Face It – The Convenience of a Biometric Password May Mean Forfeiting Your Fifth Amendment Rights

Ariel N. Redfern*

> "*If someone steals your password, you can change it. But if someone steals your thumbprint, you can't get a new thumb.*" – Bruce Schneier

ABSTRACT

The shift toward enhanced data security has led to biometric encryption of personal devices through technology like Apple's FaceID and TouchID. The inalterable nature of biometric passwords allows for enhanced security and increased user convenience. However, law enforcement's targeting of biometric passwords as an investigatory tool has raised novel constitutional questions.

The Fifth Amendment privilege against self-incrimination prohibits the government from compelling incriminating testimony from an individual. As a result, law enforcement cannot coerce someone to speak the words or letters that decrypt, or unlock, his or her personal device. Yet, the majority of courts do not recognize the same constitutional protection for biometric passwords, raising the issue of compelled biometric decryption.

In addition to addressing how legislatures are reacting to technological advancements, this Comment analyzes the inception and evolution of the Fifth Amendment privilege against self-incrimination and highlights the inherent privacy concerns raised by compelled biometric decryption. In doing so, this Comment seeks to reconcile the Fifth Amendment privilege against self-incrimination with the digital age.

This Comment argues that, today, the information on a personal device is an extension of the mind, almost functioning as an external hard drive of the self. As such, biometric passwords should not become a loophole for the government's inability to compel an alphanumeric

* J.D. Candidate, The Pennsylvania State University, Penn State Law, 2021.

password. To protect personal privacy, this Comment ultimately recommends that courts give deference to the public policy concerns implicated when the government forces private citizens to decrypt their personal devices using a unique biometric password.

Table of Contents

I. INTRODUCTION

"123456" received the honor of being one of the least secure passwords of all time.[1] This combination of numbers is easy to guess and even easier to hack.[2] While this simple password may not provide protection from privacy invasions on the internet, it may be amongst the safest passwords should you have a run-in with the law.[3] The irony this bad password embodies is reflected by the current state of Fifth Amendment jurisprudence surrounding the government's ability to

1. *See* Bruce Sussman, *Do Not Use: Top 15 'Worst Passwords'*, SECUREWORLD (Oct. 10, 2019, 7:50 AM), http://bit.ly/2wizXOt.

2. *See id.* Passwords like "12345" are easy for hackers to guess and are considered "hot" passwords that cybercriminals know to exploit. *See id.*

3. *See infra* Section II.C.2.

compel individuals to unlock their personal devices[4] using a biometric password.[5]

The majority of courts interpreting the Fifth Amendment find that it protects an individual's right to refuse to speak the digits or letters that unlock that individual's personal device. However, at this time, no uniform Fifth Amendment protection applies if that same individual refuses to press a finger to a fingerprint scanner, or refuses to gaze into a face scanner, to unlock the personal device.[6] Thus, while "123456" may be an inadequate password for securing a smartphone from cybercriminal invasion, the numbers remain constitutionally protected from government intrusion.[7] Meanwhile, the government's key to your iPhone is written across your face.[8]

Consider for a moment the following scenarios:[9]

Scenario 1:

> *Law enforcement has a valid Fourth Amendment warrant to search X's iPhone. X does not have TouchID*[10] *or FaceID*[11] *enabled, and the only means of entering her phone is with the password "1234." X refuses to input the password, and law enforcement leaves because they cannot compel X to say or type "1234," because doing so would be a violation of her Fifth Amendment privilege against self-incrimination. Therefore, all of X's data remains encrypted.*

4. For the purposes of this Comment, the term "personal device" encompasses smartphones, laptops, and tablets owned by an individual. *See Personal Device*, PC MAG, http://bit.ly/3bFPJDi (last visited Jan. 12, 2020).

5. "Biometric password" refers to a biometric identifier (like a fingerprint or face) that a user can integrate into personal device technology (like a fingerprint scan, iris scan, face scan, etc.) to encrypt that personal device, in addition to a traditional numeric and alphanumeric password. *See* Alison Grace Johansen, *Biometrics and Biometric Data: What Is it and Is it Secure?*, NORTON (Feb. 8, 2019), https://nr.tn/3oDSGdO.

6. *See infra* Section II.C.2.

7. *See infra* Section II.C.2.

8. *See About FaceID Advanced Technology*, APPLE, https://apple.co/2SKE7WL (last visited Jan. 12, 2020) (referring to the Apple, Inc. technology that allows users to decrypt their devices with their unique facial features).

9. Scenarios adapted from Seo v. State, 109 N.E.3d 418, 420 (Ind. Ct. App.), *transfer granted, opinion vacated*, 119 N.E.3d 90 (Ind. 2018). *See also* Paul Wallin, *Can You Be Jailed for Refusing to Unlock Your Phone?*, WK LAW, https://bit.ly/35uPuu0 (last visited Oct. 26, 2020); Jim Nash, *Another Federal Court Says Biometrics Can Be Used to Open Devices if a Warrant Has Been Issued*, BIOMETRICUPDATE.COM (July 6, 2020), https://bit.ly/3iCaRNy.

10. *See Use Touch ID on iPhone and iPad*, APPLE, https://apple.co/31U33iQ (last visited Jan. 12, 2020) (referring to the Apple, Inc. technology that allows users to decrypt their personal devices using the unique grips of their fingerprints).

11. *See About FaceID Advanced Technology*, *supra* note 8.

Scenario 2:

> *Law enforcement has a valid Fourth Amendment warrant to search Y's iPhone. Y encrypts his phone with FaceID technology. When asked to input his password, Y refuses. Law enforcement then places Y's iPhone in front of his face. Y refuses to open his eyes, rendering the face scan impossible. Y is held in contempt of court for failure to comply with the warrant because in Y's jurisdiction the choice not to submit to biometric decryption is currently not protected by the Fifth Amendment privilege against self-incrimination.*

These scenarios demonstrate that only one means to the same end is constitutionally protected—you are protected from having to say "1234" but have no right to keep your eyes closed.[12] In the above scenario, X is in the minority because most individuals have made the shift from using alphanumeric passwords to using biometric passwords.[13] Thus, many in the United States are left powerless to resist government intrusion into their personal devices because they choose to encrypt their devices with a biometric password.[14]

The majority of courts that have addressed the constitutional issue posed by biometric passwords have determined that the Fifth Amendment does not protect individuals against compelled biometric decryption.[15] This outcome raises the question of whether citizens should be forced to trade in their constitutional protections in order to use the latest technologies. This Comment thus explores the privacy implications raised when courts fail to recognize the same constitutional protections for users of biometric passwords that are afforded to users of alphanumeric passwords.[16]

Part II of this Comment provides an overview of what biometric encryption is and how it works in personal devices.[17] Part II then describes the source of the Fifth Amendment privilege against self-incrimination and how courts apply it today.[18] Part II goes on to discuss the impact that advancing technology has on how the law is interpreted

12. *See* Wallin, *supra* note 9.

13. *See* Diego Poza, *3 Critical Trends in Biometric Authentication in 2019*, AUTH0 (Mar. 21, 2019), http://bit.ly/31YUtiS.

14. *See id.*; *see also infra* Part III.

15. "Compelled biometric decryption" refers to a government's demand that an individual unlock his or her personal device with a biometric password. *See* Aloni Cohen & Sunoo Park, *Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries*, 32 HARV. J.L. & TECH. 170, 173 (2018); *infra* Section II.C.2.

16. *See infra* Part III. In this Comment, "alphanumeric passwords" refer to passwords that contain letters or numbers, rather than a biometric identifier, as a means of decryption. *See* Margaret Rouse, *Alphanumeric (Alphameric)*, TECHTARGET, http://bit.ly/3bROnp8 (last visited Nov. 6, 2020).

17. *See infra* Section II.A.

18. *See infra* Section II.B.

and also discusses how state and federal courts are adjudicating the issue of compelled biometric decryption.[19] In addition, Part II briefly summarizes how federal and state legislatures are addressing advancing biometric technology.[20]

Part III of this Comment examines the majority of courts' analysis of compelled biometric decryption and concludes that the majority analysis fails to account for the uniqueness of modern personal devices.[21] In Part III, this Comment ultimately proposes that, in order to protect the privacy interests that are the foundation of the Fifth Amendment privilege against self-incrimination, courts should analyze the issue of compelled biometric decryption through a public policy lens.[22] Finally, Part IV of this Comment offers concluding statements on the issues raised.[23]

II. BACKGROUND

Understanding the evolution of the Fifth Amendment privilege against self-incrimination is essential to apply the privilege to biometric decryption today.[24] Moreover, the relationship between biometrics and the Fifth Amendment may be misunderstood if one fails to consider how biometrics have been integrated into everyday life.[25] To ignore the fact that technology is constantly evolving is perilous and, thus, this Section also addresses the concept that law should evolve with technology.[26] This Section also explores the means by which state legislatures are reacting to the prevalence of biometrics.[27] Before diving into the legal and social implications of compelled biometric decryption, it is beneficial to have an overview of what biometrics are and how biometric encryption works.

19. *See* discussion *infra* Section II.C.
20. *See infra* Section II.D.
21. *See infra* Part III.
22. *See infra* Section III.D.
23. *See infra* Part IV.
24. *See* Terrance Sandalow, *Federalism and Social Change*, 43 L. & CONTEMP. PROBS. 30, 33–34 (1980).
25. *See infra* Section II.C.
26. *See infra* Section II.B.2.
27. "[States] contribute to the resolution of important social issues . . . . [T]hey continue to have important decision-making responsibilities . . . [and] must act within the framework of norms that the large society regards as fundamental, norms that are to be given legal expression by institutions of the national government." Sandalow, *supra* note 24, at 33–34.

A. What Are Biometrics and How Does Biometric Encryption of a Personal Device Work?

Biometrics are inherently intertwined with personal privacy;[28] they are used to access bank accounts, enter residences, unlock personal devices, and so forth.[29] Understanding what biometrics are and how they are ingrained into personal devices underscores the types of privacy concerns that accompany biometric password protection.[30] Such concerns reinforce the need for Fifth Amendment protection from compelled biometric decryption.[31]

Biometrics encompass a breadth of technology that uses "unique identifiable attributes of people . . . for identification and authentication."[32] This includes "a person's fingerprint, iris print, hand, face, voice, gait or signature."[33] Evolving from cryptography, encryption functions to keep secret messages unreadable until accessed with the correct corresponding key.[34] When unlocking a personal device, the primary purpose is authentication.[35] Therefore, proper encryption functions as a lock that only the person with the authorized key is able to decipher.[36]

Authentication of a person or a computer can occur through methods like password protection, "pass cards,"[37] digital signatures, and

---

28. *See generally* Jan Grijpink, *Privacy Law: Biometrics and Privacy*, 17 COMPUTER L. & SEC. REV. 154 (2001) (discussing biometric identification and its effects on privacy).

