Volume 53 | Number 2 pp.427-466

"Your Device is Disabled": How and Why Compulsion of Biometrics to Unlock Devices Should be Protected by the Fifth Amendment Privilege

Harrison Metz

"YOUR DEVICE IS DISABLED": HOW AND WHY COMPULSION OF BIOMETRICS TO UNLOCK DEVICES SHOULD BE PROTECTED BY THE FIFTH AMENDMENT PRIVILEGE

I. INTRODUCTION

You press your thumb to the scanner on your iPhone.[1] Your fingers are sweaty, and you hope the scanner will not read your fingerprint correctly. Normally, this misreading of your thumb is only a minor inconvenience, requiring a quick wipe on your shirt. Today though, with the officer standing at your shoulder telling you to try again just as your iPhone tells you the same, you hope it keeps malfunctioning. This time, however, the phone unlocks, and the officer takes the phone and hands it to a technician. You feel like your privacy has been violated, like you should not have had to hand over everything in your phone. Your texts, pictures, notes, Apple account, and countless other private items are now in the hands of the government. If you had used a normal password, the officer could not have forced you to unlock it without a warrant. Compulsion to provide your normal password would have been protected by the Fifth Amendment privilege against self-incrimination. However, providing a biometric password is not protected by the Fifth Amendment privilege.

Modern technologies, such as Apple's Touch ID and Face ID, Samsung's Iris Scanner, and even fingerprint scanners on the average laptop, challenge the traditional rule that biometric data is not protected by the Fifth Amendment privilege.[2] These recent technologies use a person's biometric data in a different context than it was traditionally used but is used no differently than an alphanumeric password.[3] However, only compulsion of alphanumeric passwords is protected by Fifth Amendment privilege, and the increasing use of biometric encryption necessitates protection of this new form of encryption by the privilege against self-incrimination.[4]

---

1 This is a hypothetical situation created by the author and mirrors no other source.

2 *See infra* Part III (providing the argument in support of extending the privilege against self-incrimination to cover compulsion of a person's biometrics to unlock that person's device).

3 *See infra* Part II.B (discussing the similarities between normal encryption and biometric encryption).

4 *See infra* note 197 (providing an example of how alphanumeric passwords are protected and how the increasing use of biometric encryption creates a need for its protection from compulsion of biometric passwords by the government).

To be protected by the privilege, one must be: (1) compelled by the government; (2) to give testimony; (3) that self-incriminates.[5] Courts have long held that biometric data such as fingerprints, hair samples, and voice samples are not protected by the privilege because providing biometric data is not testimonial in nature.[6] The idea was, and largely remains, that providing biometric data is merely for identification purposes.[7] As a result, some courts have recently held that compulsion to provide biometric data, such as fingerprints, to unlock devices is not protected by the Fifth Amendment privilege.[8] Few courts have held that the privilege protects against compulsion of biometrics to unlock a device.[9]

This Note proposes a combined argument for a new doctrine, testimonial biometrics, that a defense attorney can use in court to sway the judge in favor of extending the privilege.[10] With the increasing use of biometric encryption on all kinds of devices, a need exists to extend the privilege to protect compulsion of biometric decryption.[11] Without this

---

5 *See* Fisher v. United States, 425 U.S. 391, 408 (1976) (expressing the three elements that must be present for the privilege to be properly invoked).

6 *See, e.g.*, Schmerber v. California, 384 U.S. 757, 765 (1966) (holding that the taking of a blood sample from a suspected drunk driver for a blood-alcohol test did not violate the suspect's privilege against self-incrimination because it is not testimonial). *See also* United States v. Dionisio, 410 U.S. 1, 6 (1973) (ruling that compulsion of a voice sample did not violate the privilege because compelled display of identifiable physical characteristics infringes no interest protected by the privilege against compulsory self-incrimination); United States v. Wade, 388 U.S. 218, 222 (1967) (finding that being compelled to display oneself in a police lineup did not violate the privilege because it is not giving testimony).

7 *See, e.g.*, *Schmerber*, 384 U.S. at 763–65 (reasoning that providing blood for testing has no communicative value and, therefore, is not testimonial); *Dionisio*, 410 U.S. at 5–7 (explaining that providing a voice exemplar is a type of verbal response, but it does not communicate anything because it is only used for identification purposes); *Wade*, 388 U.S. at 221–23 (stating that standing in a police lineup did not communicate anything and that it merely displayed physical characteristics for identification).

8 *See* State v. Diamond, 890 N.W.2d 143, 150–51 (Minn. Ct. App. 2017) (finding that providing a fingerprint to unlock a device is not testimonial and therefore not protected by the privilege against self-incrimination); Commonwealth v. Baust, No. CR14-1439, 2014 WL 10355635, at *4 (Va. Cir. Ct. Oct. 28, 2014) (deciding that compulsion of a fingerprint to unlock a device is not protected by the privilege against self-incrimination).

9 *See In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073–74 (N.D. Ill. 2017) (holding that compulsion of a fingerprint to unlock a person's device is testimonial and, therefore, protected by the privilege against self-incrimination); In the Matter of the Search of a Residence in Oakland, Cal., No. 4-19-70053, 2019 WL 176937, at *2–4 (N.D. Cal. Jan 10, 2019) (following the example set in *In re Application for a Search Warrant* that providing biometrics to unlock a device is protected by the privilege against self-incrimination).

10 *See infra* Part III (proposing an argument that a defense attorney can use in court to argue in favor of extending the privilege to cover compulsion of a person's biometrics to unlock that person's device).

11 *See iPhone X*, APPLE (Sept. 26, 2017), https://www.apple.com/iphone-x/ [http://perma.cc/SMH2-V4HJ] (displaying the iPhone X's new technology to unlock access to a device using facial recognition, Face ID). This is the first Apple phone since the

protection, the possibility of government overreach and intrusion into individual privacy with the increasing popularity of biometric encryption increases.[12]

First, Part II discusses the background information necessary to fully understand the Fifth Amendment privilege and encryption.[13] Second, Part III delves into the analysis, which provides the lines of reasoning necessary to make the argument for extending the privilege in future litigation.[14] Next, Part IV contributes the new doctrine of testimonial biometrics; addresses possible counterarguments to the doctrine, including its limits; and lays out how a defense attorney can use it.[15] Finally, Part V concludes the Note, recapping why the protection is needed.[16]

II. BACKGROUND

Understanding the necessity of extending the privilege against self-incrimination to compulsion of a person's biometrics to unlock that person's device requires background of the privilege, what encryption is, and what encryption traditionally protects.[17] Part II.A begins with a

---

introduction of the 5s in 2014 to not use Apple's signature Touch ID. *Id.* However, Apple's iPhone 8 and 8 Plus retain that feature. *See iPhone 8*, APPLE (Oct. 23, 2017), https://www.apple.com/iphone-8/specs/ [https://perma.cc/4G5Z-YUUK] (explaining the iPhone 8's capabilities and features). Further, laptops continue to use fingerprint scanners as an alternative to a traditional alphanumeric passcode to unlock the computer. *See HP Elitebook*, HEWLETT PACKARD, http://store.hp.com/us/en/pdp/hp-elitebook-755-g4-notebook-pc---customizable-w5r00av-mb [http://perma.cc/C6LF-ED3D] (providing product specifications for the HP Elitebook laptop).

12 *See* Ullmann v. United States, 350 U.S. 422, 426–28 (1956) (discussing how the privilege was created and added to the Constitution, in part, to prevent the overreach of government).

13 *See infra* Parts II.A, II.B, II.C & II.D (explaining the background to the privilege against self-incrimination, cases that have applied the privilege to biometrics, and how encryption works).

14 *See infra* Part III (laying out the argument in support of extending the privilege to protect the compulsion of biometrics to unlock a person's device).

15 *See infra* Parts IV.A & IV.B.

16 *See infra* Part V.

17 *See infra* Parts II.A, II.B, II.C & II.D. This Note focuses almost entirely on the Fifth Amendment privilege against self-incrimination. *See infra* Parts II, III & IV (covering the Fifth Amendment privilege against self-incrimination and the testimonial biometrics doctrine that needs to be argued to extend the privilege). However, it is worth noting a few instances in which the Supreme Court recognized that the development of new technologies could result in the government infringing on individual privacy interests. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206 (2018) (finding that using cell phone location data to track a suspect, without a warrant, invades the suspect's reasonable expectation of privacy in his physical movements); Riley v. California, 134 S. Ct. 2473 (2014) (holding that officers need a warrant to search a cell phone during a traffic stop); Kyllo v. United States, 533 U.S. 27 (2001) (holding that the warrantless scanning of a suspect's house with an infrared camera to determine if a

history of what the privilege is and how it has been applied by courts since its adoption in the Constitution.[18] Part II.B discusses what encryption is and how it works.[19] The discussion of encryption also covers biometric encryption.[20] Next, Part II.C provides an overview of what the privilege traditionally does not protect.[21] Last, Part II.D gives examples in which courts proved willing to expand the privilege, as well as incorporate the Fourth Amendment protection against unreasonable searches and seizures.[22]

A. Privilege Against Self-Incrimination

First, it is vital to understand what the privilege against self-incrimination is and its history before discussing why it should be extended to cover biometric encryption.[23] The Framers of the Constitution included the privilege against self-incrimination as the third clause of the Fifth Amendment.[24] The clause states that "no person . . . shall be

---

drug farm was present violated the Fourth Amendment protection from unreasonable searches and seizures). Cases like *Kyllo*, *Carpenter*, and *Riley* show the Supreme Court's willingness to extend privacy doctrines in the face of new technologies that can allow government overreach. *See Kyllo*, 533 U.S. at 36 (discussing the advancements in technology that affect how the Fourth Amendment is applied).

18 *See infra* Part II.A.

19 *See infra* Part II.B.

20 *See infra* Part II.B.

21 *See infra* Part II.C.

22 *See infra* Part II.D.

23 *See infra* notes 24–54.

24 *See* U.S. CONST. amend. V. *See also Development and Scope: Self-Incrimination*, JUSTIA, https://law.justia.com/constitution/us/amendment-05/07-self-incrimination.html [https://perma.cc/RN5B-K2PP] (providing the history of the privilege and its scope). Prior to its inclusion in the United States Constitution, six states already included the privilege in their own constitutions. *Id*. However, the origin of the privilege predates these state constitutions significantly. *See id*. (describing the seventeenth-century English roots of the privilege against self-incrimination). Debate exists surrounding the privilege's arrival in colonial America. *See id*. (explaining the few instances of the privilege prior to the American Revolution). There is also debate on how the privilege rose to prominence. *See* LEONARD W. LEVY, ORIGINS OF THE FIFTH AMENDMENT: THE RIGHT AGAINST SELF-INCRIMINATION (1968) (expounding the privilege's origin and its use during accusatorial and inquisitorial criminal proceedings in England's Star Chamber and High Commission). *See also* John Fabian Wit, *Making the Fifth: The Constitutionalization of American Self-Incrimination Doctrine, 1791–1903*, 77 TEX. L. REV. 825 (1999) (discussing the new scholarship that led to the new belief that the privilege was borrowed from medieval and Renaissance Europe); John H. Langbein, *The Historical Origins of the Privilege Against Self-Incrimination at Common Law*, 92 MICH. L. REV. 1047 (1994) (asserting that the privilege gained prominence in the late eighteenth century with the rise of adversarial systems of criminal procedure). Both Langbein and Levy provide interesting historical approaches to the origin of the privilege that can help further understand the privilege's role in American jurisprudence. *Compare id*. (arguing that the privilege's prominence coincided with the transition to adversarial systems of criminal

compelled in any criminal case to be a witness against himself."[25] A simple statement in theory, applying the privilege proved far more difficult in practice after its inclusion in the Constitution.[26] James Madison, the main proponent and drafter of the privilege, provided no explanation of its fundamental purpose or scope, and it was subsequently left to the Supreme Court to interpret.[27]

Over the following centuries, the Supreme Court and lower courts faced the task of interpreting the scope and implementation of the privilege many times.[28] Indeed, prior to the ratification of the Fourteenth Amendment and the Fifth Amendment's incorporation in 1964, the privilege only applied to federal criminal proceedings.[29] Despite this, late

---

procedure), *with* LEVY (propounding that the privilege arose from the resistance to England's use of the Star Chamber and High Commission in criminal proceedings).

[25] U.S. CONST. amend. V. *See also Fifth Amendment: An Overview*, CORNELL UNIV. L. SCH., https://www.law.cornell.edu/wex/Fifth_Amendment (stating that the privilege protects criminal defendants and witnesses from being compelled to provide testimony that would incriminate themselves).

