact that the alphanumeric and fingerprint passwords serve the same function. Both cases rely on Supreme Court precedent from a non-digital era to compel defendants to unlock their secured devices using their fingerprints. Both cases analogize the fingerprint to other forms of physical evidence in a context that is distinguishable in meaning and purpose. When cases such

142. *Id.*

143. *Id.*

144. *See In re* Single-Family Home & Attached Garage, No. 17 M 85, 2017 U.S. Dist. LEXIS 170184, at *18 (N.D. Ill. Feb. 21, 2017), *rev'd in part, In re* Search Warrant Application for [Redacted Text], 279 F. Supp. 3d. 800 (N.D. Ill. 2017).

145. U.S. CONST. amend. V.

146. State v. Diamond, 890 N.W.2d 143, 150 (Minn. Ct. App. 2017).

147. *Id.* at 151.

as *Fisher, Doe,* and *Schmerber* were handed down by the Supreme Court, the idea of biometric security using fingerprints was nonexistent and certainly not something the Supreme Court likely ever imagined. However, Justice Stevens' dissent in *Doe* expressed a forward-looking approach for handling a potential change in technology.[148] Now that the potential change in technology has come to fruition, courts are well advised to find the Stevens' dissent in *Doe* instructive.

This line of cases viewed fingerprints and their capacity for identification in a completely different light than what is required of courts today.[149] Today, courts must be willing to recognize a fingerprint's capacity as a high security password that deserves constitutional protection. It does not make common or legal sense for courts in today's digital era to rely on principles enunciated in outdated cases and draw false analogical lines, as the *Baust* and *Diamond* courts did. There must be a legal and doctrinal change in Fifth Amendment jurisprudence to account for this critical disconnect between the fingerprint's previous purpose and its newfound power to self-incriminate defendants at one touch.

C. In Re Single-Family Home & Attached Garage Correctly Applied The Fifth Amendment Privilege Against Self-Incrimination

Notwithstanding the failure of the *Baust* and *Diamond* courts to identify the true similarities between an alphanumeric password and a fingerprint password, the court in *In re Single-Family Home & Attached Garage* saw beyond the empty legal formalism that was enunciated in the previously discussed fingerprint password cases to find that compelling the fingerprint password would violate the defendants' right against self-incrimination.[150]

In arriving at its determination that the fingerprint passcode could not be compelled, the court identified the pertinent question in determining whether a compelled act truly is "testimonial" under the Supreme Court's precedent.[151] The court announced that one must ask, "whether, under the specific facts and circumstances presented, the act implicitly conveys incriminating information unknown to the government."[152] The court correctly reasoned that when a device is

148. Doe v. United States, 487 U.S. 201, 219 (1988).

149. *See* Goldman, *supra* note 14, at 215.

150. *In re* Single-Family Home & Attached Garage, No. 17 M 85, 2017 U.S. Dist. LEXIS 170184, at *23–24 (N.D. Ill. Feb. 21, 2017), *rev'd in part*, *In re* Search Warrant Application for [Redacted Text], 279 F. Supp. 3d. 800 (N.D. Ill. 2017).

151. *Id.* at *23.

152. *Id.*

unlocked via fingerprint, thereby allowing government access to the contents on the device, it implicitly communicates to the government that the individual who unlocked it has control of the device or has enough meaningful control to have set up the fingerprint password.[153] With such an action, that individual is "being compelled to implicitly testify that he possesses and controls the device and the contraband stored on it" which in many situations establishes criminality of some degree.[154] In sum, the simple act of unlocking the device with a fingerprint communicates very clearly and candidly to the government that the individual is in control of the device and that any information stored on it, can be attributed to that individual. Although this may be considered an implicit testimonial communication, it is nonetheless testimonial and deserving of Fifth Amendment protection, as this court correctly held.[155]

This court correctly recognized that categorizing the fingerprint password as physical evidence versus testimonial evidence is superficial and hollow legal reasoning.[156] Unlike in *Baust* and *Diamond,* the court acknowledged the difference between the use of the fingerprint for identification purposes and as a passcode in the digital era.[157] The notable and meaningful distinction is that "[t]here will be no need for a third party's analysis to convert the act of production into incriminating evidence, as when a fingerprint compelled from a suspect for identification purposes is sent to a lab to compare with prints from a crime scene."[158] The incriminating communication associated with the compelled fingerprint passcode will be "both direct and immediate" if the device contains contraband and is successfully unlocked, compared to the traditional use and concept of fingerprints in the law.[159]