29. *See* Alison Arthur & Bethany Frank, *Five Examples of Biometrics in Banking*, ALACRITI (May 8, 2019), http://bit.ly/320ZrMc; Danny Thakkar, *Efficient Building Access Control, Facilities and Services with Biometrics*, BAYOMETRIC, http://bit.ly/2wltFxH (last visited Feb. 13, 2020) (discussing how apartment buildings and other residential dwellings are incorporating fingerprint and other form of biometric authentication in lieu of standard keys); *About FaceID Advanced Technology*, *supra* note 8.

30. *See* N.K. Ratha et al., *Enhancing Security and Privacy in Biometrics-Based Authentication Systems*, 40 IBM SYSTEMS J. 614, 614 (2001).

31. *See infra* Part III.

32. BIOMETRICS INSTITUTE, http://bit.ly/2Jkeono (last visited Oct. 16, 2019).

33. *Id.*

34. *See* Jeff Tyson, *How Encryption Works*, HOW STUFF WORKS (Apr. 6, 2001), http://bit.ly/3bDjRz5. Cryptographic use dates back to the Greeks when Spartan generals used cryptic messages to communicate sensitive military information. *See id.* The essence of cryptography was to encode the desired message using a combination of certain letters and numbers so that the message appeared as nonsense to an individual who lacked the matching decipher. *See id.*

35. *See id.*; *see also* Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 GEO. L.J. 989, 993–96 (2018).

36. *See Tyson*, *supra* note 34; *see also* Kerr & Schneier, *supra* note 35, at 993.

37. "Pass cards" include security cards that can range in complexity. *See* Tyson, *supra* note 34. Credit cards, cards with magnetic strips, and computer chips are all forms of secure pass cards. *See id.*

biometrics.[38] Biometric authentication not only serves as a key to unlock a device but also as a means to identify an individual.[39] Since biometric authentication is almost synonymous with individual identification, biometric passwords serve as a more secure method than traditional passwords for protecting data.[40] Biometric passwords, unlike alphanumeric passwords, are "immutable."[41] Individuals cannot change the grooves of their fingerprints or the biological structures of their irises.[42] These characteristics of biometric passwords contribute to why technology innovators are shifting toward equipping new devices with biometric authentication, in addition to alphanumeric passwords.[43] Rather than having to remember or type a lengthy password, biometric passwords offer the convenience and speed of short passwords while providing enhanced security.[44] Accordingly, technology experts widely agree that biometric passwords are superior to their alphanumeric counterparts.[45] Nevertheless, the majority of courts that have examined compelled biometric decryption have failed to extend constitutional protections to biometric passwords.[46]

The science behind encryption is only one component of the compelled biometric decryption issue.[47] Examining the privacy rationales and ideas that created the privilege against self-incrimination can help explain how compelled biometric decryption finds its place in modern jurisprudence.[48]

38. *See id.*

39. *See id.*

40. Maria Korolov, *What is Biometrics? 10 Physical and Behavioral Identifiers That Can Be Used for Authentication*, CSO (Feb. 12, 2019, 3:00 AM), http://bit.ly/37uzIwB.

41. *Id.* Since biometric passwords are unchangeable, they pose heightened security concerns if they are compromised. *See id.*

42. *See id.*

43. *See id.* (identifying popular methods of biometric authentication, including fingerprint, retina, and face scans, along with voice identification); *see also* Ratha et al., *supra* note 30, at 614.

44. *See* Ratha et al., *supra* note 30, at 615.

45. *See* Louis Columbus, *Why Your Biometrics Are Your Best Password*, FORBES (Mar. 8, 2020, 12:38PM), https://bit.ly/34yDBT0 (describing the best protection as a Two-Factor Authentication system incorporating biometric passwords).

46. *See infra* Section II.C.2; *see also* Chad Hammond, *Biometric Security Is Convenient, but Is It Safe?*, NORDPASS (Sep. 5, 2020), https://bit.ly/2F4MauX.

47. *See infra* Section II.C.2.

48. *See infra* Section II.B.

B. What Is the Privilege Against Self-Incrimination and Where Did It Come From?

The Framers of the Constitution deliberately incorporated the privilege against self-incrimination into the Bill of Rights.[49] The privilege against self-incrimination began as a commonly held belief that no individual should be forced to divulge information that incriminated himself or herself.[50] That same belief that influenced the development of the privilege against self-incrimination must be considered when applying it to modern issues.[51]

1. From Common Law to the Constitution

The Fifth Amendment provides that "[n]o person . . . shall be compelled in a criminal case to be a witness against himself."[52] This privilege against self-incrimination can be linked back to the common law privilege fueled by the "the maxim '*nemo tenetur seipsum accusare*,'" loosely translated to "no man is bound to accuse himself."[53] Although scholars agree that the privilege against self-incrimination far predates the United States Constitution,[54] viewpoints conflict as to the exact historical course that produced the privilege[55]—the depths of which are far beyond the scope of this Comment.

For purposes of this Comment, the roots of the privilege against self-incrimination can be traced back to the *oath ex officio* in the ecclesiastical courts of thirteenth-century England.[56] The oath functioned as a "sworn statement to give true answers to whatever questions might be asked."[57] In 1557, under Queen Mary, the Court of High

49. *See* U.S. CONST. amend. V; *see also* LEONARD W. LEVY, ORIGINS OF THE FIFTH AMENDMENT 31 (1968). *See generally* William J. Brennan Jr., *Why Have a Bill of Rights?*, 9 OXFORD J. LEGAL STUD. 426 (1989) (discussing the purpose of the Bill of Rights).

50. *See* LEVY, *supra* note 49, at 31.

51. When applying the constitution to novel legal issues, its language cannot "safely" be interpreted without "reference to the common law and to British institutions as they were when the instrument was framed and adopted." *Ex parte* Grossman, 267 U.S. 87, 109 (1925).

52. U.S. CONST. amend. V.

53. *See* John H. Langbein, *The Historical Origins of the Privilege Against Self-Incrimination at Common Law*, 92 MICH. L. REV. 1047, 1072 (1994); *see also Self Incrimination*, JUSTIA, http://bit.ly/2SKULpl (last visited Oct. 17, 2019).

54. *See generally* LEVY, *supra* note 49 (discussing the historical roots of the Fifth Amendment "right" of self-incrimination).

55. John Fabian Witt, *Making the Fifth: The Constitutionalization of American Self-Incrimination Doctrine, 1791–1903*, 77 TEX. L. REV. 825, 831 (1999).

56. *See* LEVY, *supra* note 49, at 46.

57. *Id.* at 47. Levy argues this oath was objectionable, considering the accused was subject to it without first being formally charged. *See id.*; *see also In re* Search Warrant Application for the Cellular Telephone in United States v. Anthony Barrera, No. 19 CR

Commission[58] was tasked with using the *oath ex officio* to procure confessions for crimes against the Church.[59] Failure to comply carried penalties of fines, imprisonment, or execution.[60] Persistent opposition to the *oath ex officio* led to the understanding that individuals should not be compelled to accuse themselves under oath.[61]

In 1645, an English court first recognized the privilege against self-incrimination in the case of John Lilburne.[62] Lilburne was accused of seditious libel for publishing damaging statements in pamphlets under a pseudonym.[63] Lilburne, who refused to take the *pro confesso* oath, which had evolved out of the *oath ex officio*, argued that he could not be compelled to incriminate himself.[64] Lilburne acted as a catalyst for the idea that, as a matter of personal liberty and freedom, individuals should be free from self-incrimination by moral or physical compulsion.[65]

In 1776, after the United States claimed independence from Britain, individual states acted to secure their rights by creating state Constitutions.[66] Virginia, spearheading the commitment to freedom from self-incrimination, included in its Constitution "that a man 'cannot be compelled to give evidence against himself.'"[67] This provision, drafted

439, 2019 WL 6253812, at *2 (N.D. Ill. Nov. 22, 2019) (explaining that the Star Chamber courts would require an individual to succumb to this oath to elicit evidence of crimes that the individual had not yet been charged with).

58. The Court of High Commission was one of the ecclesiastical courts of England, which was established in the sixteenth century to maintain control over the Church of England. *See Court of High Commission*, ENCYCLOPEDIA BRITANNICA, http://bit.ly/2StDguK (last visited Jan. 12, 2020). The court became a tool used to repress those who did not succumb to the power of the Church. *See id.*

59. *See* LEVY, *supra* note 49, at 76–77.

60. *See id.*

61. *See Self Incrimination*, *supra* note 53.

62. *See* LEVY, *supra* note 49, at 266–300.

63. *See id.* at 288.

64. *See* Harold W. Wolfram, *John Lilburne: Democracy's Pillar of Fire*, 3 SYRACUSE L. REV. 213, 220, 241 (1952).

65. *See* Ullman v. United States, 350 U.S. 422, 448 (1956); *id.* at 446. (Douglas, J., dissenting); *see also* Miranda v. Arizona, 384 U.S. 436, 458–60 (1966).

66. *See* LEVY, *supra* note 49, at 405.

67. *Id.* In full, the provision read:

> That in all capital or criminal prosecutions a man hath a right to demand the cause and nature of his accusations, to be confronted with the accusers and witnesses, to call for evidence in his favor, and to a speedy trial by an impartial jury of twelve men of his vicinage, without whose unanimous consent he cannot be found guilty; *nor can he be compelled to give evidence against himself*; that no man be deprived of his liberty, except by the law of the land or the judgement of his peers.