[26] *See* Akhil Reed Amar & Renee B. Lettow, *Fifth Amendment First Principles: The Self-Incrimination Clause*, 93 MICH. L. REV. 857 (1995) ("The Self-Incrimination Clause of the Fifth Amendment is an unsolved riddle of vast proportions, a Gordian knot in the middle of our Bill of Rights."). *See also* Ronald J. Allen & M. Kristin Mace, *The Self-Incrimination Clause Explained and Its Future Predicted*, 94 J. CRIM. L. & CRIMINOLOGY 243 (2004) ("Testimony, however, has never been defined clearly and is the source of the remaining unpredictability in the future of the Fifth Amendment."); Albert W. Alschuler, *A Peculiar Privilege in Historical Perspective: The Right to Remain Silent*, 93 MICH. L. REV. 2625 (1996) ("Supreme Court decisions have vacillated between two incompatible readings of the Fifth Amendment guarantee that no person 'shall be compelled in any criminal case to be a witness against himself.'" (citation omitted)). *Compare* Fisher v. United States, 425 U.S. 391 (1976) (holding that compelling a taxpayer to produce documents made by her accountants is not testimonial in nature), *with* United States v. Doe, 465 U.S. 605 (1984) (recognizing that the act of producing documents created by the suspect or defendant may be privileged depending on the facts of the particular case).

[27] *See* Ullmann v. United States, 350 U.S. 422 (1956) (interpreting the intent of the privilege and its importance in constitutional jurisprudence); Hoffman v. United States, 341 U.S. 479, 486 (1951) (reiterating that the privilege must be liberally construed "in favor of the right it was intended to secure" (citing Counselman v. Hitchcock, 142 U.S. 547, 562 (1892))). *See also* United States v. Hubbell, 530 U.S. 27 (2000) (holding that the privilege is invoked through the testimony "inherent in the act of producing" documents); Andrew J. M. Bentz, *The Original Public Meaning of the Fifth Amendment and Pre-Miranda Silence*, 98 VA. L. REV. 897, 918 (2012) ("Unfortunately, there is no evidence of Madison's motivations for changing the typical phrasing of the right. He said nothing during his presentment of the amendments about the right against self-incrimination.").

[28] *See* cases cited *supra* note 27 (giving examples of cases in which the Supreme Court interpreted the intent of the privilege or implemented it). *See also* United States v. Kirschner, 823 F. Supp. 2d 665 (E.D. Mich. 2010) (ruling that a subpoena requiring defendant to disclose all device passwords violated the privilege).

[29] *See Incorporation Doctrine*, CORNELL UNIV. L. SCH., https://www.law.cornell.edu/wex/incorporation_doctrine (stating that the Fifth Amendment has been partially incorporated, with the right to an indictment by a grand jury not yet incorporated). Indeed,

in the nineteenth century the Supreme Court began expanding the scope of the privilege.[30]

Counselman v. Hitchcock ushered in the extension of the privilege to witnesses in criminal proceedings.[31] Prior to *Counselman*, the privilege generally applied only to criminal defendants.[32] A witness, not the defendant, at trial was at risk of incriminating herself while testifying as a witness during a separate proceeding.[33] Even if a witness testified on behalf of the prosecution, she could open herself up to prosecution through her possibly self-incriminating testimony.[34] In *Counselman*, the Court found that the privilege applied to both criminal defendants, as well

---

the privilege against self-incrimination did not become incorporated until 1964 in *Malloy v. Hogan*. *See* Malloy v. Hogan, 378 U.S. 1 (1964) (holding that the privilege against self-incrimination is incorporated by the Fourteenth Amendment and applies to the states). *See* Hon. Joseph R. Weisberger, *The Selective Incorporation Process and Judicial Activism*, 59 R.I. B.J., Mar.–Apr. 2011, at 13, 13–15 ("In *Twining v. New Jersey*, 211 U.S. 106 (1908) the Court held the Fifth Amendment privilege against self-incrimination was not binding upon the states. . . . *In Malloy v. Hogan*, 378 U.S. 1 (1964) the Fifth Amendment right against self-incrimination was incorporated."). *See also Malloy*, 378 U.S. at 6 ("We hold today that the Fifth Amendment's exception from compulsory self-incrimination is also protected by the Fourteenth Amendment against abridgment by the States.").

30 *See, e.g.*, Counselman v. Hitchcock, 142 U.S. 547, 586 (1892) (extending the privilege to cover witnesses and not just criminal defendants as the privilege had in the past).

31 *See id.* (holding that the privilege against self-incrimination extends to witnesses as well as criminal defendants). The Northern District of Illinois issued a subpoena requiring Counselman to appear in court as a witness. *Id*. at 548–49. Counselman appeared and refused to answer several questions asked of him by the court. *Id*. Upon his refusal, he was ordered to show cause for why he refused to answer. *Id*. at 549. The court found his responsive reasons insufficient, and he appeared again to answer more questions. *Id*. at 551–52. After refusing to answer more questions, he was found in contempt and held in custody by U.S. Marshal Hitchcock until he answered the questions. *Id*. at 552. He then challenged the contempt order. *Id*. at 562.

32 *See generally* STEVEN M. SALKY & PAUL B. HYNES, JR., THE PRIVILEGE OF SILENCE: FIFTH AMENDMENT PROTECTIONS AGAINST SELF-INCRIMINATION 3 (2014) (noting that after ratification, the courts initially understood the amendment to simply affirm the common-law protections afforded defendants against improper methods used for gaining confessions).

33 *See id.* (explaining that the privilege was originally only thought to affirm common-law principles that only defendants were protected from forced self-incrimination). *See also Counselman*, 142 U.S. at 563 (discussing how New York's very similar state constitution privilege was interpreted by New York courts to only protect criminal defendants).

34 *See Counselman*, 142 U.S. at 586 (providing that witnesses and criminal defendants are given total transactional immunity from future prosecution because of their testimony). Originally, *Counselman* required full "transactional" immunity, meaning that the witness or defendant in a criminal proceeding could not be the subject of future prosecution due to any part of her testimony. *See id*. (holding that witnesses and criminal defendants receive complete immunity from self-incriminating testimony); Amar & Lettow, *supra* note 26, at 858 (expounding how *Counselman* affected the level of immunity witnesses and defendants receive). However, full transactional immunity was later overturned in *Kastigar v. United States. See* Kastigar v. United States, 406 U.S. 441, 461–62 (1972).

as witnesses in a criminal proceeding.[35] Despite this extension, the Supreme Court did not create any kind of surefire way of applying the privilege to a set of facts.[36] That kind of analysis would not come along until near the end of the twentieth century.[37] Still, the Supreme Court continued to expand the scope of privilege.[38]

Blau v. United States reiterated that the privilege not only protected testimony that would itself support a conviction but also protected testimony that led to a "link in the chain of evidence needed" to support a conviction.[39] The Court used that case to elaborate on this doctrine.[40] *Blau* firmly laid out that the privilege protected both compelled responses that directly supported conviction and any response that was an evidentiary link that supported conviction.[41] During the twentieth century the Supreme Court not only provided more context as to what the privilege did and did not protect but also expounded on what it believed the privilege's intent was.[42]

---

35 *See Counselman*, 142 U.S. at 562–63 ("It is broadly contended . . . that a witness is not entitled to plead the privilege of silence, except in a criminal case against himself; but such is not the language of the constitution. Its provision is that no person shall be compelled in any criminal case to be a witness against himself.").

36 *See id*. at 586 (restricting the analysis to only whether the privilege extends to witnesses and not providing a test for how to apply the privilege to any set of facts).

37 *See* Fisher v. United States, 425 U.S. 391, 408 (1976) (providing a three-part test to determine whether the privilege applies to the disclosure the government seeks to compel).

38 *See* Blau v. United States, 340 U.S. 159, 161 (1950) (protecting responses that may not directly support a conviction but were parts of the chain of evidence that supported a conviction).

39 *See id*. (stating that responses that are part of the evidentiary chain that supports a conviction are also privileged). In *Blau*, the Supreme Court laid to rest the notion that only responses that directly incriminate or support a conviction are protected. *Id*. Now, any response that can be used to furnish a "link in the chain of evidence" is protected. *Id*. *See also* Hoffman v. United States, 341 U.S. 479, 485–86 (1951) (providing guidance on the intent and scope of the privilege).

40 *See Blau*, 340 U.S. at 161 ("Answers to the questions asked by the grand jury would have furnished a link in the chain of evidence needed in a prosecution . . . .").

41 *See id*. (explaining that any response that furnishes a "link in the chain of evidence" is protected by the privilege). *See also* Emspak v. United States, 349 U.S. 190 (1955) (reiterating the standard reached in *Blau* that responses that create a link in the chain of evidence supporting a conviction are protected).

42 *See, e.g.*, *Hoffman*, 341 U.S. at 485–86 (expounding what the intent and scope of the privilege is). *See also* Miranda v. Arizona, 384 U.S. 436, 459–61 (1966) (discussing the privilege's intent to be a preventative measure against government overreach and to preserve an accusatorial system of justice). While *Miranda* noted that the privilege's intent is to help secure an accusatorial, rather than inquisitorial, system of government, the two are not incompatible. *Id*.

Two examples of these decisions are *Hoffman v. United States* and *Ullmann v. United States*.[43] In *Hoffman*, the Supreme Court made note of the growing number of cases in front of it in which persons asserted the privilege during federal grand jury investigations.[44] It reiterated the important necessity that judges and prosecutors "be 'alert to repress'" abuses of the federal grand jury.[45] The Supreme Court noted that the Framers included the privilege because they believed that unhampered law enforcement sacrificed "other social objects of a free society."[46] The Court in *Ullmann* included a lengthy dialogue of the privilege's importance in our free society and even acknowledged the "far-reaching evil" of the Inquisition and Star Chamber the privilege was enacted to prevent.[47] It discussed the privilege's lengthy history and the idea that "it were better for an occasional crime to go unpunished than that the prosecution should be free to build up a criminal case . . . with the assistance of enforced disclosures by the accused."[48] *Ullmann* further

---

[43] *See Hoffman*, 341 U.S. at 485–86 (providing guidance on the liberal construction and strict enforcement of the privilege); Ullmann v. United States, 350 U.S. 422, 426–28 (1956) (giving background on the intent of the privilege when the Framers added it to the Constitution).

[44] *See Hoffman*, 341 U.S. at 485 (providing the factual background to the case). *Hoffman* was one of five cases in front of the Supreme Court at that time where defendants invoked the privilege during federal grand jury investigations. *Id*. The government issued a subpoena on Hoffman to appear before a grand jury and testify regarding several criminal charges. *Id*. at 481. He refused to answer several questions posed to him, and the government challenged his invocation of the privilege. *Id*. at 482. The court found in favor of the government and ordered Hoffman to appear again and answer, but he refused to do so. *Id*. The court found him in criminal contempt, and he appealed. *Id.* The Court of Appeals for the Third Circuit affirmed his conviction. *Hoffman*, 341 U.S. at 484. After the Third Circuit denied a rehearing, he appealed to the Supreme Court. *Id*. at 485.

[45] *Id*. at 485. This case arose during the time of McCarthyism, when Senator Joseph McCarthy began a relentless campaign to root out communism in the United States. *Joseph R. McCarthy*, HISTORY, http://www.history.com/topics/cold-war/joseph-mccarthy [https://perma.cc/B3CY-9542] (describing McCarthyism and how Senator McCarthy operated his campaign against communism). McCarthy used his power to launch investigations into citizens and encourage prosecutors to charge citizens suspected of communism. *Id*.

[46] Hoffman v. United States, 341 U.S. 479, 486 (1951). *Hoffman* is considered the defining case for incrimination. *See* Lisa Tarallo, *The Fifth Amendment Privilege Against Self-Incrimination: The Time Has Come for the United States Supreme Court to End Its Silence on the Rationale Behind the Contemporary Application of the Privilege*, 27 NEW ENG. L. REV. 137, 146 (1992) (stating that *Hoffman* provides the leading definition for self-incriminating evidence).

[47] *Ullmann*, 350 U.S. at 428. The Star Chamber and Inquisition had a history of oppression and abuse of power that influenced the decision to include the privilege against self-incrimination in the Constitution. *Id*.

[48] *Id*. at 427. *See also* MARK BERGER, TAKING THE FIFTH 9–13 (2006) (outlining a brief history of the Star Chamber and the resistance to its methods by various groups in England during its use); SALKY & HYNES, JR., *supra* note 32, at 2 (expounding a short history of the Star Chamber and its use of the *oath ex officio*).

warned against approaching the privilege in a hostile manner because doing so did not properly honor its creators.[49] Perhaps the most helpful development in jurisprudence regarding the privilege came in the Supreme Court's decision in *Fisher v. United States* in 1976.[50]

In *Fisher*, the Supreme Court created a three-part element test, still in place today, stating that the privilege "applies only when the accused is compelled to make a testimonial communication that is incriminating."[51] Broken into the three parts, this new test requires that a person: (1) be compelled by the government; (2) to give testimony; (3) that is incriminating.[52] The test seems simple enough, but the testimonial element causes problems when a new issue arises that tiptoes the testimonial line.[53] Such a case arises with the compulsion of biometrics to unlock a device, which challenges precedent holdings that compulsion of biometric data is not testimonial.[54] But first, before moving to a

---

[49] *See* Ullmann v. United States, 350 U.S. 422, 426–27 (stating that approaching the privilege in a hostile manner did not honor the "patriots who sponsored the Bill of Rights as a condition to acceptance of the Constitution by the ratifying states"). *See also* SALKY & HYNES, JR., *supra* note 32, at 4 (discussing the *Ullmann* case and its impact).