TouchID technology has categorically expanded the meaning and power of the fingerprint into a type of password that protects users' private information in a unique and convenient way.[160] However, the true value of such a secure method of locking devices is undermined when courts refuse to interpret the law without regard to the new purpose of the fingerprint.[161] *In re Single-Family Home & Attached Garage* properly

153. *Id.*
154. *Id.* at *25.
155. *Id.*
156. *Id.* at *21.
157. *Id.* at *23.
158. *Id.*
159. *Id.*
160. *See* Ritchie, *supra* note 1.
161. *See, e.g., Single-Family Home*, 2017 U.S. Dist. LEXIS 170184; Commonwealth v. Baust, 89 Va. Cir. 267 (2014); State v. Diamond, 890 N.W.2d 143 (Minn. Ct. App. 2017).

recognized that, although the method of unlocking the phone was different than an alphanumeric password, the "implicit testimony resulting from the unlocking of the device is unchanged."[162] In sum, applying outdated and superficial formalism to this area of the law not only creates problematic outcomes that will have to be addressed in the future, but it expressly deprives defendants of their right against self-incrimination that they are entitled to during a criminal proceeding.

D. FaceID Cases Should Be Treated Under the Same Analysis

Moving beyond the fingerprint password, with the advent of FaceID or facial recognition technology as a password on devices, the same analysis proposed in Section C must also apply. FaceID technology is a brand-new concept in the legal field and, because of that, the case law has not been developed. This Note presumes that many courts will take the same incorrect position on FaceID technology as many courts[163] did on TouchID regarding its implications with the Fifth Amendment. There is no doubt that there will be cases in the near future that involve the interaction of FaceID technology and the Fifth Amendment. Facial recognition technology deserves equal Fifth Amendment protection as an alphanumeric password because they serve the same purpose and perform function.

With the simple, volitional movement required to unlock a device using FaceID technology, all that is required is that the defendant glance at their device to unlock it.[164] Similar to TouchID, knowledge is not expended to open a device using FaceID. This is the precise reason why courts have refused to allow Fifth Amendment protection for fingerprints or TouchID in the past.[165]

There is an argument that one's facial features, like fingerprints, are physical evidence obtained from the body which in turn means that the evidence is nontestimonial and unentitled to Fifth Amendment protection.[166] On the other hand, when the facial features of a suspect

---

162. *Id.* at *24.

163. *Id.*

164. *See* deAgonia, *supra* note 10.

165. *See* Schmerber v. California, 384 U.S. 757, 764 (1966) ("Both federal and state courts have usually held that it offers no protection against compulsion to submit to fingerprinting, photographing, or measurements, to write or speak for identification, to appear in court, to stand, to assume a stance, to walk, or to make a particular gesture.") (citing 8 Colin McNaughton, Wigmore: Evidence in Trials at Common Law § 2252 (4th ed. 1961)).

166. *See id.* at 764 (1966) (finding that the compulsion of a blood sample was non-testimonial in nature); *see* United States v. Dionisio, 410 U.S. 1 (1973) (finding that the production of a voice exemplar was non-testimonial in nature); *see* United States v.

function as a lock on a device, there is a strong argument that it does possess testimonial qualities and characteristics just like how fingerprint passwords function.

The use of facial recognition technology presents another type of situation that makes the application of the controlling Fifth Amendment jurisprudence troublesome. The testimonial qualities involved with FaceID technology are identical to that of TouchID technology—both provide the government a direct and immediate link between the suspect and the contents held on the device. That link is not only communicative in nature because it binds the suspect to the device with a touch or a glance, but also because any incriminating information about the defendant or relating to the actions of the defendant on the device is inextricably connected to the defendant from that point forward. As the court stated in *In re Single Family Home & Attached Garage*, ". . . an individual—with a touch of a finger—is now able to produce the entire (often vast) contents of a computer device such as a smartphone."[167] The same reasoning should hold true for FaceID technology.