Id.

by George Mason,[68] became the model for other states and would ultimately be adopted into the Bill of Rights.[69]

2. Evolution of the Privilege Against Self-Incrimination

Since its ratification, the Fifth Amendment continues to evolve in ways the Framers could not have dreamt.[70] The Supreme Court first interpreted the issue of privacy as it relates to the privilege against self-incrimination in the 1886 case of *Boyd v. United States*.[71]

In *Boyd*, the Court held that requiring a man to give over his private books and papers violated the Fifth Amendment because the act amounted to the government forcing him to be a witness against himself.[72] The Court explained that government invasion into the "sanctity of a man's home and the privacies of life," as well as the invasion of a citizen's personal privacy, fueled the need for protection under the privilege against self-incrimination.[73]

Following *Boyd*, the Supreme Court, in *Counselman v. Hitchcock*,[74] extended the privilege against self-incrimination to witnesses in criminal proceedings.[75] In reaching this decision, the Court observed that "[i]t is the duty of courts to be watchful for the constitutional rights of the citizen, and against stealthy encroachments thereon."[76] Later, the Supreme Court in *Blau v. United States*[77] reaffirmed the notion that the privilege against self-incrimination protects against compelled testimony.[78]

Throughout the twentieth century, as society continued to develop, so did the privilege against self-incrimination.[79] New rationales and expansive ideas continued to enhance the privilege.[80] In *Ullman v.*

68. *See id.* at 407–10; *see also George Mason*, BIOGRAPHY (Sept. 24, 2020), http://bit.ly/2uLgPIt.

69. *See* LEVY, supra note 49, at 414–16.

70. *See infra* Section II.C.

71. Boyd v. United States, 116 U.S. 616, 634–35 (1886).

72. *See id.*

73. *See id.* at 630.

74. Counselman v. Hitchcock, 142 U.S. 547, 586 (1892).

75. *See id.* At the time this case was decided, the Fifth Amendment had not yet been incorporated to the states, making the Court's decision an exemplary lead. *See* Witt, *supra* note 55, at 906 n.358.

76. *Counselman*, 142 U.S. at 582.

77. Blau v. United States, 340 U.S. 159, 161 (1950).

78. *See id.* The Court reasoned that the privilege protected testimony that was considered a "link in the chain of evidence," which the prosecution could not use to support a conviction. *See id.* ("Under such circumstances, the Constitution gives a witness the privilege of remaining silent."); *see also* Hoffman v. United States, 341 U.S. 479, 485–86 (1951).

79. *See* Witt, *supra* note 55, at 910.

80. *See id.* at 831.

United States,[81] the Supreme Court again embraced the privilege against self-incrimination, explaining that the privilege:

> serves as a protection to the innocent as well as to the guilty, and we have been admonished that it should be given a liberal interpretation. If it be thought that the privilege is outmoded in the conditions of this modern age, then the thing to do is to take it out of the Constitution, not to whittle it down by the subtle encroachments of judicial opinion.[82]

The Supreme Court acknowledged that a liberal interpretation of the privilege may hinder government efforts—or even spare a guilty man his "just deserts"—but that the privilege serves a greater, more noble purpose of shielding citizens from "future abuses by law-enforcing agencies."[83]

With each successive interpretation of the Fifth Amendment privilege against self-incrimination, the underlying personal privacy rationale remained strong. As stated in the landmark case, *Miranda v. Arizona*,[84] "the constitutional foundation underlying the privilege is the respect a government—state or federal—must accord to the dignity and integrity of its citizens."[85]

Notably, the Supreme Court's 1976 interpretation of the privilege against self-incrimination in *Fisher v. United States*[86] created the framework that courts employ in interpreting the privilege today.[87] In *Fisher*, the Court determined that a case must satisfy three requirements to implicate the privilege against self-incrimination.[88] An individual must be (1) compelled by the government, (2) to make a testimonial[89] communication, (3) that is incriminating.[90] The issue addressed in *Fisher* arose out of Internal Revenue Service (IRS) summons that required two attorneys to produce documents related to federal income tax accusations

81. Ullmann v. United States, 350 U.S. 422, 427 (1956) (citing *Hoffman*, 341 U.S. at 486).

82. *Id.* at 427–28 (citing Maffie v. United States, 209 F.2d 225, 227 (1st Cir. 1954)).

83. *Id.* at 428 (referencing the "evil" that were the brutal confessions under the Inquisition and Star Chamber courts).

84. Miranda v. Arizona, 384 U.S. 436, 439 (1966).

85. *Id.* at 460.

86. Fisher v. United States, 425 U.S. 391, 408 (1976).

87. *See id.*

88. *See id.*

89. The term "testimonial" in this Comment is used in accordance with Fifth Amendment jurisprudence only. It does not include the interpretation of the term under any other Amendment (e.g., Sixth Amendment interpretation of the term "testimonial" as it relates to the confrontation clause).

90. *See Fisher*, 425 U.S. at 408.

against their clients.[91] On appeal, both attorneys asserted the privilege against self-incrimination.[92]

The Court in *Fisher* reasoned that, as with any other amendment, the Fifth Amendment is not absolute, meaning that not all invasions of privacy are protected by the privilege against self-incrimination.[93] The Court distinguished privacy in the Fourth and Fifth Amendment contexts to explain that the Fifth Amendment focuses on compulsion of testimony rather than invasion of privacy.[94] Yet, the Court affirmed that the Fifth Amendment shields a person asserting the privilege from "physical or moral compulsion."[95] In doing so, the Court preserved personal privacy protections as a central purpose of the privilege against self-incrimination.[96] However, the Court in *Fisher* came to the ultimate conclusion that "the Fifth Amendment protects against 'compelled self-incrimination, not (the disclosure of) private information.'"[97]

With the Court's interpretation of the privilege against self-incrimination in *Fisher* came the introduction of the "foregone conclusion doctrine."[98] The foregone conclusion doctrine states that when the government has enough substantive evidence—so much so that compelling the information adds nothing to the government's collective information—the acquisition of the testimony becomes a matter of "surrender."[99] Thus, the status of the communication is transformed from testimonial to nontestimonial, thereby making the compulsion of the testimony constitutional under the Fifth Amendment.[100] In these

91. *See id.* at 394 (discussing how individuals facing civil and criminal liability had retained counsel to look over their tax documents in the face of these charges). "In each case the summons was ordered enforced by the District Court and its order was stayed pending appeal." *Id.* at 395.

92. *See id.* at 395–96 (resolving the issue in favor of the government and concluding that the taxpayer's Fifth Amendment Privilege did not excuse the attorney from producing the summoned documents).

93. *See id.* at 399 (noting that not every invasion into privacy violates the privilege against self-incrimination).

94. *See id.* at 400 (referencing the fact that the Framers included personal privacy directly in the Fourth Amendment rather than in the Fifth).

95. *Id.* at 397. The Court cited an abundance of case law to support this proposition. *See id.*

96. *See id.* at 399.

97. *Id.* at 401 (citing United States v. Nobles, 422 U.S. 225, 233 n. 7 (1975)).

98. *Id.* at 411.

99. *Id.* (explaining that in a situation of this nature, "no constitutional rights are touched").

100. *See Fisher*, 425 U.S. at 411; *see also* United States v. Hubbell, 530 U.S. 27, 44 (2000); State v. Andrews, 197 A.3d 200, 204–05 (N.J. Super. Ct. App. Div. 2018) (restating that, in order for the foregone conclusion doctrine to apply, the state must prove with "reasonable particularity (1) knowledge of the existence of the evidence demanded; (2) defendant's possession and control of that evidence; and (3) the authenticity of the evidence").

circumstances, the burden is on the government to show that the possession, existence, or authentication of the evidence is a foregone conclusion.[101]

Although all members of the Court agreed with the holding in *Fisher*, the pushback on the majority's rationale is particularly insightful when analyzing how the Fifth Amendment should be applied to emerging issues in a modern society.[102] The concurring justices opined that the privilege against self-incrimination was not given its proper weight, in light of its history.[103] In Justice Brennan's concurring opinion, he viewed the reasoning of the Court as disruptive to the privacy principles that were settled nearly a century prior in *Boyd*[104] and asserted that the majority opinion's rationale dismantled established personal privacy rights.[105] He further explained that the privilege against self-incrimination is central to the human experience and "reflects 'our respect for the inviolability of the human personality and of the right of each individual "to a private enclave where he may lead a private life."'"[106] Viewed this way, the Fifth Amendment's construction creates a safe place for an individual to harbor feelings and thoughts safe from government intrusion[107]—so much so that the privilege against self-incrimination "enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment."[108] The idea that private thoughts and personal writings could be used in criminal proceedings crystallized the need for a constitutional safeguard to protect these intimacies of the mind.[109] Justice Marshall also authored a concurring opinion in which he echoed that the testimonial element the majority adopted in *Fisher* was "contrary to the history and tradition of the privilege against self-incrimination both in this country and in England, where the privilege originated."[110]

---

101. *See* United States v. Doe, 465 U.S. 605, 614 n.13 (1984); *see also Hubbell*, 530 U.S. at 44–45 (comparing its facts to those in *Fisher* and finding that the government had not established that the documents in question were a foregone conclusion because the government had not shown any prior knowledge of the documents' existence or whereabouts).

102. *See Fisher*, 425 U.S. at 415–34 (concurring opinions by Justices Brennan and Marshall); *see also Doe*, 465 U.S. at 620–23 (Stevens, J., dissenting in part) (discussing the Fifth Amendment implications of the case).

103. *Fisher*, 425 U.S. at 421; *see also id.* at 430 (Marshall, J., concurring).

104. *See id.* at 415–16 (Brennan, J., concurring).

105. *See id.* at 416 (Brennan, J., concurring).

106. *Id.* (Brennan, J., concurring) (citing Murphey v. Waterfront Comm'n, 378 U.S. 52, 55 (1964)).

107. *See id.* (Brennan, J., concurring).

108. *Id.* (Brennan, J., concurring) (citing Griswold v. Connecticut, 381 U.S. 479, 484 (1965)).

109. *See id.* at 420 (Brennan, J., concurring).

110. *Id.* at 431 (Marshall, J., concurring).

Following *Fisher*, the Supreme Court addressed the issue of compelled production of potentially incriminating documents in *Doe v. United States*.[111] In *Doe*, the Court not only reiterated the history and purpose of the Fifth Amendment,[112] but elaborated further on the testimonial component required for asserting the privilege against self-incrimination.[113] The petitioner in *Doe* adamantly fought government efforts to compel production of bank records tied to his offshore accounts.[114] The district court had denied the government's motions to compel Doe to sign numerous consent forms which would have allowed the government to access the accounts at issue.[115] The district court's denial was based on the grounds that signing the forms could be considered testimonial and would essentially require Doe to admit the existence of the alleged accounts.[116] However, the Court of Appeals for the Fifth Circuit reversed the decision, finding no testimonial significance to Doe's signature.[117]

The Supreme Court granted certiorari and concluded that for a person to be compelled to be a "witness" against himself or herself, as stated in the Fifth Amendment, the nature of his or her communication must be explicitly or implicitly related to a "factual assertion or disclosure of information."[118] In shaping what constitutes a testimonial communication, the Court relied on previous decisions that held certain actions were not privileged, despite their incriminating results.[119] For example, compelling a suspect to submit to a blood test,[120] furnish a handwriting[121] or voice sample,[122] stand in a line-up,[123] or try on a

111. Doe v. United States, 487 U.S. 201, 202–03 (1988).

112. *See id.* at 212; *see also id.* at 220 (explaining that the purpose behind the Fifth Amendment was to right the wrongs of the Star Chamber courts and uphold what we consider to be an "accusatorial system of justice") (Stevens, J., dissenting).