[50] *See* Fisher v. United States, 425 U.S. 391, 408 (1976) (stating the rule for when the Fifth Amendment privilege against self-incrimination applies). *See also* Allen & Mace, *supra* note 26, at 246 (describing the elements of the privilege established in *Fisher*).

[51] *Fisher*, 425 U.S. at 408. *See also* Allen & Mace, *supra* note 26, at 246 (referring to the approach taken in *Fisher* as the "new textual analytical approach" (quoting Lance Cole, *The Fifth Amendment and Compelled Production of Personal Documents After* United States v. Hubbell—*New Protection for Private Papers?*, 29 AM. J. CRIM. L. 123, 142–43 (2002))). While *Fisher* is the first example of the Supreme Court using the "new textual analytical approach," *Schmerber* is the first example of the Court introducing the testimonial requirement into self-incrimination jurisprudence. Allen & Mace, *supra* note 26. *See also* Michael S. Pardo, *Self-Incrimination and the Epistemology of Testimony*, 30 CARDOZO L. REV. 1023 (2008) (stating that *Schmerber* saw the introduction of the testimonial element into self-incrimination jurisprudence by the Supreme Court).

[52] *See Fisher*, 425 U.S. at 408 (stating that a claim of the privilege requires a person to be compelled by the government to give testimony that is incriminating). *See also* Allen & Mace, *supra* note 26 (explaining that the privilege requires government compulsion, testimony, and incriminating evidence).

[53] *See* Erin M. Sales, Note, *The "Biometric Revolution": An Erosion of the Fifth Amendment Privilege to be Free From Self-Incrimination*, 69 U. MIAMI L. REV. 193, 213 (2014) (providing background on the second element of the privilege against self-incrimination). *See also* Allen & Mace, *supra* note 26 (discussing the Supreme Court's lack of clear explanation as to what constitutes testimony); Pardo, *supra* note 51 (analyzing the epistemology of the testimony in self-incrimination).

[54] *See* Jack Linshi, *Why the Constitution Can Protect Passwords But Not Fingerprint Scans*, TIME (Nov. 6, 2014), (exploring why fingerprint scans are not protected in the face of the introduction of Touch ID). *See also* Schmerber v. California, 384 U.S. 757, 763–65 (1966) (reasoning that providing a biometric, such as a blood sample, does not fall under the protection of the privilege because it is not testimonial). *See generally* Sales, *supra* note 53 (explaining how the rise of biometrics is challenging the traditional jurisprudence for self-incrimination). For a recent example where a court held that compulsion of biometric data

background of examples the privilege traditionally does not protect, encryption, and how it works, must be explained.[55]

B. Encryption Explained

Prior to covering cases that deal with encryption, one must know how traditional encryption and biometric encryption work.[56] Encryption began long before the advent of computers, but the focus here is on electronic encryption.[57] At its heart, encryption is a simple idea, but in technical terms it is a much more complex practice.[58] If a person peered into an encrypted computer without it being decrypted, everything on it would be an undecipherable mess of numbers, letters, and symbols.[59] This keeps the information on the computer safe from those who do not have the key to decrypt the information.[60]

---

to unlock a device violated the privilege against self-incrimination, see *In the Matter of the Search of a Residence in Oakland, Cal.*, No. 4-19-70053, 2019 WL 176937, at *2–4 (N.D. Cal. Jan. 10, 2019) (holding that compulsion of biometric data to unlock a device violated the Fifth Amendment privilege against self-incrimination).

55 *See infra* Part II.B.

56 *See infra* notes 58–70. *See also infra* Part II.C (covering cases in which courts began to hold that compulsion of passwords to unlock encryption violates the privilege against self-incrimination).

57 *See* Jeff Tyson, *How Encryption Works*, HOW STUFF WORKS, https://computer.howstuffworks.com/encryption1.htm [https://perma.cc/HDD7-2YSM] (canvassing the history of encryption and its basis on the science of cryptography). Encryption is based on cryptography. *Id*. Some of the first examples of cryptography came from the writing of Plutarch, who stated that Spartan generals used a device called a scytale to jumble orders on the battlefield. *Id*. The scytale was a small cylinder made of wood that the general would wrap parchment around and write the message along the length. *Id*. When the parchment was not wrapped around the cylinder it appeared as nonsense. *Id*. The receiving general would use his own scytale of similar size to wrap the parchment around, which then revealed the information on the parchment. *Id*.

58 *See id.* (explaining the technical details behind computer encryption). Encryption generally takes the form of symmetric key encryption or public-key encryption. *Id*. *See also* Whitson Gordon, *A Beginner's Guide to Encryption: What It Is and How to Set It Up*, LIFEHACKER (Jan. 27, 2014), https://lifehacker.com/a-beginners-guide-to-encryption-what-it-is-and-how-to-1508196946 [https://perma.cc/5QDL-D8PD] (providing more information on how encryption works); Sales, *supra* note 53, at 208–10 (giving a brief explanation of how encryption works on computers and other devices).

59 *See* Tyson, *supra* note 57 (discussing how encryption scrambles the information on the device so that it is unreadable without the decryption key). *See also* Gordon, *supra* note 58 (exploring how encryption jumbles the information on the device); Sales, *supra* note 53, at 208–10 (analyzing briefly what encryption is and how it works on electronic devices).

60 *See* Tyson, *supra* note 57 (highlighting the fact that the decryption key is needed to unscramble the information on the device). *See also* Sales, *supra* note 53, at 208–10 (explaining how traditional encryption works on electronic devices); Efren Lemus, *When Fingerprints Are Key: Reinstating Privacy to the Privilege Against Self-Incrimination in Light of Fingerprint Encryption in Smartphones*, 70 SMU L. REV. 533, 541–42 (2017) (expounding how encryption works in devices).

In theory, the only way to decrypt the device and descramble its data is to have the decryption key.[61] The decryption key authenticates that the person accessing the information is the trusted user and decrypts the information.[62] This key can be a passcode, such as a series of letters, numbers, and signals.[63] The decryption key can also be a unique biometric feature, such as a fingerprint.[64] While it is possible to hack and decrypt the information, doing so is usually difficult and time-consuming.[65] Biometric encryption is essentially the same as traditional encryption with the exception of what operates as the decryption key.[66]

With biometric encryption, a unique piece of biometric datum must be provided, which then acts as the alternative for the alphanumeric password.[67] The software then gives that unique biometric datum, say a

---

61 *See* Tyson, *supra* note 57 (explaining that the only efficient way to decrypt a device is to use the decryption key). *See also* Lemus, *supra* note 60, at 541–42 (providing that the encryption key "is required to fully decrypt an encrypted device"); Sales, *supra* note 53, at 208 (stating that the text on a device "essentially becomes unreadable, appearing as random letters, numbers, and symbols, unless the correct password is entered to unscramble the texts").

62 *See* Tyson, *supra* note 57 (pointing out that the decryption key authenticates the user as the authorized user of the device that is being decrypted). *See also* Lemus, *supra* note 60, at 542 ("Passwords and other verification and authentication tools, when entered into a device, trigger the encryption key and grant access to the data contained in the device.").

63 *See* Tyson, *supra* note 57 (identifying several of the forms that a decryption key can take, including passwords, pass cards, and digital signatures).

64 *See* Roger Cheng, *The Perfect Password? You've Put Your Finger on It*, CNET (Aug. 31, 2015), https://lifehacker.com/a-beginners-guide-to-encryption-what-it-is-and-how-to-1508196946 [https://perma.cc/LK7D-3UR2] (discussing the increased security in using a fingerprint as the password to a device instead of a traditional password). *See* Sales, *supra* note 53, at 215 ("Various biometric authentication methods currently exist. Some of the more prevalent ones include fingerprint analysis, facial recognition, iris scanning, voice recognition, and DNA analysis.").

65 *See* Tyson, *supra* note 57 (expounding how encryption is difficult and time-consuming for a hacker to attempt to break through without having the decryption key). The new standard for encryption strength is the Advanced Encryption Standard (AES). *Id*. AES uses 128-, 192-, and 256-bit decryption keys. *Id*. For example, a 128-bit encryption key can have more than three hundred decillion possible combinations. *Id*. Finding the correct combination "would be like trying to find one particular grain of sand in the Sahara Desert." *Id*.

66 *See* Tyson, *supra* note 57 (explaining that biometrics can be used to unlock normal encryption just like a typical decryption key can). *See also* Ann Cavoukian & Alex Stoianov, *Biometric Encryption: A Positive-Sum Technology That Achieves Strong Authentication, Security AND Privacy*, COMBINED ARMS CTR. (Mar. 2007), http://usacac.army.mil/cac2/cew/repository/papers/Biometric_Encryption.pdf [https://perma.cc/LF43-N9C3] (giving a further explanation of how biometric encryption works and how it relates to traditional encryption).

67 *See* Tyson, *supra* note 57 (examining several of the types of biometric decryption that act as substitutes for traditional decryption keys). *See also* Cavoukian & Stoianov, *supra* note 66, at 16 ("Biometric encryption is a process that securely binds a PIN or a cryptographic key to

fingerprint, a unique code that unlocks the device and information.[68] When the biometric datum is entered, the software translates the datum into the unique code and enters it, unlocking the device.[69] Biometric encryption has been around for some time but has seen a recent increase in popularity, especially in mobile devices and laptops.[70] Its increasing popularity creates trouble when considering biometric decryption's unprotected status.[71]

C. Examples of Compulsion of Biometrics' Unprotected Status

Traditionally, the Supreme Court and lower courts held that compulsion of biometrics did not violate the privilege against self-incrimination.[72] Part II.C provides several examples of cases in which the Supreme Court and lower courts ruled against extending the privilege to protect compulsion of biometrics.[73]

In the latter half of the twentieth century, the Supreme Court faced the issue of compelled production of biometrics in *Schmerber v. California*.[74]

---

a biometric, so that neither the key nor the biometric can be retrieved from the store template.").

[68] *See* Tyson, *supra* note 57 (laying out how biometric decryption keys work in a similar fashion to traditional decryption keys); Cavoukian & Stoianov, *supra* note 66, at 16 ("The digital key . . . is randomly generated on enrolment, so that the user (or anybody else) does not even know it.").

[69] *See* Soutar et al., *Biometric Encryption*, BIOSCRYPT INC., http://www.cse.lehigh.edu/prr/Biometrics/Archive/Papers/BiometricEncryption.pdf [https://perma.cc/ZG4D-7CHK] (expounding how using the biometric unlocks access to the key that will then decrypt the information on the device).

[70] *See supra* note 11 (giving examples of new devices that use biometric encryption as the primary method for unlocking the device).

[71] *See infra* Part II.C.

[72] *See* cases cited *infra* note 73 (providing background on cases such as *Schmerber*, *Dionisio*, and *Wade*, which all held that compulsion of a person's biometrics to unlock that person's device does not violate the privilege against self-incrimination).

[73] *See* Schmerber v. California, 384 U.S. 757, 765 (1966) (reasoning that providing a blood sample is not testimonial and therefore not protected by the privilege). *See also* United States v. Dionisio, 410 U.S. 1, 7–8 (1973) (holding that compulsion of a voice exemplar does not violate the privilege against self-incrimination); United States v. Wade, 388 U.S. 218, 223 (1967) (ruling that compelling a defendant to stand in a lineup is only used for identification and therefore not a violation of the privilege).

[74] *See Schmerber*, 384 U.S. at 758 (providing the facts of the case where the defendant was forced to submit to a blood test to determine intoxication). In highlighting *Schmerber*, this Note focuses on the history of using biometric data and the issue of whether compelling a blood sample, as a form of biometrics, violates the Fifth Amendment privilege against self-incrimination. For case law addressing whether compelling a blood sample violates Fourth Amendment unlawful search and seizure jurisprudence, see the Court's reasoning in *McNeely*. Missouri v. McNeely, 569 U.S. 141 (2013) (distinguishing *Schmerber* for having exigent circumstances not present in the instant case and finding a Fourth Amendment violation for compelling a blood sample without a warrant).