Forcing a suspect to unlock their device using facial recognition software has the strong potential to force the defendant to self-incriminate—a risk that courts must account for when adjudicating such cases in the future. This connection would implicitly force the defendant linked to the device to testify that they are in control and possession of the contraband held on the device. In the end, the defendant is forced to testify against themselves, clearly violating their privilege against self-incrimination.

Looking to the future, a court adjudicating this type of case must recognize and reevaluate its interpretation and application of Supreme Court precedent to accommodate for such changes in technology. Despite the fact that it was drafted centuries before the concept of biometric passwords was even envisioned, the Fifth Amendment, and its underlying policy and purpose, has remained unchanged. The Fifth Amendment and the privilege against self-incrimination, as it is understood today and when it was drafted, supports the treatment of fingerprint passwords and facial recognition passwords as what they truly are–passwords.[168] Passwords, regardless of their form, are considered testimonial evidence which is entitled to constitutional

---

Wade, 388 U.S. 218 (1967) (finding that standing up in a police lineup was non-testimonial); *see* Gilbert v. California, 388 U.S. 263 (1967) (finding that the compulsion of a hand-writing exemplar was non-testimonial in nature).

167. *Single-Family Home*, No. 17 M 85 at *23.

168. *See* Goldman, *supra* note 14, at 225. Although Goldman only refers to fingerprint passwords in her article, this Note analogizes the same reasoning as directly applicable to facial recognition passwords, as well.

protection.[169] It is undisputed that today's devices, whether it is a smartphone, tablet or laptop, can hold a tremendous amount of private, personal information.[170] This type of information must be protected from governmental intrusion when it is protected by a password. A password is a password, regardless of its form. If alphanumeric passwords are protected under the Fifth Amendment from forced compulsion, a password in the form of a fingerprint or by facial recognition is equally deserving of protection by the Fifth Amendment.

IV. CONCLUSION

Biometric passwords have put the traditional classification of testimonial evidence (entitled to Fifth Amendment protection) and physical evidence (not entitled to Fifth Amendment protection) at odds with one another. Biometric passwords do not fall neatly into either category of evidence because they incorporate both physical and testimonial qualities. The pertinent question that this Note addresses is whether the future use of biometric passwords should prevent an individual from properly invoking their Fifth Amendment privilege against self-incrimination simply because it is not a traditional alphanumeric password. This Note proposes that a password is a password, and, if an alphanumeric password is entitled to Fifth Amendment protection, then its current counterparts, TouchID and FaceID passwords, should be entitled to the same protection.[171]

There must be a change in the legal doctrine to accommodate the high risk of compelled self-incrimination through the fingerprint password, which is a violation of the Constitution. As the *Fisher* court wisely articulated, the questions of whether a compulsion is testimonial and incriminating ". . . do not lend themselves to categorical answers; their resolution may instead depend on the facts and circumstances of particular cases or classes thereof."[172] Future courts hearing these issues must realize that a blind, mechanical application of the outdated case law and rules regarding what is considered testimonial and nontestimonial evidence does not adequately address the constitutional implications that biometric passwords bring to light. In the future, when courts are

169. *Id.*

170. *See* Riley v. California, 134 S. Ct. 2473 (2014) (holding that a warrant is required before a search of the contents of a cell phone, even if seized during an arrest).

171. *See* Goldman, *supra* note 14. The rate at which biometric security is advancing is faster than the law. Just three years ago, the biggest concern was TouchID with fingerprints, and now FaceID has brought in a new set of legal dilemmas that need to be answered in accordance with the Fifth Amendment's intended purpose. *Id.*

172. Fisher v. United States, 425 U.S. 391, 410 (1976).

reviewing and analyzing compelled biometric password cases, they must keep one important factor in mind—that biometric passwords serve the same function as alphanumeric passwords—securing a device from intrusion. A password is a password, and despite the fact that one password requires the utilization of knowledge, and the other requires a touch or a glance, both are testimonial in nature and capable of communicating a tremendous amount of incriminating evidence to the government. Moving forward, this proposed analysis will protect individuals from being locked out of their Fifth Amendment rights that they are entitled to.