113. *See id.* at 210.

114. *See id.* at 202 (detailing that petitioner, Doe, ended up in civil contempt of court and was ordered to be confined until he cooperated with the government's order, although his sanction was stayed pending appeal of his case).

115. *See id.*

116. *See id.* at 203–04.

117. *See id.* at 205.

118. *See id.* at 210.

119. *See id.*

120. *See* Schmerber v. California, 384 U.S. 757, 765 (1966) (holding that withdrawal, testing, and the subsequent analysis were not testimonial statements by the defendant and, therefore, were not subject to Fifth Amendment protection).

121. *See* Gilbert v. California, 388 U.S. 263, 266–67 (1967) (holding that the taking of handwriting exemplars during an FBI interrogation was not testimonial because a "mere handwriting exemplar" is a physical characteristic outside of Fifth Amendment protection, unlike the writing's content).

122. *See* United States v. Dionisio, 410 U.S. 1, 6–7 (1973) (holding that compelled voice recordings from the defendant did not give rise to Fifth Amendment protection

particular article of clothing[124] are all incriminating acts disqualified from the privilege's protection due to their nontestimonial nature.[125] In each case, the Supreme Court found that the testimony did not possess the communicative characteristic of the defendant disclosing knowledge or voicing guilt.[126] The Court in *Doe* rationalized that the compulsion in the listed examples did not force the suspect "to disclose the contents of his [or her] own mind."[127] Rather, those cases hinged on the idea that the identifiable physical characteristics of the testimony discounted their communicative nature.[128] For those reasons, the Court in *Doe* held that the consent directive compelling Doe's signature was not testimonial and, therefore, did not trigger Fifth Amendment protection.[129]

Justice Stevens dissented in *Doe*, distinguishing the case, not by physical evidence but by the idea that compelling Doe's signature was forcing him to use his mind to aid the government in the case against him.[130] Justice Stevens analogized that a defendant can be "forced to surrender a key to a strongbox containing incriminating documents, but [cannot] be compelled to reveal the combination to his wall safe—by word or deed."[131] In the eyes of Justice Stevens, the situation presented in *Doe* was a combination rather than a key.[132]

---

because the recordings were being used as a measure of the physical properties of the witnesses' voices rather than for the testimonial content of the communication).

123. *See* United States v. Wade, 388 U.S. 218, 221–22 (1967) (holding that the defendant's appearance in a pretrial lineup did not violate his self-incrimination privilege because "it [was] compulsion of the accused to exhibit his physical characteristics, not compulsion to disclose any knowledge he might have").

124. *See* Holt v. United States, 218 U.S. 245, 252–53 (1910) (holding that the defendant compelled to try on a blouse for the jury to test its fit did not violate the self-incrimination privilege). *Holt* is one of the earliest cases to mention the idea of the defendant's bodily features as evidence rather than communication, and the Court cites to virtually no authority to support that assertion. *See id.*

125. *See* Doe v. United States, 487 U.S. 201, 210 (1988).

126. *See id.* at 211 (quoting Curcio v. United States, 354 U.S. 118, 128 (1957)).

127. *Id.*

128. *See* Schmerber v. California, 384 U.S. 757, 765 (1966); Gilbert v. California, 388 U.S. 263, 266–67 (1967); United States v. Dionisio, 410 U.S. 1, 6–7 (1973); *Wade*, 388 U.S. at 221–22; *Holt*, 218 U.S. at 252–53; *cf. Schmerber*, 384 U.S. at 773–78 (Warren, C.J., dissenting) (dissenting justices voiced their deep concern for the Court's holding and rationale, stating that its "restrictive" reading of the Fifth Amendment deprives citizens of their rights and would be used as an "instrument" to narrow more constitutional protections in the future); *Wade*, 388 U.S. at 260–62 (Fortas, J., concurring in part) (Justice Fortas, joined by the Chief Justice, explaining the disdain for the "insidious doctrine" created in *Schmerber* to "extend beyond the invasion of the body" and encroach upon the rights of the individual).

129. *See Doe*, 487 U.S. at 219.

130. *See id.* (Stevens, J., dissenting).

131. *Id.* (Stevens, J., dissenting).

132. *See id.* (Stevens, J., dissenting).

The combination-key analogy employed by Justice Stevens has continually been used to compare the nontestimonial characteristics of a blood test or fingerprint identification to compelled biometric decryption.[133] Courts have used the analogy to hold that a biometric password is more akin to a key to a phone rather than a combination to a safe.[134] The notion that biometric passwords lack a testimonial component, coupled with the foregone conclusion doctrine introduced in *Fisher*, are common arguments asserted to rationalize why compelled biometric decryption should be considered nontestimonial.[135] Accordingly, courts that adopt this reasoning find that compelled biometric decryption is not protected under the privilege against self-incrimination.[136] Courts agreeing with the dissenting and concurring justices in the aforementioned cases[137] focus on the implications of advancing technology and ongoing privacy concerns to hold that compelled biometric decryption *is* testimonial and constitutionally protected.[138]

C. The Juxtaposition of Case Law and Technology

In 1787, the Framers of the Constitution could never have imagined a six-by-three-inch device with two cameras on the back[139] that would house every intimate detail of our lives—never mind the fact that this device can be unlocked using the unique anatomy of an individual's face.[140] However, such technology is a reality of the twenty-first century; this Section explores how the judicial system is currently wrestling with how to reconcile these innovations with existing law.[141]

133. *See infra* section II.C.2.

134. *See infra* Section II.C.2.

135. *See infra* Section II.C.2.

136. *See infra* Section II.C.2.

137. *See Doe*, 487 U.S. at 219 (Stevens, J., dissenting); Fisher v. United States, 425 U.S. 391, 415 (1976) (Brennan, J., concurring); *see also Fisher*, 425 U.S. at 431 (Marshall, J., concurring).

138. *See infra* Section II.C.2; *see also supra* note 128 and accompanying text.

139. *See iPhone 11*, APPLE, https://apple.co/2OVBdgT (last visited Oct. 14, 2019) (detailing the features of the Apple iPhone 11).

140. *See id.* On Apple products, the Face ID TrueDepth "camera captures accurate face data by projecting and analyzing over 30,000 invisible dots to create a depth map of your face and also captures an infrared image of your face." *About FaceID Advanced Technology*, *supra* note 8.

141. *See* Sandalow, *supra* note 24, at 30; *see also infra* Part III.

1. Supreme Court Jurisprudence Recognizing Technological Advancement

The concept that courts interpret the law while considering the beliefs of society is well-settled,[142] and the holdings, dicta, and rationale of landmark cases show that the law can accommodate an advancing society.[143] In 2014, the Supreme Court in *Riley v. California*[144] addressed the intersection of personal-device privacy and Fourth Amendment warrant requirements.[145] The Court noted that just because the convenience of technology allows individuals to carry around the "privacies of life," that does not mean the information stored in the technology is "less worthy of the protection for which the Founders fought."[146] Particularly, the Court emphasized the impact of technological advancements, claiming that comparing data stored on a cell phone to the search of a physical item was like "saying a ride on horseback is materially indistinguishable from a flight to the moon."[147] In sum, the storage capacity and ubiquity of smartphones are fundamentally distinct from stacks of paper or photo albums because smartphones allow individuals to carry around their most important and intimate life details in their pocket.[148]

In 2018, the Supreme Court in *Carpenter v. United States*[149] stated that any "rule the Court adopts 'must take account of more sophisticated [technology] systems that are already in use or in development.'"[150] The Court's majority explained that the Court is obligated to protect the privacy rights of individuals as "[s]ubtler and more far-reaching means of invading privacy have become available to the Government."[151] Couched within *Carpenter*'s narrow scope is the idea that, as technology inevitably advances, the Court must continue to protect citizens' privacy rights—rather than leaving them "at the mercy of advancing technology."[152]

142. *See* Sandalow, *supra* note 24, at 30.
143. *See infra* Part III.
144. Riley v. California, 573 U.S. 373, 378 (2014).
145. *See id.* at 394–95.
146. *Id.* at 403 (citing Boyd v. United States, 116 U.S. 616, 630 (1886)).
147. *Id.* at 393.
148. *See id.* at 394.
149. Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).
150. *Id.* at 2218–19 (quoting Kyllo v. United States, 533 U.S. 27, 36 (2001)); *see also In re* Search of a Residence in Oakland, 354 F. Supp. 3d. 1010, 1014 (N.D. Cal. 2019).
151. *Carpenter*, 138 S. Ct. at 2223 (quoting Olmstead v. United States, 277 U.S. 438, 474–74 (1928) (Brandeis, J. dissenting)).
152. *Id.* at 2214 ("As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to

2. Common Law Treatments of Compelled Biometric Decryption of a Personal Device

For nearly a decade, courts have been examining the evidentiary predicament posed by personal devices, like smartphones.[153] The war of smartphone-password production began as a battle over spoken words.[154] Now, however, it is generally understood that an individual's speaking the password that unlocks a personal device is testimonial and that compelling that disclosure would violate the Fifth Amendment privilege against self-incrimination.[155]

Government requests to decrypt a personal device with an alphanumeric password,[156] a password that requires a testimonial communication, have now become requests to press a finger, or position a face, to a scanner to decrypt that same personal device.[157] Lower courts remain divided on the issue of whether compelled biometric decryption of a personal device is protected by the Fifth Amendment privilege against self-incrimination.[158] At this time, neither the Supreme Court nor any federal circuit court has specifically addressed the compelled

'assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" (alteration in original)).

153. Due to the amount of data smartphones can harbor, law enforcement has always been eager to decrypt personal devices in crime-solving efforts. *See* Evan T. Barr, *Compelled Use of Biometric Identifiers to Unlock Electronic Devices*, 261 N.Y.L.J., June 25, 2019, at 121, http://bit.ly/39yUlcs.

154. *See* United States v. Kirschner, 823 F. Supp. 2d 655, 669 (E.D. Mich. 2010) (discussing whether forcing a defendant to reveal a password is constitutional).