Schmerber, the defendant, was convicted in the Los Angeles Municipal Court for driving under the influence of alcohol.[75] His conviction rested, at least in part, on blood sample evidence taken against his will at the hospital at the direction of a police officer.[76] The blood sample showed that Schmerber was indeed intoxicated.[77] The municipal court allowed the sample into evidence and found him guilty.[78] Schmerber then challenged the admission of the evidence on the grounds that it violated his privilege against self-incrimination.[79]

On appeal, the Supreme Court decided that Schmerber's forced blood sample did not violate the privilege.[80] The Supreme Court reasoned that nothing in the compelled act of providing the blood sample was testimonial because it was not communicative in nature.[81] The Supreme Court declared it to be physical evidence that was not protected by the privilege.[82] *Schmerber* was the first case in which the Supreme Court laid out the testimonial element, which remains troublesome.[83]

United States. v. Wade provides another example.[84] In *Wade*, the government forced the defendant in a bank robbery case to stand in a lineup with strips of tape covering his face just like the suspected robber had done.[85] Two employees that were present when Wade robbed the

---

75 *See Schmerber*, 384 U.S. at 758. Schmerber was in an accident while driving and was arrested at the hospital where he was receiving treatment for his injuries. *Id*. The arresting officer directed a physician at the hospital to take blood from Schmerber, against Schmerber's will, for blood-alcohol testing. *Id*. The blood analysis showed that Schmerber was intoxicated at the time of the accident. *Id*. at 759.

76 *See id*.

77 *See id*. at 758–59.

78 *See id*. at 759. *See also* Paul A. Clark, *Do Warrantless Breathalyzer Tests Violate the Fourth Amendment?*, 44 N.M. L. REV. 89, 90–91 (2014) (providing a brief recitation of the facts of the *Schmerber* case).

79 *See* Schmerber v. California, 384 U.S. 757, 758–59 (1966).

80 *See id.* at 765. *See also* Sales, *supra* note 53, at 200 (discussing how the Supreme Court "determined that a blood sample taken from the petitioner was not 'compulsion'").

81 *See Schmerber*, 384 U.S. at 761–65 (reasoning that the compelled act of providing a blood sample is not testimonial). *See* Sales, *supra* note 53, at 199 (stating that the Supreme Court believed that the evidence was not communicative in nature).

82 *See Schmerber*, 384 U.S. at 761–64. *See also* SALKY & HYNES, JR., *supra* note 32, at 286–87 (providing further details of the case, the Court's reasoning, and its possible future implications).

83 *See Schmerber*, 384 U.S. at 763–65.

84 *See* United States v. Wade, 388 U.S. 218, 221 (1967) ("We have only recently reaffirmed that the privilege 'protects an accused only from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature . . . .'" (quoting Schmerber v. California, 384 U.S. 757, 761 (1966))). *See also* Sales, *supra* note 53, at 200 (covering the facts and reasoning of the Court in *Wade*).

85 *See Wade*, 388 U.S. at 220 (providing the background facts of the case, including the lineup the government forced the defendant to stand in with strips of tape over his face). *See also* Sales, *supra* note 53, at 200 ("In Wade, the Supreme Court considered a situation in which

bank pointed him out in the lineup as well as at trial, and Wade was convicted.[86] Wade challenged the compulsion to stand in a lineup and contended that it violated his privilege against self-incrimination.[87]

Again, the Supreme Court relied on the testimonial element of the privilege.[88] It held that compulsion to stand in a lineup did not violate the privilege because it did not involve testimony.[89] It reasoned that displaying oneself in a lineup does not communicate anything and, therefore, is not testimonial.[90] The Supreme Court cited to *Schmerber* and followed similar analysis: merely providing biometrics does not communicate anything and is used only for identification.[91]

The Court continued this analysis in *United States v. Dionisio* in 1973, where the district court held the defendant in contempt for refusing to provide a voice exemplar in a federal grand jury proceeding.[92] The defendant challenged the contempt order, alleging that providing the exemplar violated his privilege against self-incrimination.[93] The Court of Appeals for the Seventh Circuit upheld the district court's holding on the

---

the government compelled the petitioner to stand in a lineup wearing strips of tape similar to those worn by a bank robber and to speak the words uttered by the bank robber.").

86 *See Wade*, 388 U.S. at 220 (expounding that a government agent "arranged to have the two bank employees observe a lineup made up of Wade and five or six other prisoners and conducted in a courtroom of the local county courthouse. . . . Both bank employees identified Wade in the lineup as the bank robber.").

87 *See id.* (stating that Wade's counsel sought to strike "the bank officials' courtroom identifications on the ground that conduct of the lineup, without notice to and in the absence of his appointed counsel, violated his Fifth Amendment privilege against self-incrimination . . .").

88 *See id.* at 222 ("We have no doubt that compelling the accused merely to exhibit his person for observation by a prosecution witness prior to trial involves no compulsion of the accused to give evidence having testimonial significance."). *See also* Sales, *supra* note 53, at 200 ("A year after Schmerber, the Supreme Court further restricted the meaning of 'testimonial' in United States v. Wade.").

89 See United States v. Wade, 388 U.S. 218, 222 (1967) ("It is compulsion of the accused to exhibit his physical characteristics, not compulsion to disclose any knowledge he might have."). *See also* Sales, *supra* note 53, at 200 ("Wade further clarified that even compelled speech is not 'testimonial' in nature if the speech is to be used solely as an identifying physical characteristic and not to admit guilt.").

90 *See Wade*, 388 U.S. at 222 ("It is no different from compelling Schmerber to provide a blood sample or Holt to wear the blouse, and, as in those instances, is not within the cover of the privilege.").

91 *See id.* at 222–23.

92 *See* United States v. Dionisio, 410 U.S. 1, 3–4 (1973) (providing the facts establishing the reason for Dionisio's appeal). The district court held a hearing before trial to hear Dionisio's challenge to the constitutionality of the subpoena requiring a voice exemplar. *Id*. The district court found that the voice exemplar was used for identification similar to fingerprints and handwriting exemplars. *Id*. The district judge ordered Dionisio to submit his exemplar, and when Dionisio refused, the judge found Dionisio in contempt until he provided the voice exemplar or for no longer than eighteen months. *Id*. Dionisio appealed. *Id*.

93 *See id.* at 4–5 (canvassing the facts of the case and its procedural history).

privilege against self-incrimination issue and reversed on other grounds, and the Supreme Court ultimately upheld the ruling on the Fifth Amendment issue.[94] Following a similar line as it previously had, the Court ruled that compulsion of a voice exemplar did not violate the privilege.[95]

The Supreme Court acknowledged that one's voice is a means of communication; however, in this case it focused on the substance and use of the biometric at issue.[96] The Supreme Court reasoned that the voice exemplar merely provided an identifiable physical characteristic.[97] The defendant did not speak to his guilt or innocence in the exemplar but only provided an example of his voice to be used for identification, and the testimonial content within was not the intent of the exemplar.[98] Despite the Supreme Court's unwillingness to extend the privilege to biometrics in the past, it has proven willing to extend the privilege and other privacy interests in other areas.[99]

D. Courts' Willingness to Expand Individual Privacy Interests

Since the inception of the privilege, there are several instances where the Supreme Court and lower courts proved willing to extend the

---

94 *See Dionisio*, 410 U.S. at 4–8 (upholding the Court of Appeals for the Seventh Circuit's decision regarding the privilege against self-incrimination issue). The court of appeals affirmed the district court's decision on the Fifth Amendment issue but reversed the district court's decision regarding a Fourth Amendment issue in the case. *Id*. The Supreme Court granted certiorari in order to resolve a circuit split between the Seventh and Second Circuits on the Fourth Amendment issue. *Id*. at 5. The Supreme Court ultimately upheld the Fifth Amendment decision by the court of appeals and reversed the decision on the Fourth Amendment issue. *Id*. at 7.

95 *See id.* at 4–7 (following the same line of reasoning as it had in *Schmerber*, the Supreme Court found that requiring a defendant to provide a voice exemplar does not violate the Fifth Amendment privilege against self-incrimination). *See also* Floralynn Einesman, *Vampires Among Us—Does a Grand Jury Subpoena for Blood Violate the Fourth Amendment?*, 22 AM. J. CRIM. L. 327, 345 (1995) (providing the facts of the *Dionisio* case); D.H. Kaye, *The Constitutionality of DNA Sampling on Arrest*, 10 CORNELL J.L. & PUB. POL'Y 455, 474 (2001) (expounding further facts of the *Dionisio* case).

96 *See Dionisio*, 410 U.S. at 6–7 (acknowledging that one's voice is a means of communication but that "[t]he voice recordings were to be used solely to measure the physical properties of the witnesses' voices, not for the testimonial or communicative content of what was to be said"). *See also* Einesman, *supra* note 95, at 345 (covering the background of the *Dionisio* case).

97 *See Dionisio*, 410 U.S. at 7 (ruling that the voice exemplars were only to be used for identification purposes and not for the testimonial or communicative content within).

98 *See id.*

99 *See infra* Part II.D (providing cases in which the Supreme Court and lower courts have extended the privilege against self-incrimination and other privacy interests in the face of government overreach with new technologies).

protection of the privilege or the Fourth Amendment to new issues.[100] While the Supreme Court declined in *Fisher* and subsequent cases to hold that the contents of documents are protected by the privilege, it has held that the act of producing documents is.[101] Subsequent cases have reiterated this belief, including *United States v. Doe*, *In re Grand Jury Subpoena Duces Tecum Dated May 9, 1990*, and *United States v. Hubbell*.[102] In each case, the courts reiterated that even if the contents of the documents are not protected, the act of producing them is testimonial and therefore protected by the privilege.[103]

Of importance, lower courts have held that the privilege protects against government compulsion to provide a password to a device.[104] Providing a traditional password, according to those courts, contains a testimonial aspect.[105] Whether the password is written or spoken, there is a communicative nature to it, and by providing the password defendants are essentially testifying that they own or have access to the incriminating

---

100 *See, e.g.*, United States v. Doe, 465 U.S. 605 (1984) (holding that, while the contents of documents may not be privileged under the Fifth Amendment, the act of producing them can be testimonial and therefore protected by the privilege against self-incrimination).

101 *See* Fisher v. United States, 425 U.S. 391, 414 (1976) (declining to broach the question of whether the contents of documents are protected by the privilege against self-incrimination). *See also Doe*, 465 U.S. at 612–13 ("Although the contents of a document may not be privileged, the act of producing the document may be." (citation omitted)).

102 *See Doe*, 465 U.S. at 612–13 (holding that the act of producing a document itself may be testimonial and therefore protected by the privilege); *In re* Grand Jury Subpoena Duces Tecum Dated May 9, 1990, 741 F. Supp. 1059, 1072 (S.D.N.Y. 1990) (declaring that the privilege still protects the production of private documents in response to government compulsion); United States v. Hubbell, 530 U.S. 27, 35–37 (2000) (reiterating that the act of producing personal documents in response to government compulsion can be testimonial). *See also* In the Matter of the Search of a Residence in Oakland, Cal., No. 4-19-70053, 2019 WL 176937, at *2–4 (N.D. Cal. Jan. 10, 2019) (reinforcing that it is accepted that producing documents is testimonial).

103 *See* cases cited *supra* note 102 (giving examples of several cases in which courts reiterated that the act of producing documents in response to government compulsion can be protected by the privilege against self-incrimination).

104 *See* United States v. Kirschner, 823 F. Supp. 2d 665 (E.D. Mich. 2010) (holding that the government cannot compel a person to provide her decryption password because doing so violates the privilege against self-incrimination); *In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *2 (D. Vt. Feb. 19, 2009) (ruling that compulsion to provide a password violates the privilege, except in cases where the government can prove the foregone conclusion doctrine); *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012) (deciding that compulsion to provide a password to decrypt an encrypted device violated the privilege against self-incrimination); *Search of a Residence*, 2019 WL 176937, at *2–3 (reaffirming that compelled production of a traditional alphanumeric password violates the privilege against self-incrimination).

105 *See* cases cited *supra* note 104 (summarizing the holdings of several cases in which courts decided that compulsion of a password to unlock a device violates the privilege against self-incrimination).

information.[106] However, the foregone conclusion doctrine is an important exclusion to keep in mind when talking about the protection of compelled passwords.[107]

These cases provide only several examples of courts' willingness to extend the Fifth Amendment privilege.[108] Some important cases have also extended Fourth Amendment protections. *Kyllo v. United States* and *Riley v. California* extended Fourth Amendment protections to new technologies that were becoming increasingly popular and sophisticated.[109] While

---

[106] *See, e.g.*, *Kirschner*, 823 F. Supp. 2d at 668–69 (holding that providing a password in response to subpoena communicates factual knowledge and is therefore testimonial).