155. *See id.* at 669 (holding that requiring a defendant to communicate mental knowledge requires him or her to "disclose the contents" of his or her mind and thus implicates the self-incrimination clause); *accord In re* Boucher, No. 2:06-mj-91, 2007 WL 4246473, at *6 (D. Vt. Nov. 9, 2007) (explaining that the forgone conclusion doctrine did not apply to a password that existed only in the mind of the defendant, because the password was not a physical thing); *see also* United States v. Warrant, No.19-mj-71283-VKD-1, 2019 WL 4047615, at *2 (N.D. Cal. Aug. 26, 2019).

156. *See* Barr, *supra* note 153, at 121; Brief for the ACLU et al. as Amici Curiae Supporting Defendant-Appellee, Commonwealth v. Gelfgatt, No. SJC-11358, at *1 (Mass. Oct. 28, 2013).

157. *See* United States v. Maffei, No. 18-cr-00174-YGR-1, 2019 WL 1864712, at *1 (N.D. Cal. Apr. 25, 2019); State v. Diamond, 905 N.W.2d 870, 871 (Minn. 2018); *In re* Search of [Redacted], 317 F. Supp. 3d 523, 534 (D.D.C. 2018); *In re* Search Warrant Application for [Redacted Text], 279 F. Supp. 3d 800, 802–803 (N.D. Ill. 2017) (overturning magistrate judge's decision that compelled decryption violated the Fifth Amendment); Commonwealth v. Baust, No. CR14-1439, 2014 WL 10355635, at *1 (Va. Cir. Ct. Oct. 28, 2014).

158. *See* MICHAEL A. FOSTER, CATCH ME IF YOU SCAN: CONSTITUTIONALITY OF COMPELLED DECRYPTION DIVIDES THE COURTS 4 (2020), https://bit.ly/3jHzQzB.

biometric decryption issue[159]—requiring lower courts to apply outdated case law to a novel issue.[160]

To trigger the privilege against self-incrimination, the individual's action must be (1) compelled, (2) testimonial, and (3) incriminating.[161] In most instances of compelled biometric decryption, the elements of compulsion and incrimination are undisputed, as a government request for the production of the password likely exists,[162] as well as the likelihood that incriminating evidence follows.[163] Thus, the issue of compelled biometric decryption turns on whether the act of decryption is testimonial under the Fifth Amendment.[164] In other words, is the action of pressing the finger, or positioning the face, upon a scanner merely physical?

Lower courts disagree over whether compelled biometric decryption of a personal device is testimonial.[165] The majority of courts to have addressed the issue have decided that compelled biometric decryption of a personal device is not testimonial and, therefore, not protected under the Fifth Amendment.[166] These majority courts have interpreted the Fifth Amendment's provision that no person "shall be compelled . . . to be a

159. *See Diamond*, 905 N.W.2d at 876.

160. *See In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073 (N.D. Ill. 2017) (noting that United States v. Wade, 388 U.S. 218, 223 (1967), dealing with interpretating term "testimonial" under the Fifth Amendment, was decided before the creation of cell phones and dealt with the use of fingerprints for identification purposes only); *see also In re* Search of a White Google Pixel 3 XL Cellphone in a Black Incipio Case, 398 F. Supp. 3d 785, 790 (D. Idaho. 2019).

161. *See supra* Section II.B.2; *see also In re* Search Warrant Application for the Cellular Telephone in United States v. Anthony Barrera, No. 19 CR 439, 2019 WL 6253812, at *2 (N.D. Ill. Nov. 22, 2019).

162. The fact that users voluntarily create the information stored on phones—meaning the creation is not compelled—does not diminish the legal force of the government's request that it be disclosed. *See* United States v. Hubbell, 530 U.S. 27, 36 (2000).

163. *See Barrera*, 2019 WL 6253812, at *2.

164. *See id.*

165. *See Barrera*, 2019 WL 6253812, at *1, United States v. Maffei, No. 18-cr-00174-YGR-1, 2019 WL 1864712, at *1 (N.D. Cal. Apr. 25, 2019); State v. Diamond, 905 N.W.2d 870, 871 (Minn. 2018); *In re* Search of [Redacted], 317 F. Supp. 3d 523, 534 (D.D.C. 2018); *In re* Search Warrant Application for [Redacted Text], 279 F. Supp. 3d 800, 802–803 (N.D. Ill. 2017); Commonwealth v. Baust, No. CR14-1439, 2014 WL 10355635, at *1 (Va. Cir. Ct. Oct. 28, 2014). *But c.f. In re Application for a Search Warrant*, 236 F. Supp. 3d at 1073–74; *In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1013 (N.D. Cal. 2019); Seo v. State, 109 N.E.3d 418, 431 (Ind. Ct. App.), *transfer granted*, *opinion vacated*, 119 N.E.3d 90 (Ind. 2018).

166. *See Barrera*, 2019 WL 6253812, at *1; *In re* Search of a White Google Pixel 3XL Cellphone in a Black Incipio Case, 398 F. Supp. 3d 785, 793 (D. Idaho 2019); *Maffei*, 2019 WL 1864712, at *7; *Diamond*, 905 N.W.2d 870 at 871; *In re Search of [Redacted]*, 317 F. Supp. 3d at 534; *In re Search Warrant Application for [Redacted Text]*, 279 F. Supp. 3d at 802–03; *Baust*, 2014 WL 10355635, at *1.

witness against himself"[167] to mean the defendant is protected from disclosing evidence that is testimonial or communicative in nature[168]—encompassing only those acts that force the accused to reveal the contents of his or her mind.[169] As a result, these courts consider biometric decryption of a personal device to be equivalent with submitting to a blood test,[170] furnishing a handwriting[171] or voice sample,[172] standing in a line up,[173] or trying on a particular article of clothing[174] for a jury[175]—all of which qualify as purely physical acts.[176] It follows, these courts explain, that compelled biometric decryption uses a purely physical feature, visible to the world, to decrypt the device without any input from the psyche of the individual.[177]

These courts distinguish the compelled biometric decryption issue from the line of cases dealing with compelled document production, which is sometimes considered a testimonial act.[178] The courts in the majority reason that submitting to compelled biometric decryption is distinct from the testimonial act of producing documents because gathering documents in response to a subpoena "*inherently* represent[s] communications from the defendant."[179] Instead, for compelled biometric decryption, law enforcement chooses the finger to place on the sensor to decrypt the device, thereby removing the defendant's mental processes

167. U.S. CONST. amend. V. (emphasis added).

168. *Baust*, 2014 WL 10355635, at *1; *see also In re* Grand Jury Subpoena Duces Tecum, 670 F.3d 1335, 1342 (11th Cir. 2012).

169. *See Baust*, 2014 WL 10355635, at *1; *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d at 1342; *see also* United States v. Doe, 487 U.S. 201, 212 (1987).

170. *See* Schmerber v. California, 384 U.S. 757, 765 (1966).

171. *See* Gilbert v. California, 388 U.S. 263, 266–67 (1967).

172. *See* United States v. Dionisio, 410 U.S. 1, 6–7 (1973).

173. *See* United States v. Wade, 388 U.S. 218, 221–22 (1967).

174. *See* Holt v. United States, 218 U.S. 245, 252–53 (1910).

175. *See In re* Search Warrant Application for the Cellular Telephone in United States v. Anthony Barrera, No. 19 CR 439, 2019 WL 6253812, at *6 (N.D. Ill. Nov. 22, 2019); *In re* Search of a White Google Pixel 3 XL Cellphone in a Black Incipio Case, 398 F. Supp. 3d 785, 793 (D. Idaho. 2019); *In re* Search of [Redacted], 317 F. Supp. 3d 523, 536 (D.D.C. 2018); State v. Diamond, 905 N.W.2d 870, 875–76 (Minn. 2018); *In re* Search Warrant Application for [Redacted Text], 279 F. Supp. 3d 800, 803–804 (N.D. Ill. 2017); Commonwealth v. Baust, No. CR14-1439, 2014 WL 10355635, at *3–4 (Va. Cir. Ct. Oct. 28, 2014).

176. *See supra* note 175 and accompanying text.

177. *See In re Search Warrant Application for [Redacted Text]*, 279 F. Supp. 3d at 805 (explaining that "physical characteristics do not themselves communicate anything"); *see also Barrera*, 2019 WL 6253812, at *6.

178. *See In re Search Warrant Application for [Redacted Text]*, 279 F. Supp. 3d at 804 (first citing Fisher v. United States, 425 U.S. 391, 410 (1976); then citing United States v. Doe, 465 U.S. 605, 614 (1984); and then citing United States v. Hubbell, 530 U.S. 27, 31 (2000)).

179. *Id.*

from the equation.[180] Another majority court determined that the biometric decryption could take place without the defendant even being conscious.[181] Thus, the courts that fall on the majority side of the compelled biometric decryption issue draw the line between testimonial and nontestimonial at speaking "12345"—viewing the fingerprint or the face as an unprotected, nontestimonial key rather than a testimonial combination.[182]

On the other hand, a few courts have elaborated on the gray area that compelled biometric decryption creates[183] and have held that the act of biometric decryption *is* testimonial.[184] In 2017, the United States District Court for the Northern District of Illinois denied a government request for "forced fingerprinting,"[185] appreciating the difference between using a fingerprint for identification purposes and using that same fingerprint to gain access to the "most intimate details of an individual's life."[186] The court observed that when a person unlocks a phone with an immutable password, like a fingerprint, that person effectively *tells* the government that he or she has accessed the phone and has enough control over it to enable fingerprint-password capabilities.[187] The court also alluded to the privacy implications supported by *Riley*, concluding that, in the modern era, the Fifth Amendment should shield individuals from compelled biometric decryption.[188]

---

180. *See* Search Warrant Application for [Redacted Text], 279 F. Supp. 3d at 804 (explaining that "fingerprint seizure" differs from compelled document production because a defendant is not making use of the contents of the mind in order to respond); *see also Barrera*, 2019 WL 6253812, at *6.

181. *See* State v. Diamond 905 N.W.2d 870, 877 (Minn. 2018).

182. *See id.* at 874. These cases follow the analogy that "telling an inquisitor the combination to a wall safe, [is] not like being forced to surrender the key to a strongbox." Commonwealth v. Baust, No. CR14-1439, 2014 WL 10355635, at *3 (Va. Cir. Ct. Oct. 28, 2014); *see also Diamond*, 905 N.W.2d at 872.

183. *See* United States v. Warrant, No.19-mj-71283-VKD-1, 2019 WL 4047615, at *1–2 (N.D. Cal. Aug. 26, 2019).

184. *See* United States v. Wright, No. 3:19-cr-00012-MMD-WGC-1, 2020 WL 60239, at *8 (D. Nev. Jan, 6, 2020); *In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1013 (N.D. Cal. 2019); Seo v. State, 109 N.E.3d 418, 431 (Ind. Ct. App. 2018), *transfer granted, opinion vacated*, 119 N.E.3d 90 (Ind. 2018); Matter of Single-family Home & Attached Garage, No. 17 M 18, 2017 WL 4563870, at *9 (N.D. Ill. Feb. 21, 2017); *In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1074 (N.D. Ill. 2017); *Warrant*, 2019 WL 4047615, at *1.

185. The court used this term to describe compelling someone to use their fingerprint to unlock their cell phone. *See In re Application for a Search Warrant*, 236 F. Supp. 3d at 1074.

186. *Id.* at 1073–74.

187. *See id.* at 1073.

188. *See id.* at 1074 (concluding that the "simple analogy that equates the limited protection afforded a fingerprint used for identification purposes to forced fingerprinting

In addition, the Court of Appeals of Indiana in *Seo v. State*[189] determined that compelled biometric decryption of a smartphone in any form is testimonial.[190] Although its decision was later vacated,[191] the court astutely described the dilemma of applying obsolete case law to a modern issue.[192] In *Seo*, the court observed that the breadth of case law that courts have to rely on regarding compelled decryption dealt with compelled document production.[193] The court provided a multitude of statistics[194] that culminated to one conclusion—a smartphone is fundamentally different than "paper-based media."[195]

In 2019, another court found that compelled biometric decryption triggers Fifth Amendment protection.[196] In this case, a magistrate judge in Oakland, California, denied a government warrant application to compel an individual to use his thumb or face to unlock a device found at a crime scene.[197] Judge Kandis Westmore noted the challenge of "technology outpacing the law,"[198] and cited to both *Carpenter* and *Kyllo v. United States*[199] to emphasize that citizens should not have to forfeit their constitutional rights to use the newest technologies.[200]

The government, in the warrant application before Judge Westmore, admitted that a biometric password may be used in lieu of an alphanumeric passcode to unlock a device, acknowledging that users are frequently prompted to enter a passcode when biometric verification fails

---

to unlock an Apple electronic device . . . is [not] supported by Fifth Amendment jurisprudence").

189. Seo v. State, 109 N.E.3d 418, 431 (Ind. Ct. App. 2018), *transfer granted, opinion vacated*, 119 N.E.3d 90 (Ind. 2018).

190. *See id.*

191. *See* Eunjoo Seo v. State, 112 N.E.3d 1082 (Ind. 2018).

192. *See Seo*, 109 N.E.3d at 438–49.

193. *See id.* Majority courts in compelled biometric decryption cases rely primarily on *Fisher*, *Doe*, and *Hubell*. *See supra* note 180 and accompanying text.

194. According to Apple statistics from 2016, individuals send up to 200,000 iMessages per second. *See* Kif Leswing, *Apple Says People Send as Many as 200,000 iMessages per Second*, BUSINESS INSIDER (Feb. 12, 2016, 2:08 PM), http://bit.ly/3bEFW0c. Smartphones have also been dubbed a "second brain." *See* Yo Zushi, *Life With a Smartphone Is Like Having a Second Brain in Your Pocket*, NEWSTATESMANAMERICA (Feb. 22, 2017), http://bit.ly/3bFRi48.

195. *Seo*, 109 N.E.3d at 438 (analogizing a smartphone to a personal privacy warehouse rather than mere production of documents).

196. *See In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1013 (N.D. Cal. 2019), *rev'd sub nom*, *In re* Search of a Residence in Oakland, No. 19-mj-70053-KAW-1(JD), 2019 WL 6716356, at *4 (N.D. Cal. Dec. 10, 2019) (upholding Judge Westmore's opinion by dismissing motion to review).

197. *See id.*

198. *In re Search of a Residence in Oakland*, 354 F. Supp. 3d at 1013–14.

199. Kyllo v. United States, 533 U.S. 27 (2011); *see supra* Section II.C.1.

200. *See id.* at 1015; *see also supra* Section II.C.1.

or a device restarts.[201] Since compelling an individual to speak the numbers or letters of a password violates the privilege against self-incrimination, Judge Westmore deciphered the government's desire to compel a biometric password as a means of circumventing the privilege against self-incrimination.[202]

Further, Judge Westmore denied the warrant application on the grounds that unlocking a personal device with a fingerprint or a face fundamentally differs from a suspect submitting to a fingerprint analysis, which is a nontestimonial act.[203] Rather than using the fingerprint or physical evidence for comparison or corroboration purposes, compelling a biometric password signals that the suspect has "possession and control" of the device and "authenticates [his or her] ownership and access to the [device] and all of its digital contents."[204] Thus, due to the implications that flow from successfully unlocking a device with a biometric password, the act surpasses the threshold of testimonial communication by exceeding mere "physical evidence."[205] Judge Westmore's line of reasoning has been applied by several courts across the United States to find that compelled biometric decryption is testimonial.[206]

In the *Oakland* opinion, Judge Westmore admitted that an admirable government interest is furthered by allowing law enforcement to compel an individual to decrypt his or her phone with a biometric password.[207] Uncovering evidence on a personal device can lead to the apprehension of violent criminals[208] and can provide proof of heinous sexual crimes.[209] However, classifying compelled biometric decryption

201. *See In re Search of a Residence in Oakland*, 354 F. Supp. 3d at 1015–16 (reaffirming that these tools are used as privacy methods to secure the information encrypted in the device); *In re* Search Warrant Application for [Redacted Text], 279 F. Supp. 3d 800, 802–803 (N.D. Ill. 2017) (discussing that an alphanumeric password must be used instead of a biometric password in instances of device restarting or after a 48-hour interval of inactivity).

202. *See In re Search of a Residence in Oakland*, 354 F. Supp. 3d at 1016 (explaining that the processes are two means to the same end).

203. *See id.*

204. *Id.* This can be especially incriminating when possession is an essential element of the crime being charged. *See, e.g.*, United States v. Wright, No. 3:19-cr-00012-MMD-WGC-1, 2020 WL 60239, at *8 (D. Nev. Jan, 6, 2020).

205. *See In re Search of a Residence in Oakland*, 354 F. Supp. 3d at 1016.

206. *See* United States v. Warrant, No.19-mj-71283-VKD-1, 2019 WL 4047615, at *2–3 (N.D. Cal. Aug. 26, 2019); *Wright*, 2020 WL 60239, at *8.

207. *See In re Search of a Residence in Oakland*, 354 F. Supp. 3d at 1016.

208. *See* People v. Davis, 438 P.3d 266, 267, 270 (Colo. 2019); *see also* Commonwealth v. Baust, No. CR14-1439, 2014 WL 10355635, at *1 (Va. Cir. Ct. Oct. 28, 2014) (indicting the Defendant for "strangling another causing wounding or injury").

209. Many biometric decryption cases involve prosecution for child pornography. *See* United States v. Apple MacPro Computer, 851 F.3d 238, 242 (3d Cir. 2017); *In re*

as testimonial does not render the government helpless.[210] The forgone conclusion doctrine introduced in *Fisher* continues to serve as a means of transforming testimonial acts into nontestimonial matters of surrender.[211]

As more devices incorporate biometric encryption, the prevalence of compelled biometric decryption litigation is likely to increase.[212] As noted by one court, due to lack of Supreme Court guidance, lower courts on both sides of the issue are operating with a degree of uncertainty, leaving individual rights at the mercy of the courts.[213]

D. Legislative Initiative to Protect Biometric Identifiers

Ultimately, for lawyers arguing compelled biometric decryption cases, the issue turns on whether the compelled decryption of the personal device is testimonial.[214] However, in reality, it is the everyday citizen that is left with the consequences of those court battles.[215] Therefore, to offer a workable and comprehensive analysis of the Fifth Amendment privilege against self-incrimination, one must consider how biometric identifiers, like the face behind FaceID, are protected at the state and federal level.[216] Accordingly, this Section explores emerging biometric privacy legislation.

In examining how legislatures are protecting biometric privacy, the author does not intend to conflate the issues of constitutional jurisprudence and biometric privacy law.[217] Rather, the legislation discussed below is examined *in addition to* the history and evolution of the Fifth Amendment to emphasize the degree of protection biometric identifiers, like fingerprints and faces, are being afforded by legislatures.[218]

Search Warrant Application for [Redacted Text], 279 F. Supp. 3d 800, 801 (N.D. Ill. 2017); United States v. Kirschner, 823 F. Supp. 2d 665, 666–67 (E. D. Mich. 2010).

210. *See Seo v. State*, 109 N.E.3d 418, 439 (Ind. Ct. App. 2018), *transfer granted, opinion vacated*, 119 N.E.3d 90 (Ind. 2018) (noting the government can use the third party doctrine, and other methods, to obtain the information).

211. *See* Fisher v. United States, 425 U.S. 391, 411 (1976); *see also Baust*, 2014 WL 10355635, at *4.

212. *See* FOSTER, *supra* note 158.

213. *See In re Search Warrant Application for [Redacted Text]*, 279 F. Supp. 3d at 807; *see also* Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).

214. *See Fisher*, 425 U.S. at 400; *see also supra* Section II.B.2.

215. *See generally* Sandalow, *supra* note 24, at 38 (discussing how the Supreme Court's response to important legal issues relates to social change).

216. The discussion of the following statutes does not aim to provide an intricate account of all the inner workings and applications of these statutes. Rather, the discussion seeks to provide an overview of the broader issue the legislation is addressing. For a more comprehensive analysis of these state statutes, see Michael A. Rivera, *Face Off: An Examination of State Biometric Privacy Statutes & Data Harm Remedies*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 571 (2019).

217. *See infra* Section III.D.

218. *See infra* Section III.D.

The first piece of legislation that initiated the trend of biometric privacy laws was Illinois' Biometric Privacy Information Act (BIPA),[219] enacted on October 3, 2008.[220] The Illinois legislature enacted the BIPA in response to public apprehension[221] concerning the rapidly expanding use of biometric technology in commercial transactions[222] and the corresponding lack of safeguards for biometric information in such transactions.