[107] *See Boucher*, 2009 WL 424718, at *3–4 (explaining the foregone conclusion doctrine and how it applies to encryption). The foregone conclusion doctrine is an important exception to the privilege against self-incrimination. *See id.* Generally, the foregone conclusion doctrine establishes that a witness's act of production may be protected by the privilege unless the government can show with reasonable particularity that: it has knowledge of the existence, possession, and authenticity of the testimony, usually documents, it seeks; the information is a foregone conclusion; and forcing the witness to testify about it will not cause harm. *See* Fisher v. United States, 425 U.S. 391, 411 (1976) (establishing the foregone conclusion doctrine). *See also* Allen & Mace, *supra* note 26, at 279–80 (covering the establishment of the foregone conclusion doctrine); *Search of a Residence*, 2019 WL 176937, at *4–5 (applying the foregone conclusion doctrine to a case in which data on a mobile device was sought). However, there is some split in authority regarding how to apply this doctrine to files on devices. *Compare Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d at 1348–49 (finding that the government must show that it knows with reasonable particularity that specific files exist in some specified location and that the file is owned or controlled by the witness or defendant), *with* Commonwealth v. Gelfgatt, 11 N.E.3d 605, 614–15 (Mass. 2014) (holding that the government must only show that the witness or defendant has control over the device containing possible evidence, not knowledge of specific files). The Eleventh Circuit adopted a more stringent standard requiring that the government show that it has knowledge of specific files on a device owned or controlled by the suspect. *Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d at 1347–49. Massachusetts, however, adopted a more lenient standard allowing the government to show merely that it knows with reasonable particularity that the suspect owns or controls the device containing files that may be incriminating. *Gelfgatt*, 11 N.E.2d at 614–15.

[108] *See* cases cited *supra* note 104 (giving several examples of cases in which courts held that compulsion to provide a password to decrypt an encrypted computer violated the privilege against self-incrimination).

[109] *See* Kyllo v. United States, 533 U.S. 27 (2001) (ruling that the police cannot use a thermal imaging camera to scan a suspect's house for heat signatures without a warrant because it constituted a search). In *Kyllo*, the police used a thermal imaging camera to scan the defendant's home and noticed a large heat source in the attic of the home. *Id*. at 30. The police used this information and other evidence to obtain a search warrant, and a subsequent search revealed that the defendant was growing marijuana in his home. *Id*. The defendant moved to suppress the evidence from the thermal scan but was unsuccessful. *Id*. The Court of Appeals for the Ninth Circuit remanded for a hearing on the intrusiveness of the scan, and the district court found it to be non-intrusive. *Id*. The court of appeals reversed, but that opinion was withdrawn, and a panel affirmed. *Id*. The Supreme Court granted certiorari and held that the use of thermal imaging constituted a search of the home because thermal imaging gathered evidence that could not otherwise be found without entering the home. *Id*. at 40. The Supreme Court noted the advance of technology and its effect on individual

these are Fourth Amendment issues, they involve new technologies clashing with old law, and both the Fourth and Fifth Amendments involve individual privacy rights and government intrusion.[110]

E. Recent Cases Ruling on Compulsion of Biometrics to Unlock a Device

Little litigation exists that addresses the issue of whether compulsion of a person's biometrics to unlock that person's device is protected by the privilege.[111] Two state court decisions ruled against extending the privilege to protect compulsion of biometrics to unlock a person's device.[112] *Commonwealth v. Baust* from Virginia and *State v. Diamond* from the Minnesota Court of Appeals both ruled against extending the privilege.[113] In both cases, authorities in each state sought to force the defendant to unlock his phone via his fingerprint.[114] Similarly, the courts used the same line of reasoning to support their declination.[115] Each court reasoned that each defendant would not be forced to disclose the contents of his mind.[116] Providing the fingerprints would not require the defendants to communicate any knowledge or assert any fact.[117] However, the Northern District of Illinois took a different approach and ruled in favor of extending the privilege.[118]

---

privacy. *Id*. at 33–34. *See also* Riley v. California, 134 S. Ct. 2473 (2014) (deciding that, due to the modern pervasiveness and amount of personal information contained on cell phones, police must obtain a warrant before searching cell phones at a traffic stop); Carpenter v. United States, 138 S. Ct. 2206, 2216–22 (2018) (finding that law enforcement must obtain a warrant prior to accessing an individual's cell phone location data).

110 *See* cases cited *supra* notes 104 & 109 (canvasing cases in which courts expanded privacy rights under both the Fifth Amendment privilege against self-incrimination and the Fourth Amendment protection from unreasonable searches and seizures in the face of new technologies).

111 *See* cases cited *infra* notes 112 & 118 (providing the few cases that have ruled on whether compulsion of biometric data to unlock a person's device violates the Fifth Amendment privilege against self-incrimination).

112 *See* Commonwealth v. Baust, No. CR14-1439, 2014 WL 10355635, at *4 (Va. Cir. Ct. Oct. 28, 2014) (holding that compelling a defendant to provide a fingerprint to unlock a device does not implicate his privilege against self-incrimination); State v. Diamond, 890 N.W.2d 143, 150–51 (Minn. Ct. App. 2017) (deciding that compelling a defendant to provide a fingerprint to unlock a cell phone does not violate the privilege against self-incrimination).

113 *See* cases cited *supra* note 112 (highlighting two state cases where the courts declined to extend the privilege to protect providing biometrics to unlock a device).

114 *See* cases cited *supra* note 112.

115 *See* cases cited *supra* note 112.

116 *See, e.g.*, *Baust*, 2014 WL 10355635 at *3–4 (reasoning that providing a fingerprint did not require the defendant to communicate the contents of his mind).

117 *See id*. (ruling that providing a fingerprint does not communicate any kind of fact or knowledge).

118 *See In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073–74 (N.D. Ill. 2017) (deciding that providing a fingerprint to unlock a device in response to a subpoena is

In re Application for a Search Warrant found that providing biometrics to unlock a device is testimonial and, therefore, protected by the privilege.[119] The federal court there reasoned that by providing the biometric datum, the defendant is communicating that she controls or owns the device and the information within.[120] She is not just providing the biometric information for identification purposes.[121] The court found the communication of knowledge of ownership to be sufficiently testimonial to enter the territory of the privilege.[122] Therefore, the court ruled that the government cannot compel a person to provide biometric data to unlock that person's devices because doing so is testimonial.[123]

III. ANALYSIS

Part III analyzes important jurisprudence surrounding the Fifth Amendment privilege to establish the argument for why compulsion of biometrics for decrypting devices should be protected by the Fifth Amendment.[124] First, Part III.A discusses the intent of the Fifth Amendment privilege.[125] Second, Part III.B closely scrutinizes cases in which the court in question did not extend the privilege's protection.[126] Third, Part III.C provides examples of the judiciary's willingness to expand privacy interests, particularly the Fifth and Fourth Amendments in relation to new technologies.[127] Fourth, Part III.D reaches the main substance of this Note: case law that held compulsion of biometrics to

---

protected by the privilege against self-incrimination). During the final stages of publication of this Note, a new decision from the Northern District of California followed the example set by *Application for a Search Warrant*. *See* In the Matter of the Search of a Residence in Oakland, Cal., No. 4-19-70053, 2019 WL 176937, at *2–5 (N.D. Cal. Jan. 10, 2019) (holding that providing biometric data to unlock a device is testimonial).

119 *See Application for a Search Warrant*, 236 F. Supp. 3d at 1073–74.

120 *See id*. *See also Search of a Residence*, 2019 WL 176937, at *3 (stating that providing biometric data to unlock a device asserts the fact that the provider has some level of control over the device).

121 *See Application for a Search Warrant*, 236 F. Supp. 3d at 1073–74.

122 *See id*.

123 *See id*. at 1074 (ruling that the government cannot force a person to provide biometrics to unlock a device without first proving the foregone conclusion). *See also Search of a Residence*, 2019 WL 176937, at *2–5 (finding that compulsion to provide biometric data to unlock a device violates the privilege against self-incrimination).

124 *See* U.S. CONST. amend V. While this Note focuses on the Fifth Amendment privilege, it is important to take notice of the Fourth Amendment protection. The Fourth Amendment ties into the privacy concern covered by the privilege and can bolster the argument for extending the privilege to compulsion of biometrics to decrypt devices. *See* U.S. CONST. amend IV.

125 *See infra* Part III.A.

126 *See infra* Part III.B.

127 *See infra* Part III.C.

unlock a device is not protected by the privilege and the lone case that ruled in favor of extending the privilege to the compulsion of biometrics to decrypt devices.[128]

A. The Fifth Amendment Privilege's Intent

Part III.A analyzes two Supreme Court cases that have touched upon the intent and scope of the Fifth Amendment privilege.[129] These cases help establish a foundation for individual privacy interests that make the argument for extending the privilege more compelling.[130] Starting with *Hoffman v. United States*, Part III.A moves forward in time to cover *Ullmann v. United States*.[131] After an analysis of each case, a synthesized intent of the privilege will be put forth as the framework upon which to build the argument in favor of extending the privilege.[132]

Beginning with *Hoffman*, the framework for the argument to extend the privilege to cover compulsion of biometrics for unlocking devices takes shape.[133] The Court places high emphasis on the import of this privilege.[134] Specifically, that the privilege protects the "social objects of a free society" from unhindered intrusion by the government.[135] This shows that the protection from self-incrimination outweighs the government's

---

128 *See infra* Part III.D.

129 *See* cases cited *infra* notes 133 & 143 (discussing two cases that expound upon the intent and scope of the Fifth Amendment privilege against self-incrimination).

130 *See* cases cited *infra* notes 133 & 143.

131 While these cases are the primary focus of Part III.A, each of these cases relies on past Supreme Court decisions to reach its interpretation of the privilege's intent. *See, e.g.*, Counselman v. Hitchcock, 142 U.S. 547, 564 (1892) (expounding the intent of the privilege and how it must be construed).

132 Assuredly, many more cases exist upon which to build a more detailed analysis and synthesis. However, that is not the focus of this Note. These two cases provide the important takeaways regarding the approach to take when looking at a Fifth Amendment privilege issue for the purpose of this Note. *See, e.g.*, United States v. Balsys, 524 U.S. 666 (1998) (elaborating on the intent and scope of the privilege).

133 *See* Hoffman v. United States, 341 U.S. 479, 486 (1951) (analyzing the importance the privilege holds, as well as the intent and scope of it). In *Hoffman*, the Court faced several cases in which individuals asserted the privilege in federal grand jury investigations. *Id*. at 485. Hoffman was convicted of criminal contempt after refusing to answer questions that he believed may result in criminal charges. *Id*. at 482. The Court also noted the number of cases being handled in lower courts and decided it was time to reinforce "the continuing necessity that prosecutors and courts alike" be alert to abuses of that investigatory power. *Id*. at 485.

134 *See id*. at 486 (noting that the Fifth Amendment privilege "was added to the original Constitution in the conviction that too high a price may be paid even for the unhampered enforcement of the criminal law and that, in its attainment, other social objects of a free society should not be sacrificed" (quoting Feldman v. United States, 322 U.S. 487, 489 (1944))).

135 *Id*.

interest in unhindered law enforcement.[136] In turn, this means that a person's interest in protection from compelled disclosure of biometrics for access to a device is also heavily weighted.[137] *Hoffman* also helps bridge the gap from oral responses to the current issue.[138]

This bridge comes in the form of the Court's statement that the privilege must be construed liberally in favor of protecting the right to be free from compelled self-incrimination.[139] The Supreme Court recognized that a rigid interpretation of the intent of the privilege would preclude the protection of certain things that, logically, should be protected.[140] Here, that very scenario is playing out with a new and increasingly popular technology, which is challenging the placement of compulsion of biometrics in its traditional cubbyhole.[141] With liberal construction of the privilege, the leap from unprotected to protected becomes more feasible because courts are not constrained to a literal, rigid interpretation.[142] Five years later, the Supreme Court in *Ullmann* further elaborated the "spirit" that should be taken when approaching the privilege.[143]

---

136 *See Hoffman*, 341 U.S. at 486 (expounding that the Framers added the privilege to the Constitution because they realized that other important "social objects of a free society" should not be subordinate to an unhindered enforcement of the laws).

137 *See id*. (opining that a free society outweighs the unhindered enforcement of criminal laws by the government).

138 *See id*. (explaining that the privilege must be construed liberally).

139 *See id*. ("This provision of the Amendment must be accorded liberal construction in favor of the right it was intended to secure." (citing Counselman v. Hitchcock, 142 U.S. 547, 562 (1892))).

140 *Id*.

141 *See iPhone X*, APPLE (Sept. 26, 2017), https://www.apple.com/iphone-x/ [https://perma.cc/SMH2-V4HJ] (describing the new iPhone X's Face ID capabilities); Erik Ortiz, *Apple Unveils New iPhone 5C and 5S with Fingerprint Touch ID*, N.Y. DAILY NEWS (Sept. 10, 2013), http://www.nydailynews.com/news/national/apple-unveils-new-iphone-5c-price-article-1.1451007 [https://perma.cc/3AV4-2CAV] (discussing the then-new Touch ID system on the iPhone 5s, which has carried through to the newly-released iPhone 8); *Galaxy S8 Security*, SAMSUNG (Sept. 26, 2017), http://www.samsung.com/global/galaxy/galaxy-s8/security/ [https://perma.cc/NN3B-PF7Q] (explaining Samsung's new IRIS technology, which uses the user's iris to unlock the phone). There are even examples of laptops, new and old, that use fingerprint scanning to allow access to the devices. *See, e.g.*, *HP EliteBook*, *supra* note 11 (displaying HP's fingerprint technology used on its laptops to unlock access for the device's owner).