The BIPA applies to an individual's retina or iris scans, fingerprints, voiceprints, or the anatomy of the hand or face[223]—all common biometric keys used to decrypt personal devices.[224] The BIPA requires covered entities[225] to take protective measures to secure an individual's "biometric identifiers" in order to remain in compliance with the Act.[226] Section 14/15(e)(2) of the BIPA is especially informative as to the protection of biometric encryption of personal devices.[227] Here, the statute requires that a covered entity must protect "biometric identifiers" (fingerprints, face scans, and the like) in the same manner as passcodes, account numbers, or pin numbers.[228] In section 14/15(e)(2), the Illinois legislature chose to treat biometric identifiers, and biometric information derived from those identifiers, with the same respect as other unique identifying information.[229]

The BIPA has served as a model statute for similar legislation across the country.[230] States that have since passed similar legislation include Texas,[231] Washington,[232] and California,[233] with many other

219. 740 ILL. COMP. STAT. 14/5 (2008).

220. Nicole Olson, *Biometrics Laws and Privacy Policies*, PRIVACYPOLICIES.COM BLOG (Sep. 4, 2019), http://bit.ly/2SNRLZ9 (discussing how Illinois law is the "archetype of biometric privacy laws").

221. *See id.* 14/5(d).

222. *See* 740 ILL. COMP. STAT. 14/5(b) (2008).

223. *See id.* 14/10. Within the BIPA these biometric markers are termed "biometric identifiers" because their unique nature can be used to identify an individual. *See id.*

224. *See* COLIN SOUTAR ET AL., ICSA GUIDE TO CRYPTOGRAPHY, at ch. 22 (Randal K. Nichols & McGraw-Hill eds., 1990), http://bit.ly/31TdTFI; *see also supra* Section II.A.

225. The BIPA defines a "covered entity" as a private entity, including "any individual, partnership, corporation, limited liability company, association, or other group." 740 ILL. COMP. STAT. 14/10 (2008).

226. *See id.* 14/15.

227. *See id.* 14/15(e)(2).

228. *See id.* 14/15(e)(2). This includes "stor[ing], transmit[ting], and protect[ing] from disclosure all biometric identifiers and biometric information." *Id.*

229. *See id.* 14/10.

230. *See* Olson, *supra* note 220 (discussing how Illinois law is the "archetype of biometric privacy laws"). For more information on the BIPA, see Charles N. Insler, *How to Ride the Litigation Rollercoaster Driven by the Biometric Information Privacy Act*, 43 S. ILL. U. L.J. 819 (2019).

231. The Texas Capture or Use Statute. *See* TEX. REV. CIV. STAT. § 503.001 (2017).

232. WASH. REV. CODE § 19.375 (2017).

states proposing legislation that closely resemble the BIPA.[234] While the enacted and proposed legislation do not perfectly mirror the BIPA, all are based on the premise that individual biometric identifiers deserve protection from unfettered commercial use.[235] At this time, no federal statute in existence regulates biometric privacy, despite pressure from the academic and legal communities to act on this deficiency, given the increasing popularity of biometrics.[236]

The crux of compelled biometric decryption cases is not whether the legislature has enacted statutes protecting biometric identifiers.[237] Nevertheless, the fact that legislative bodies at the state and federal levels have discussed protection of biometrics in modern society speaks volumes about the privacy interests that compelled biometric decryption raises.[238]

III. ANALYSIS

"[M]odern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[239] Consequently, these modern personal devices have forced courts to grapple with the issue of compelled biometric decryption.[240] The majority of courts that have addressed the compelled biometric decryption issue have turned a blind eye to technological advancements, and their respective holdings erode the history and tradition of the Fifth Amendment.[241] Given inconsistent lower court applications, the Supreme Court will likely be called upon again to provide guidance on this issue.[242] Until then, and in

233. The California Consumer Privacy Act of 2018 (CCPA). *See* CAL. CIV. CODE § 1798.105 (2020).

234. Molly K. McGinley et al., *The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States*, NAT. L. REV. (Mar. 25, 2019), http://bit.ly/39ycHu6 (explaining how Arizona, Florida, and Massachusetts have all proposed legislation closely resembling the BIPA).

235. 740 ILL. COMP. STAT. 14/5 (2008); TEX. REV. CIV. STAT. § 503.001 (2017); WASH. REV. CODE § 19.375.010 (2017).

236. *See generally* Carra Pope, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data*, 26 J.L. & POL'Y 769 (2018) (discussing biometric data and the need for federal biometric protection legislation). The Senate also introduced biometric privacy legislation on March 13, 2019, named the Commercial Facial Recognition Privacy Act of 2019, http://bit.ly/31WuOr4.

237. *See supra* Section II.C.2.

238. *See* Sandalow, *supra* note 24, at 33–34.

239. Riley v. California, 573 U.S. 373, 385 (2014).

240. *See supra* Section II.C.2.

241. *See Riley*, 573 U.S. at 403.

242. *See* FOSTER, *supra* note 158.

light of constantly advancing technology,[243] courts should err on the side of individual liberty and take modern advancements into account when evaluating whether compelled biometric decryption is testimonial.[244]

This Comment proposes that, as courts face the issue of compelled biometric decryption, they should analyze the issue through a public policy lens, giving deference to the history and purpose that created the privilege against self-incrimination.[245] By looking to public policy to evaluate the inherent connection between the personal device and the self, courts will more effectively apply the privilege against self-incrimination to modern society. Three components support the argument that public policy should be considered: (1) courts do an injustice to the evolution of the Fifth Amendment by continuing to classify all compelled biometric decryption as purely physical;[246] (2) society, by embracing evolving privacy practices and shifting toward biometric encryption, has demonstrated that advancing technology should be met with increased protection;[247] and (3) the communicative aspect of decrypting a personal device can label the decryption testimonial.[248]

A. A Textualist Interpretation: The Fifth Amendment Protects Privacy

Over centuries, society has built and bolstered the privilege against self-incrimination,[249] and society's embrace of advancing technology should not now render the privilege ineffective.[250] The evolution of the privilege against self-incrimination started with an emphasis on personal privacy.[251] The Supreme Court emphasized the protections of the privilege against self-incrimination so much that, in *Ullman*, the Court proclaimed that it would rather see a guilty person go free than infringe on the rights of an innocent person.[252]

The Fifth Amendment continues to protect intimate "human thought[s] and expression[s]" from government intrusion.[253] Today,

243. *See* Binary District Journal, *The Case Against Traditional Passwords — and How Biometrics Can Better Secure Us*, THE NEXT WEB (Oct. 2019), http://bit.ly/2vvXUBs.

244. *See infra* Section III.D.

245. *See infra* Section III.D.

246. *See supra* Section II.B.

247. *See supra* Sections II.C.1, II.D.

248. *See infra* Section III.C.

249. *See supra* Section II.B.

250. *See infra* Section III.D.

251. *See* Boyd v. United States, 116 U.S. 616, 630 (1886) (holding that Boyd did not have to turn over his private books).

252. *See* Ullmann v. United States, 350 U.S. 422, 427 (1956).

253. Braswell v. United States, 487 U.S. 99, 119 (1988) (Marshall, J., dissenting).

personal devices are the epicenter of human thought and expression.[254] Personal devices, today, are akin to Boyd's books in 1886.[255] By condoning compelled biometric decryption and access into what the Supreme Court has called "minicomputers,"[256] lower courts have allowed unfettered invasion into the psyche of the individual, left citizens without Fifth Amendment protection, and contradicted the purpose of the Fifth Amendment's privilege against self-incrimination.[257]

Supreme Court justices, since the opinions in *Fisher*, have warned against whittling down the protections of the privilege against self-incrimination.[258] Justice Stevens, in his dissent in *Doe*, described the privilege against self-incrimination as "a prohibition of the use of physical or moral compulsion to extort communications."[259] Today, compelled biometric decryption is exactly that. Compelled biometric decryption presents the twenty-first-century citizen with a disclosure quandary: convenience or privacy, information security or constitutional protection, biometric decryption or contempt of court.[260] This Comment thus proposes that courts give proper weight to the evolution of the privilege against self-incrimination, which was designed specifically to protect the individual from these disclosure dilemmas.[261]

B. The Modern Emphasis on Privacy Protection

Indeed, state legislatures have recognized that it is just as invasive, if not more invasive, to use biometric data to complete a transaction as it is to use a personalized identification number (PIN).[262] Introducing a barrage of biometric privacy legislation, numerous state legislatures are recognizing the prevalence of biometrics and advocating for consumer

254. *See* Riley v. California, 573 U.S. 373, 394 (2014).

255. *See* Boyd v. United States, 116 U.S. 616, 630 (1886).

256. *Riley*, 573 U.S. at 393 (calling cellphones "minicomputers" because they just as easily could be called "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers").

257. *See id.* at 403.

258. *See* Fisher v. United States, 425 U.S. 391, 415–16 (1976) (Brennan, J., concurring); Doe v. United States, 487 U.S. 201, 219 n.1 (1987) (Stevens, J., dissenting) ("[T]he deviation from this principle can only lead to mischievous abuse of the dignity the Fifth Amendment commands the Government afford its citizens."); *see also supra* note 128 and accompanying text.

259. *Doe*, 487 U.S. at 219 n.1 (quoting Holt v. United States, 218 U.S. 245, 252–53 (1910)).

260. *See* Seo v. State, 109 N.E.3d 418, 438–39 (Ind. Ct. App. 2018), *transfer granted, opinion vacated*, 119 N.E.3d 90 (Ind. 2018); *see also Attending a Protest*, SURVEILLANCE SELF-DEFENSE (June 2, 2020), https://bit.ly/3jAJILD (explaining that protestors should disable biometric encryption on their phones because officers can compel them to use biometric passwords to unlock the devices).

261. *See infra* Section III.D; *see also In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1013 (N.D. Cal. 2019).

262. *See* 740 ILL. COMP. STAT. 14/5 (2008).

biometric privacy protections with full force.[263] The majority of courts, however, are turning a blind eye to this evolution.[264] In effect, these courts tell individuals to sacrifice the convenience of biometric passwords in order to protect their personal devices from government intrusion—even though the applications on that device are shielded by a stronger, legislatively imposed, privacy standard.[265]

In addition to legislative recognition of biometric privacy interests, the Supreme Court has expounded on the unique privacy concerns raised by personal devices.[266] In *Kyllo*, the Supreme Court advised lower courts to consider "more sophisticated [technology] systems that are already in use or in development."[267] Further, in *Riley*, the Supreme Court pointed out that a person not carrying a personal device loaded with all of their sensitive information is the exception rather than the rule.[268] Additionally, in *Carpenter*, the Supreme Court warned against citizens' rights succumbing to advancing technology.[269] The instructions written throughout *Kyllo*, *Riley*, and *Carpenter* all point to the Supreme Court's recognition of the *sui generis*[270] nature of personal devices.[271] This is especially true today, when personal devices are starkly different from previous storage devices, like the traditional safe.[272] Thus, *Kyllo*, *Riley*, and *Carpenter* can be interpreted as providing lower courts the doctrinal wherewithal they need to expand privacy protections to keep up with new technology as it is developed.[273]

263. *See id.*

264. *See supra* Section II.C.2.

265. *See In re Search of a Residence in Oakland*, 354 F. Supp. 3d at 1016 (noting that personal device applications can provide access to private information like medical records and/or financial accounts); *see also* 740 ILL. COMP. STAT. 14/5 (2008).

266. *See* Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018); Riley v. California, 573 U.S. 373, 393–95 (2014); Kyllo v. United States, 533 U.S. 27, 34–36 (2001).

267. *Kyllo*, 533 U.S. at 36.

268. *See Riley*, 573 U.S. at 395 ("According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower.").

269. *See Carpenter*, 138 S. Ct. at 2214.

270. *Sui generis* translates to "of its own kind," emphasizing uniqueness. *See Sui Generis*, THE LAW DICTIONARY, http://bit.ly/37y5SHA (last visited Feb. 15, 2020).

271. *See Carpenter*, 138 S. Ct. at 2218; *Riley*, 573 U.S. at 393–95; *Kyllo*, 533 U.S. at 34–36.

272. *See In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1017 (N.D. Cal. 2019).

273. *See In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073 (N.D. Ill. 2017).

C. Communication Is Key: Applying Public Policy to Compelled Biometric Decryption

Currently, most lower courts do not accept compelled biometric decryption as testimonial due to the overwhelmingly physical nature of the act.[274] However, Judge Westmore and the courts in *In re Application for a Search Warrant* and *Seo* recognized that compelled biometric decryption surpasses pure physicality and classified the act of decryption as testimonial in nature.[275] These courts recognized that, today, a fingerprint scan or a face scan are incongruous with the physical acts used for identification that previous Fifth Amendment case law addressed.[276]

Thus, majority courts that attempt to diminish the communicative nature of biometric decryption by emphasizing the lack of mental process involved[277] are no longer correct. They have gone to great lengths to explain how biometric decryption is nontestimonial.[278] In *State v. Diamond*,[279] for example, the court suggested that the government could take the fingerprint from an unconscious individual and use it to unlock a personal device;[280] or in *Matter of Search of [Redacted]*, the court reasoned that compelled biometric decryption is not testimonial only because the defendant did not choose the finger.[281] In addition, scholar Orin Kerr has added that the particular act cannot be testimonial since, theoretically, the individual's finger could be cut off and achieve the same results.[282] In each context, the underlying justification is that using TouchID or FaceID doesn't require utilization of the individual's mind.[283]

Today, "testimony is not restricted to verbal or written communications."[284] Because biometrics are unalterable, when law enforcement uses a biometric password to unlock "X's iPhone" it not only identifies that person as "X" but also proves individual ownership,

274. *See id.* at 1070; *see also supra* Section II.C.2.

275. *See supra* Section II.C.2.

276. *See In re Application for a Search Warrant*, 236 F. Supp. 3d 1066 at 1073 (citing United States v. Wade, 388 U.S. 218, 223 (1967)).

277. *See In re* Search of [Redacted], 317 F. Supp. 3d 523, 535–36 (D.D.C. 2018).

278. *See supra* Section II.C.2.

279. *See* State v. Diamond, 905 N.W.2d 870, 871 (Minn. 2018).

280. *See id.* at 877.

281. *In re Search of [Redacted]*, 317 F. Supp. 3d at 536.

282. *See Judge Denies Blanket Right to Compel Fingerprint iPhone Unlocking*, NAKED SECURITY (Feb. 28, 2017), http://bit.ly/2URpK5L.

283. *See* United States v. Hubbell, 530 U.S. 27, 43 (2000).

284. *In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1015 (N.D. Cal. 2019).

access, and control of the device.[285] In characterizing compelled biometric decryption as testimonial, minority courts have equated this communication of producing the contents on a phone to the compelled production of documents; in both situations the defendant must use the contents of his or her mind to assemble the documents in response to a subpoena.[286] The majority of courts, to the contrary, have rejected the argument that compelled biometric decryption is analogous to compelled document production, because it is law enforcement, not the individual, who picks the finger to scan.[287] According to these courts, then, biometric decryption does not rise to the level of testimonial communication.[288] However this reasoning draws a line too thin to stand on. Applying the majority courts' logic to more advanced technology, must law enforcement hold a defendant's eyelids open for an iris scan[289] to be purely physical? Such logic is irreconcilable with modern advancements.

Aside from personal privacy concerns, the issue of compelled biometric decryption also implicates privacy rights regarding the physical body.[290] By not protecting biometric decryption, the majority of courts are condoning the dilemma foisted upon individuals of: (1) using their body to incriminate themselves or (2) facing jailtime for not complying with a subpoena or warrant.[291] From a public policy standpoint, it is senseless to inflict this dilemma upon someone when, simultaneously, the choice not to disclose an alphanumeric password is protected with full constitutional force.[292]

In sum, the majority's line of reasoning made sense until the personal device became an extension of the self.[293] For example, with a quick glance towards the FaceID scanner on a smartphone, an individual can provide the government access to 256 gigabytes of the most intimate

285. *See In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073 (N.D. Ill. 2017); *see also In re Search of a Residence in Oakland*, 354 F. Supp. 3d at 1016.

286. *See In re Application for a Search Warrant*, 236 F. Supp. 3d at 1073; *see also* United States v. Hubbell, 530 U.S. 27, 31 (2000); United States v. Doe, 465 U.S. 605, 614 (1984); Fisher v. United States, 425 U.S. 391, 410 (1976).

287. *See supra* Section II.C.2.

288. *See In re* Search of [Redacted], 317 F. Supp. 3d 523, 536 (D.D.C. 2018).

289. *See Street-Level Surveillance*, ELECTRONIC FRONTIER FOUND., http://bit.ly/38oCBAl (last visited Jan. 25, 2020).

290. *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965) ("The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment.").

291. *See* Seo v. State, 109 N.E.3d 418, 420 (Ind. Ct. App. 2018) (discussing how Seo was held in contempt for denying a law enforcement request to unlock her phone).

292. *See* Commonwealth v. Baust, No. CR14-1439, 2014 WL 10355635, at *4 (Va. Cir. Ct. Oct. 28, 2014).

293. *See* Riley v. California, 573 U.S. 373, 385 (2014).

details of that individual's life[294]—not to mention the trove of private information that could be revealed if a person were compelled to unlock a personal computer.[295] It is no longer workable to separate the action of decryption from the person, especially considering the person is now the means of decryption.

D. Recommendation

When analyzing whether compelled biometric decryption is testimonial or not, courts should conduct their analyses through a public policy lens. Currently, most courts conclude their analyses after determining that the defendant had not divulged the contents of his or her mind.[296] But ending the analysis there fails to account for advancing technology and the private details stored within personal devices.[297] The law will never stop playing catch-up with technology,[298] but the introduction of a public policy approach to the analysis can spare individual privacy rights from intrusive government action.

Even after balancing public policy concerns, some courts may still categorize compelled biometric decryption as nontestimonial.[299] To support this conclusion, those courts may reason that the government would essentially be prohibited from gathering evidence, given the prevalence of biometric encryption in personal devices.[300] However, bolstering privacy protection would not spell the extinction of government investigations.[301]

There are multiple ways the government can gain access to the evidence it seeks other than compelling a biometric password.[302] First, the forgone conclusion doctrine would continue to apply to biometric decryption.[303] The government could also obtain the information from a third party.[304] Further, if a defendant grants consent or unlocks their device for law enforcement, there is no Fifth Amendment issue—assuming the consent was not coerced.[305] These options still allow the

294. *See iPhone 11*, *supra* note 139.

295. *MacBook Pro*, APPLE, https://apple.co/2tYCpsx (last visited Jan. 12, 2020).

296. *See supra* Section II.C.2.

297. *See supra* Section III.C.

298. *See In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1016 (N.D. Cal. 2019).

299. *See supra* Section II.C.2.

300. *See In re Search of a Residence in Oakland*, 354 F. Supp. 3d at 1016.

301. *See* Jonathan Mayer, *Government Hacking*, 127 Y.L.J. 570, 655 (2018).

302. *See* Seo v. State, 109 N.E.3d 418, 439 (Ind. Ct. App. 2018).

303. *See supra* Section II.B.2; *see also* Fisher v. United States, 425 U.S. 391, 410 (1976). For an analysis of how the forgone conclusion applies to smartphones, see DAVID M. NISSMAN & ED HAGEN, LAW OF CONFESSIONS § 3:19 (2d ed. 2019).

304. *See Seo*, 109 N.E.3d at 439.

305. *See* State v. Stahl, 206 So. 3d 124, 128 (Fl. Dist. Ct. App. 2016).

government to carry out its axiomatic functions of solving crime and maintaining public safety, while simultaneously respecting the constitutional rights of all citizens.

IV. CONCLUSION

The Fifth Amendment privilege against self-incrimination was designed to protect individual privacy and uphold the accusatorial system of justice.[306] Courts' failure to protect individuals from compelled biometric decryption has created a loophole that is contrary to the foundation and intent of the privilege against self-incrimination itself.[307] Allowing the government to sidestep individual privacy thwarts the privilege's potential to protect constitutional liberties.[308] To prevent such harm, courts should analyze compelled biometric decryption through the lens of public policy.[309]

Individuals' choice to embrace modern technology should not render their biometric features freely available for government exploitation.[310] "The fact that technology now allows an individual to carry . . . information in his [or her] hand does not make the information any less worthy of the protection for which the Founders fought."[311] A public policy approach preserves the privacy rights that the Fifth Amendment privilege against self-incrimination was built to protect,[312] while eliminating the dilemma of choosing between convenience or constitutional protection.

306. *See supra* Section II.B.
307. *See supra* Sections II.C.2, III.A.
308. *See supra* Part III.
309. *See supra* Section III.D.
310. *See supra* Part III.
311. Riley v. California, 573 U.S. 373, 403 (2014).
312. *See supra* Section II.B.