142 *See, e.g.*, Hoffman v. United States, 341 U.S. 479, 486 (1951).

143 Ullmann v. United States, 350 U.S. 422, 426 (1956). In *Ullmann*, the defendant was convicted of contempt for failing to answer questions in a grand jury proceeding after invoking the privilege. *Id*. at 425–26. He then appealed his conviction, and the Supreme Court upheld. *Id*. at 439. While the Supreme Court upheld the conviction, the decision provided key points as to the intent and scope of the privilege. *Id*. at 426–28.

The majority in *Ullmann* strongly reiterated the import of the privilege.[144] The Supreme Court believed that the privilege must not be approached with a hostile view.[145] Doing so would result in an approach that dishonored the Framers of the Constitution because of their experience with abuse of power and foresight.[146] The Court believed it more important to protect the innocent, who may be wronged by abridgment of the privilege, and allow the guilty to walk free than to abridge one innocent person's constitutional rights.[147] While the Court expressed a liberal construction of the privilege in *Hoffman*, it still requires a strict enforcement.[148] This is especially helpful in arguing for the extension of the privilege because a court must consider the gravity the privilege holds and its strict enforcement.[149]

Liberal construction, strict enforcement, and the high importance of the privilege can be combined to form a compelling framework to build a case around.[150] According to *Hoffman* and *Ullmann*, the privilege holds a level of importance in our society that cannot be brushed aside.[151] A defense attorney needs to include this in an argument to extend the privilege because it shows the court the weight of the privilege and that a cursory glance at the tradition is not appropriate.[152] Furthermore, the privilege must be liberally construed but strictly enforced against the government to protect individuals from compelled self-incrimination and prevent persecution of the innocent.[153] By including this standard in the

---

144 *See id.* (opining that the privilege "registers an important advance in the developments of our liberty—'one of the great landmarks in man's struggle to make himself civilized'" (quoting ERWIN N. GRISWOLD, THE FIFTH AMENDMENT TODAY 7 (1955))).

145 *See id*. (stating that the privilege "must not be interpreted in a hostile or niggardly spirit").

146 *See Ullmann*, 350 U.S. at 426–27 ("Such a view does scant honor to the patriots who sponsored the Bill of Rights as a condition to acceptance of the Constitution by the ratifying states. The Founders of the Nation were not naïve or disregardful of the interests of justice.").

147 *See id*. at 427–28 (expounding that the Founders judged that it was better for the occasional crime to go unpunished than for the government to be able to freely build a case and convict an innocent person based on compelled self-incrimination).

148 *See id*. at 427–29 (reiterating that *Hoffman* calls for a liberal construction of the privilege but that "it is in this spirit of strict, not lax, observance of the constitutional protection of the individual that we approach the claims made by petitioner in this case").

149 *See id*. (reinforcing the idea that the privilege should be strictly enforced to protect individual liberties against government overreach).

150 *See infra* Part IV.B (laying out the framework for the testimonial biometrics doctrine and how to implement it).

151 *See* Ullmann v. United States, 350 U.S. 422, 427–28 (1956) (describing the history of the implementation of the privilege by the Founders and their experiences with abuse of power that led them to include it in our fundamental law).

152 *See id*. at 426–29 (discussing the heavy weight and importance the privilege holds in American constitutional law).

153 *See id*.; Hoffman v. United States, 341 U.S. 479, 486 (1951).

argument, it reinforces to courts a need for flexibility in interpretation while also reinforcing the need for the privilege to be strictly enforced against abuses of investigatory powers.[154]

The purpose of this is to move the judge away from giving only a cursory glance at the issue and keeping with the traditional rulings in compulsion of biometrics cases.[155] The long line of cases holding compulsion of biometrics is not protected by the privilege proves to be a significant first hurdle for a defense attorney.[156] The judge may want to maintain the easier route of sticking with tradition.[157] A cursory glance likely will result in a ruling against extending the privilege against self-incrimination to protect biometrics.[158] That is not the desired result.[159] Opening the argument with this reminder can persuade the judge to keep an open mind with the rest of the argument.[160] The next step is to distinguish the current issue from the precedents that a judge may turn to in making a decision.[161]

B. What the Privilege Has Not Traditionally Protected

Part III.B delves into what the Fifth Amendment privilege has not traditionally protected.[162] Because this Note focuses on compulsion of biometrics for the purpose of unlocking devices, Part III.B focuses on past

---

154 Combined, both *Hoffman* and *Ullmann* create a compelling standard of liberal construction and strict enforcement against the government. *Hoffman*, 341 U.S. at 486; *Ullmann*, 350 U.S. at 427–29. Thus, the court must liberally construe the privilege in favor of strictly enforcing prevention of possible government overreach. *Hoffman*, 341 U.S. at 486; *Ullmann*, 340 U.S. at 427–29.

155 *See, e.g.*, Schmerber v. California, 384 U.S. 757, 761–65 (1966) (establishing that providing biometrics, generally, is not testimonial and therefore not protected by the privilege).

156 *See, e.g.*, *id*. at 765 (holding that providing blood samples is not protected by the privilege against self-incrimination). *See also* United States v. Dionisio, 410 U.S. 1, 6–7 (1973) (finding that providing a voice exemplar does not communicate any fact and is therefore not testimonial); United States v. Wade, 388 U.S. 218, 222 (1967) (deciding that presenting oneself for a lineup is not testimonial and therefore not protected).

157 *See, e.g.*, *Wade*, 388 U.S. at 222 (following the same line of reasoning as the Court did in *Schmerber*).

158 *See* cases cited *supra* note 156 (providing several Supreme Court cases ruling against extending the privilege to biometrics).

159 *See infra* Part IV (expounding the desired implementation of the testimonial biometrics doctrine).

160 *See infra* Part IV.

161 *See infra* Part III.B (analyzing cases holding biometrics are not protected by the privilege and distinguishing them from the current issue).

162 *See* cases cited *infra* notes 165 & 166 (discussing cases that hold biometrics are not protected by the privilege).

cases holding biometrics are not protected by the privilege.[163] Part III.B does not criticize the holdings of the cases it discusses but is meant to provide useful distinctions between those cases and the current issue, which can be used to persuade a court to extend the privilege.[164]

Here, the analysis focuses on cases in which compulsion of certain biometrics was held not to be protected by the privilege.[165] These cases include *Schmerber*, *Dionisio*, and *Wade*.[166] Each case is covered in turn, and an important distinction between these representative cases and the current issue is made.[167] While Part III.B contains an analysis of each of these cases, each is connected by an overarching theme: compulsion of biometric data is not protected because providing it is not testimonial.[168] Turning to *Schmerber*, keep this in mind as each case is discussed.[169]

---

163 *See infra* notes 165–86 and accompanying text (explaining the common theme that spreads across each of the cases covered, which can then be used to provide a distinguishing factor in an argument to the court).

164 Part III.B does not disagree with the past holdings that biometrics are not protected by the privilege. It only seeks to show how the compulsion of biometrics in the particular context of unlocking devices is distinguishable.

165 Fifth Amendment jurisprudence is expansive, with many cases ruling on whether or not the Fifth Amendment provides protections, but as this Note's focus is on biometrics, the analysis here focuses solely on cases concerning compulsion of biometrics. For another example of something not protected by the privilege, see Doe v. United States, 487 U.S. 201, 219 (1988) (declining to extend the privilege to artificial entities such as businesses). Interestingly, *Schmerber* does contain dicta that explores the possibility of certain physiological responses being protected by the privilege. Schmerber v. California, 384 U.S. 757, 764 (1966). Justice Brennan speaks of how the use of physiological responses to questioning to determine innocence or guilt "is to evoke the spirit and history of the Fifth Amendment." *Id*. Thus, an interesting exception to the doctrine that no biometrics are protected by the privilege was born. *Id*. Further, in this discussion the Court also mentions cases in which such a simple distinction used by the traditional approach "is not readily drawn." *Id*. The compulsion of biometrics for the purpose of unlocking devices is such a case.

166 Each of these cases provides a different example of some piece of biometric datum compelled by the government in a criminal investigation. *Schmerber* 384 U.S. at 758; United States v. Dionisio, 410 U.S. 1, 3 (1973); United States v. Wade, 388 U.S. 218, 220 (1967); United States v. Gibson, 444 F.2d 275, 275 (5th Cir. 1971).

167 *See infra* Part IV (outlining a more detailed framework of the testimonial biometrics doctrine).

168 Each case came to the conclusion, and reiterated past decisions that held the same, that providing biometric data is not communicative and therefore not testimonial. *See* cases cited *supra* note 166 (providing cases in which the Supreme Court declined to find compulsion of biometrics protected by the privilege against self-incrimination).

169 The fact that providing biometrics is not testimonial is the crux of the issue this Note covers. *See infra* Parts III.C, III.D (covering cases that touched upon decrypting devices). Understanding why that is the case, and how these cases can be distinguished from the issue of compelling biometrics to unlock devices, is key to making a compelling argument.

Schmerber held that the compulsion of a blood sample was not protected by the privilege because it was not testimonial.[170] While in the context of the time the Court most likely reached the correct conclusion, under the current circumstances this reasoning results in a troubling scenario in which no biometrically encrypted devices are protected.[171] Here, if providing fingerprints or some other biometric datum to unlock the provider's device is not considered communicative, it is not testimonial.[172] Therefore, it would not be protected by the privilege.[173] This is troubling because it gives the government the power to force individuals using biometric encryption to provide access to the device and its contents.[174] The Supreme Court in *Dionisio*, relying in part on *Schmerber*, reached the same conclusion.[175]

In *Dionisio*, the Court declined to extend the privilege to protect a voice exemplar.[176] Again, the reasoning was that a voice exemplar is not communicative.[177] Similar to *Schmerber*, this result provides an obstacle to finding that compulsion of biometrics to unlock a device is protected by the privilege against self-incrimination.[178] *Wade*, decided in 1967, provides only one more example of this rule.[179] There, the Court continued to add weight to the rationale that providing most, if not all, kinds of biometrics

---

170 Schmerber was convicted in California for driving under the influence of alcohol. *Schmerber*, 384 U.S. at 758. He was arrested at the hospital after a police officer directed a physician to withdraw blood from him and have it analyzed for intoxication. *Id*. The results were positive and admitted as evidence, which Schmerber then challenged. *Id*. at 759. The Court reasoned that providing blood was not communicative. *Id*. at 765. The Court further reasoned that without some compelled communication from the suspect, the privilege does not apply because there is no testimony. *Id*. at 765.

171 Under the test used in *Schmerber* and the ensuing cases, no devices that use biometrics to unlock the device would be protected because the biometrics are merely being used for identification purposes. *See generally id*. (opining that biometric data is only used for the purpose of identification).

172 *See, e.g.*, *Schmerber*, 384 U.S. at 764–65 (establishing that providing biometrics, such as a blood sample, is not communicative under most circumstances).

173 *See id*.

174 *See id*. (finding that the government may force a person to provide biometrics in an investigation if doing so is not communicative).

175 *See* United States v. Dionisio, 410 U.S. 1, 5–7 (1973) (holding that compulsion to provide a voice exemplar did not violate the Fifth Amendment privilege).

176 *See id*.

177 *See id*. at 7.

178 *See id*. at 6–7 (holding that biometrics such as voice communications are not always communicative if used only for identification purposes and do not communicate any substantive fact).

179 *See* United States v. Wade, 388 U.S 218, 222–23 (1967) (reasoning that displaying oneself in a police lineup in front of a witness is not testimonial because it is only for identification and does not communicate anything).

is not testimonial.[180] Under the circumstances in the above cases, the decisions made sense because none communicated any kind of fact other than identity.[181]

However, this common thread of reasoning can be distinguished from the current situation.[182] As stated above, the main reason each of the above cases landed the way it did was because compulsion of biometrics is not considered communicative and therefore not testimonial.[183] However, under the current scenario, and as will be explored fully in a later section,[184] compelled production of biometrics is testimonial in the context of unlocking a device.[185] The important distinction between the above cases and the current issue is that, when using biometrics to unlock a device, it is used for more than mere identification.[186] As will be shown later, the act of providing biometrics to unlock a device is a form of communication that says that you own, or at least have some control over, that device.[187] With that distinction, the traditional rule and reasoning followed in the cases above can be combatted.[188]

---

180 *See id*. (following the same line of reasoning as the Court did the previous year in *Schmerber*).

181 *See, e.g.*, United States v. Dionisio, 410 U.S. 1, 6–7 (1973) (reasoning that merely providing a voice exemplar does not communicate any incriminating fact, it only provides a means of identification). The Court in cases such as *Dionisio* came to the right conclusion because each of these forms of biometrics only communicated the fact of identity. *Id*. However, as the current situation shows, that is not always the case. *See In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073 (N.D. Ill. 2017) (holding that forcing a person to unlock her device using her biometrics communicates the fact of ownership of the device and its contents, including incriminating evidence). Here, a person applying biometrics to unlock a device is not just affirming identity; the person is asserting that she is the controller of the device, as well as the contents within. *Id*.

182 *See supra* note 181 (distinguishing the current issue from past cases in which biometrics were not protected).

183 *See* cases cited *supra* notes 172, 175 & 179 (providing the reasoning behind cases holding that biometrics are not protected by the privilege).

184 *See infra* Part III.D (discussing the recent case from the Northern District of Illinois that held compelled production of biometrics to unlock a device is testimonial and why this decision is correct).

185 *See Application for a Search Warrant*, 236 F. Supp. 3d at 1074 (holding that compelled production of biometric data for unlocking a device is testimonial); In the Matter of the Search of a Residence in Oakland, Cal., No. 4-19-70053, 2019 WL 176937, at *3 (positing that providing biometric data to unlock a device is testimonial).

186 *Compare Application for a Search Warrant*, 236 F. Supp. 3d. at 1073–74 (stating that providing fingerprints to unlock a device is more than identification), *with Dionisio*, 410 U.S. at 5–7 (explaining that providing biometric data, such as a voice exemplar, is only for identification purposes).

187 *See infra* Part III.D (analyzing the case supporting the assertion that providing biometrics to unlock a device is testimonial).

188 *See* cases cited *supra* note 186 (furthering the distinction between the precedent biometrics cases and the current issue).

This is a crucial distinction to make in an argument to extend the privilege to compulsion of biometrics to unlock a device.[189] These repeatedly upheld notions need a strong counterargument in order for the argument in favor of extending the privilege to be successful.[190] Including this distinguishing factor in an argument to extend the privilege provides that counter.[191] A further exploration and discussion of how providing biometrics to unlock a device is testimonial takes place in Part III.D, allowing a defense attorney to better make this argument.[192]

C. Courts' Willingness to Expand Individual Privacy Interests

With the increasing advancement of technology that can be used by the government to invade the privacy of individuals, courts have proven willing to expand individual privacy interests.[193] Part III.C analyzes cases in which both the Supreme Court and lower courts ruled in favor of expanding the privilege against self-incrimination, as well as the Fourth Amendment.[194] Part III.C focuses on lower courts' rulings on traditional encryption.[195] While this Note focuses on the Fifth Amendment privilege, Fourth Amendment cases are mentioned because both the Fourth and Fifth Amendments involve protecting citizens from government overreach.[196]

The Supreme Court has not yet provided a ruling on whether compulsion of a traditional alphanumeric password, whether through writing or speech, is protected by the privilege.[197] However, lower courts have ruled on the issue and generally reached a consensus that it is protected by the privilege.[198] *In re Grand Jury Subpoena Duces Tecum Dated*

---

189 Courts, and the opposition, will likely look to these or similar cases to rebut the assertion that the privilege should be extended. It is crucial to counter these cases with this distinguishing factor to make a stronger argument.

190 *See supra* note 6 (highlighting the cases that held compulsion of biometrics to unlock a device is not testimonial).

191 *See infra* Part III.D.

192 *See infra* Part III.D (providing a deeper analysis of cases covering biometric encryption to unlock a device).

193 *See* cases cited *infra* note 198 (analyzing cases in which courts proved willing to expand the privilege and other individual privacy interests with the rise of new technologies).

194 *See* cases cited *infra* note 198.

195 *See* cases cited *infra* note 198.

196 *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 36 (2001) (providing an example case in which the Supreme Court expanded Fourth Amendment protections).

197 *See, e.g.*, United States v. Kirschner, 823 F. Supp. 2d 665 (E.D. Mich. 2010) (holding that compelling a person to provide her password to her device violates the privilege against self-incrimination).

198 *See id.* at 669. *See also* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012) (ruling that compulsion to provide an encryption password violates the privilege against self-incrimination); In the Matter of the Search of a Residence

March 25, 2011, is the first example in which a court held that compulsion of a password to unlock traditional encryption violates the privilege.[199] The Court of Appeals for the Eleventh Circuit focused on the fact that the act of decrypting and producing the files on the device is an action that asserts a statement of fact.[200] Specifically, the defendant would disclose the contents of his own mind by providing the password.[201] In turn, providing the password was an act that "would be tantamount to testimony by Doe of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives, and of his capability to decrypt the files."[202] This statement proves to be the key analogy to pull out to make the argument to extend the privilege to biometric encryption as well.[203]

To make the argument, analogize between *Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, and the instant issue.[204] Argue that the exact situation occurs during compulsion of biometrics to decrypt the device.[205] By providing the biometric datum needed to unlock and decrypt the device, the defendant is performing an act that asserts a statement of fact.[206] This is regardless of the biometric datum used, whether it is a fingerprint, eye scan, or face scan.[207] It states the defendant's knowledge of the existence and location of the device or files sought; her possession, control, and access to the encrypted device and files; and her ability to decrypt the device or files.[208] Point to the fact that, beside the manner in which the decryption key is entered, no distinguishable difference

---

in Oakland Cal., No. 4-19-70053, 2019 WL 176937, at *2–5 (N.D. Cal. Jan. 10, 2019) (acknowledging that providing a traditional alphanumeric password is testimonial).

199 *See Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d at 1346.

200 *See id*. (focusing on the act of decrypting and producing the files on the drive as a testimonial act).

201 *See id*. ("First, the decryption and production of the hard drives would require the use of the contents of Does' mind and could not be fairly characterized as a physical act that would be nontestimonial in nature.").

202 *Id*.

203 *See infra* Part IV.A (laying out the testimonial biometrics doctrine and how to argue in support of it in litigation).

204 *See infra* Part IV.A.

205 See Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012) (reasoning that the act of decrypting a device is testimonial).

206 *See infra* Part III.D (explaining why providing biometrics asserts a statement of fact that the defendant owns or controls the device).

207 *See supra* note 11 (outlining several of the common forms of biometrics used for biometric encryption).

208 *See In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073 (N.D. Ill. 2017) (explaining that the defendant is testifying to her knowledge of ownership of the device when providing biometrics to unlock a device).

between the precedent case and the instant case exists.[209] Further this point by using *United States v. Kirschner*.[210]

The court in *Kirschner* used the same reasoning as *Grand Jury Subpoena Duces Tecum Dated March 25, 2011*.[211] Divulging a password due to government compulsion is using one's mind to commit an act that asserts a statement of fact.[212] The same reasoning can apply to the issue of compulsion of biometrics.[213] Requiring a defendant to provide biometrics to unlock a device is just like requiring the defendant to provide the password to it.[214] The defendant is asserting the fact that she owns or controls the device and the files contained within.[215] The biometric datum, in this context, is not being used solely for identification purposes.[216] It is used to assert the fact that the device and files in question are owned or controlled by the defendant.[217] That is more than mere identification.[218]

Traditional cases finding that biometrics are only used for identification purposes and do not involve any communicative aspects do not apply in this context.[219] Here, the biometric datum is used to assert facts beyond identity.[220] It asserts that the incriminating device or files sought by the government through compulsion of the biometric datum is

---

209 *Compare Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d at 1346 (reasoning that providing a traditional password is testimonial and protected by the privilege), *with Application for a Search Warrant*, 236 F. Supp. 3d at 1073 (holding that providing biometrics to decrypt a device is testimonial and protected by the privilege).

210 *See infra* note 212 and accompanying text (providing an analysis of *Kirschner*).

211 *Compare Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d at 1346 (deciding that providing a password to unlock a device is testimonial), *with* United States v. Kirschner, 823 F. Supp. 2d 665, 668–69 (E.D. Mich. 2010) (ruling that providing a password to decrypt a device is testimonial).

212 *See Kirschner*, 823 F. Supp. 2d at 668 ("In this case, the government is not seeking documents or objects—it is seeking testimony from the Defendant, requiring him to divulge through his mental processes his password—that will be used to incriminate him.").

213 *See supra* note 209 and accompanying text (comparing the similarities between providing a traditional password and biometric password).

214 *Compare Kirschner*, 823 F. Supp. 2d at 668–69 (reasoning that providing a traditional password is testimonial), *with In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073 (N.D. Ill. 2017) (ruling that providing biometrics to unlock a device is communicative because it asserts a fact about ownership).

215 *See Application for a Search Warrant*, 236 F. Supp. 3d at 1073; In the Matter of the Search of a Residence in Oakland, Cal., No. 4-19-70053, 2019 WL 176937, at *2–4 (N.D. Cal. Jan. 10, 2019).

216 *See Application for a Search Warrant*, 236 F. Supp. 3d at 1073 (deciding that when the government seeks to compel biometrics to unlock a device, it is using the biometrics for more than identification).

217 *See id*.

218 *See id*.

219 *See id*. (distinguishing the current issue from precedent cases in the analysis).

220 *See id*.

owned or controlled by the defendant.[221] The defendant is not just providing identity, she is effectively testifying that the incriminating evidence is hers.[222] Therefore, it is forced self-incrimination through testimony.[223] Three recent cases are discussed next. Few federal district courts opted to extend the privilege to cover compulsion of biometrics to unlock a person's device.[224]

D. Why the Recent Decision from the Northern District of Illinois is Right

While litigation over the issue of this Note is likely to increase soon, only a few cases have addressed it so far.[225] Part III.D analyzes two cases and explains why the decision in *In re Application for a Search Warrant* is the correct decision and pulls out the reasoning to use.[226]

The state courts in *Commonwealth v. Baust* and *State v. Diamond* both found that compulsion of biometrics to unlock a device is not protected by the privilege.[227] The courts both reasoned that, as courts traditionally do, providing biometrics is not testimonial.[228] Both courts stated that providing biometrics does not involve any kind of communication of knowledge.[229] Indeed, the courts stated that the device could be unlocked passively by the defendants.[230] While this reasoning is correct in the traditional context of using biometrics for identification, it is not the correct reasoning to use in the current context.[231]

Here, as the court in *Application for a Search Warrant* recognized, providing the biometric datum does more than just identify the

---

221 *See id*.

222 *See id*.

223 *See id*.

224 *See infra* text accompanying notes 227–36 (scrutinizing recent decisions regarding providing biometrics to unlock a device).

225 *See infra* text accompanying notes 232–36 (canvassing the recent decisions over whether providing biometrics to unlock a device is testimonial).

226 *See infra* text accompanying notes 232–36 (analyzing the recent decisions and explaining why the reasoning from the Northern District of Illinois is the correct reasoning to put in an argument to extend the privilege). *See also* In the Matter of the Search of a Residence in Oakland, Cal., No. 4-19-70053, 2019 WL 176937, at *2–4 (N.D. Ill. Jan. 10, 2019) (finding in favor of extending the privilege against self-incrimination to compulsion of biometric data to unlock a device).

227 *See* Commonwealth v. Baust, No. CR14-1439, 2014 WL 10355635, at *2–3 (Va. Cir. Ct. Oct. 28, 2014) (holding that providing biometric data to unlock a device is not testimonial and therefore not protected by the privilege).

228 *See Baust*, 2014 WL 10355635, at *2–3; State v. Diamond, 890 N.W.2d 143, 149–50 (Minn. Ct. App. 2017).

229 *See* cases cited *supra* note 228.

230 *See, e.g.*, *Baust*, 2014 WL 10355635, at *4 ("The fingerprint, like a key, however, does not require the witness to divulge anything through his mental processes.").

231 *See id*. (reasoning that providing biometrics to unlock a device is not testimonial).

defendant.[232] The difference here is that when the defendant provides the biometric datum, she is essentially communicating that she is the owner or controller of the device and its contents.[233] She is committing an act that asserts a statement of fact: she is the owner of the device with incriminating evidence on it.[234] Accordingly, she is testifying to the fact that she is the owner of the incriminating evidence and has the ability to decrypt the information.[235] The courts in *Baust* and *Diamond* failed to realize this.[236] Those courts essentially followed the tradition and failed to recognize the new context in which biometrics are used.[237] The traditional approach can no longer be applied when it comes to compulsion of biometrics to unlock a device.[238]

Application for a Search Warrant uses the correct line of reasoning.[239] The court there was correct to recognize that the precedent cases ruling against extending the privilege to biometrics could not apply because they

---

232 *Compare id*. (holding that providing biometrics does not communicate any knowledge or facts), *with In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073 (N.D. Ill. 2017) (reasoning that providing biometrics to unlock a device communicates knowledge and is not used for mere identification), *and* In the Matter of the Search of a Residence in Oakland, Cal., No. 4-19-70053, 2019 WL 176937, at *2–4 (N.D. Cal. Jan. 10, 2019) (finding that providing biometric data to unlock a device is testimonial).

233 *See supra* note 232 (comparing the holding in *Baust* with the holding in *In re Application for a Search Warrant* and *Search of a Residence in Oakland, Cal.*).

234 *See Application for a Search Warrant*, 236 F. Supp. 3d at 1073 (deciding that providing biometrics to unlock a device is tantamount to testimony that she is the owner of the device with the evidence that is sought on it); *Search of a Residence in Oakland, Cal.*, 2019 WL 176937, at *2–4 (ruling that providing biometric data to unlock a device asserts a factual statement that the provider has some level of control over the device).

235 *See Application for a Search Warrant*, 236 F. Supp. 3d at 1073 (asserting that providing biometric data to unlock a device is tantamount to testimony); *Search of a Residence in Oakland, Cal.*, 2019 WL 176937, at *2–4 (following the reasoning in *Application of a Search Warrant* that providing biometric data to unlock a personal device is testimonial).

236 *See* Commonwealth v. Baust, No. CR14-1439, 2014 WL 10355635, at *4 (Va. Cir. Ct. Oct. 28, 2014) (failing to recognize the new context in which biometrics are used compared to the traditional context); State v. Diamond, 890 N.W.2d 143, 149–50 (Minn. Ct. App. 2017) (maintaining the traditional reasoning of biometrics that no longer applies to biometrics for unlocking devices).

237 *See supra* note 236 (explaining the courts' maintenance of the traditional rule regarding biometrics).

238 *See supra* note 165 (highlighting why the traditional rule can no longer apply to biometrics to unlock a device).

239 *See In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073 (N.D. Ill. 2017) (reasoning that providing biometrics to unlock a device is testimonial and falls under the protection of the privilege). *See also* In the Matter of the Search of a Residence in Oakland, Cal., No. 4-19-70053, 2019 WL 176937, at *2–4 (N.D. Cal. Jan. 10, 2019) (stating that giving biometric data to unlock a personal device is testimonial).

were ruled on in a different time and context.[240] During that time period, the existence of devices that contained a person's entire private life that could be accessed via biometric data could not be conceived of.[241] Accordingly, those cases only dealt with the context of identifying a defendant and placing her in a certain place.[242] The court here recognized the technological development of cell phones and their central role in our lives, as well as the level of privacy they are granted.[243] These are important connections to make in the argument for extending the privilege.[244]

Not only does the court here recognize the importance of the different contexts, it recognizes the importance of the act of production.[245] Unlocking the phone essentially produces everything contained within, including documents.[246] The act of producing documents by an individual is protected by the privilege,[247] and a defense attorney can also make this point to further bolster the argument.[248]

A defense attorney needs to argue the same line of reasoning as *Application for a Search Warrant*.[249] Point out that the contexts are entirely different between the precedent cases and the current issue.[250] In the context at issue, the biometric data are not being used for identification: they are being used to force the defendant to testify that she is the owner

---

240 *See Application for a Search Warrant*, F. Supp. 3d at 1073 ("The *Wade* court could not have anticipated the creation of the iPhone nor could it have anticipated that its holding would be applied in such a far-reaching manner.").

241 *See id*. (stating the court does "not believe that a simple analogy that equates the limited protection afforded a fingerprint used for identification purposes to forced fingerprinting to unlock an Apple electronic device that potentially contains some of the most intimate details of an individual's life . . . is supported by Fifth Amendment jurisprudence").

242 *See id*.

243 *See id*. *See also* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (recognizing that the Court should be mindful of how technology can impact law).

244 *See infra* Part IV.A (providing the argument to support testimonial biometrics).

245 *See Application for a Search Warrant*, 236 F. Supp. 3d at 1073 ("By using a finger to unlock a phone's contents, a suspect is *producing* the contents on the phone.").

246 *See id*. *See also* In the Matter of the Search of a Residence in Oakland, Cal., No. 4-19-70053, 2019 WL 176937, at *2–4 (N.D. Cal. Jan. 10, 2019) (providing that unlocking a phone via biometric data is equal to providing documents).

247 *See* United States v. Hubbell, 530 U.S. 27, 45–46 (2000) (finding that the act of producing documents is testimonial and can trigger the privilege against self-incrimination).

248 *See infra* Part IV.A (establishing the argument a defense attorney needs to make in support of testimonial biometrics).

249 *See infra* Part IV.A. *See also Search of a Residence in Oakland, Cal.*, 2019 WL 176937, at *2–5 (following the example set by *Application for a Search Warrant* and ruling that providing biometrics to unlock a device is testimonial).

250 *See supra* note 232 (comparing cases using the traditional context and the new context).

or controller of the device containing incriminating evidence.[251] Argue that when a person is forced to provide biometrics to unlock a device, she is, in turn, being forced to commit an act that asserts that she is the owner of the device.[252] Be sure to raise the point of the act of production.[253] Unlocking the phone necessarily produces the device, as well as all of the files and documents contained within.[254] This makes the act testimonial, which then meets each of the three elements for invoking the protection of the privilege.[255] This is the most crucial piece of the doctrine.[256]

This argument establishes why providing biometrics to unlock a device is testimonial, which is the only bar keeping it from being protected by the privilege.[257] The other arguments above help bolster this central argument.[258] Distinguishing from *Baust* and *Diamond* and analogizing to *Application for a Search Warrant* are key to making the argument in support of the doctrine of testimonial biometrics.[259] Part IV lays out why this new doctrine is necessary with the increasing use of biometric encryption.[260]

---

[251] *See In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073 (N.D. Ill. 2017) (stating that "a suspect is testifying that he or she has accessed the phone before, at a minimum, to set up the fingerprint password capabilities, and that he or she currently has some level of control over or relatively significant connection to the phone and its contents"); *Search of a Residence in Oakland, Cal.*, 2019 WL 176937, at *2–5 (using the same reasoning as *Application for a Search Warrant*).

[252] *See supra* note 251 (providing two cases that held that providing biometric data to unlock a device is testimonial).

[253] *See Hubbell*, 530 U.S. at 45–46 (holding that production of documents can rise to the level of testimony on its own). This is another strong point to make. *Id.* In modern devices, producing the contents on the device is inevitably producing the documents contained on it as well. *See Application for a Search Warrant*, 236 F. Supp. 3d at 1073 (providing that using a fingerprint to unlock a device is "using a fingerprint to access a database of someone's most private information").

[254] *See supra* note 251 (pointing out the court's reasoning that unlocking a device produces the contents within).

[255] *See supra* note 52 (establishing the three elements of the privilege against self-incrimination).

[256] *See infra* Part IV.A (providing the argument in support of the doctrine of testimonial biometrics).

[257] *See supra* note 6 (laying out several cases that held production of biometrics does not violate the privilege against self-incrimination because it is not testimonial).

[258] *See supra* Parts III.A, III.B & III.C (analyzing the argument in support of the doctrine of testimonial biometrics).

[259] *See supra* notes 232–38 (highlighting important distinctions and analogies to make in the argument in support of testimonial biometrics).

[260] *See infra* Part IV (giving the argument in support of testimonial biometrics).

IV. CONTRIBUTION

Part IV.A puts forth the new doctrine of testimonial biometrics described in the above analysis.[261] It briefly establishes what the doctrine is and its components.[262] Part IV.B discusses why the doctrine is needed and addresses its several counterarguments and limitations.[263]

A. The Testimonial Biometrics Doctrine

The testimonial biometrics doctrine is simple: providing biometric data to unlock a device is testimonial and, therefore, protected by the privilege against self-incrimination.[264] By providing biometric data, a person is communicating knowledge that she is the owner or controller of the device and the files within.[265] The communicative nature of the act of providing biometric data makes it testimonial.[266] Because it is testimonial, as long as there is compulsion and the information sought is incriminating, it meets all the elements needed for the protection of the privilege.[267]

Testimonial biometrics are not used in the traditional context, to identify, but are used to prove the ownership of a possibly incriminating device and the incriminating evidence therein.[268] When a person commits the act of unlocking the device, it is necessarily testimony that she owns the device or at least has a measure of control over it insofar as she has set up the biometric encryption.[269] She asserts the fact that she is the owner or controller of the information contained within.[270] This is communicating knowledge of ownership or control of the incriminating device and its contents, which is self-incriminating testimony.[271]

---

261 *See infra* Part IV.A.

262 *See infra* Part IV.A.

263 *See infra* Part IV.B (explaining why the doctrine is needed and addressing the possible counterarguments).

264 *See supra* Part III.

265 *See supra* Part III (discussing how a person communicates knowledge when providing biometrics to unlock her device).

266 *See supra* Part III.

267 *See supra* Parts II & III.

268 *See supra* Part III.D (analyzing how testimonial biometrics use biometrics for more than just identification).

269 *See supra* Part III.D (explaining that the act of unlocking the device is testimony that the person owns the device or has some measure of control over it).

270 *See supra* Part III.D.

271 *See supra* Part III.D.

Therefore, the privilege protects the compulsion of biometric data from a person to unlock that person's device.[272]

A defense attorney should use the above analysis to set up the argument to extend the privilege to protect biometric decryption keys.[273] Begin with reminding the court of the historical intent of the privilege against self-incrimination.[274] Reinforce to the court the privilege's importance and weight, its purpose to protect citizens from government overreach and maintain an adversarial system of justice, and the privilege's liberal construction and strict enforcement.[275] Doing so creates a strong opening that will help open the judge's mind to the rest of the argument.[276]

Next, make the distinctions between the precedent cases on biometrics and the current issue.[277] Distinguish testimonial biometrics from historical cases such as *Schmerber*, *Dionisio*, and *Wade* by showing that, in the current circumstance, the biometrics are used for more than just identifying a person.[278] This immediately combats what is most likely to be the main counterargument.[279] Dispensing with this counterargument quickly allows the rest of the argument to focus on showing cases in which courts expanded privacy interests and the final point of exactly how testimonial biometrics are different from the traditional context.[280]

After analogizing the current issue with scenarios in which courts have proven willing to expand privacy interests, the final, and most important, point to make is how the context of testimonial biometrics is different from the traditional context.[281] This part of the argument is both a combination of analogizing to *Application for a Search Warrant* and making the same policy points set out in that case.[282] While policy arguments are often considered to be a last resort, in a case of first impression policy points can be useful.[283] It is especially so here, where a

---

272 *See supra* Part III.D (discussing why the privilege against self-incrimination should prohibit the compulsion of biometrics to unlock a device).

273 *See supra* Part III.D (laying out the argument that a defense attorney should use to support testimonial biometrics).

274 *See supra* Part III.A (explaining how to use the intent of the privilege in the argument).

275 *See supra* Part III.A.

276 *See supra* Part III.A.

277 *See supra* Part III.B.

278 *See supra* Part III.B (providing distinctions to make between testimonial biometrics and *Schmerber*, *Dionisio*, and *Wade*).

279 *See infra* Part IV.B.

280 *See infra* Part IV.B.

281 *See supra* Parts III.C & III.D (providing cases in which courts expanded the privilege).

282 *See supra* Part III.D.

283 *See, e.g.*, *supra* Part III.D (noting the policy reasons behind the court's decision to rule that compulsion to provide biometrics to unlock a device violates the privilege).

defense attorney can point to the potential policy implications in allowing authorities to compel the biometrics of the tens of millions of people using biometric encryption.[284] Distinguishing the policy differences between testimonial biometrics and traditional biometrics is important because, in the past, allowing compulsion of biometrics only allowed the identification of individuals, but now it allows access to a person's entire personal life.[285] With the above points, a well-rounded argument supporting testimonial biometrics is complete.[286]

B. Commentary

This new doctrine is needed now before the increase in litigation that is bound to happen with the increasing use of biometric encryption.[287] The use of biometric encryption is on the rise and can lead to government overreach once authorities become increasingly aware of biometric encryption's unprotected status.[288] It is feasible to imagine that, at some point in the near future, some devices will use biometric encryption almost exclusively.[289] Preventing government overreach is one of the core values the privilege is designed to prevent.[290] It is scary to imagine a world in which the government can force any person to unlock her phone using biometric encryption because it is not protected by the privilege.[291]

In a world where a large quantity of devices are not protected from government intrusion by the privilege against self-incrimination, the possibility for government intrusion increases.[292] The situations in which government overreach can occur extend beyond grand jury investigations and trials.[293] That is exactly why this doctrine advocating for the extension of the Fifth Amendment's protection is necessary now.[294] It can be a proactive solution instead of a retroactive remedy to already-committed

---

284 *See supra* Part III.D (highlighting the court's concerns with potential government overreach).

285 *See supra* Part III.D (pointing out the policy implications in allowing the traditional rule regarding biometrics to apply to testimonial biometrics).

286 *See supra* Part III.

287 *See supra* Part III.

288 *See supra* Part III.

289 *See supra* note 141 (showcasing the increasing number of devices incorporating biometric encryption).

290 *See supra* Part II.A.

291 *See supra* Part I (introducing the problem and a hypothetical situation, which can occur with the current rule governing compulsion of biometrics).

292 *See supra* note 141.

293 *See supra* Part I.

294 *See supra* Part I (introducing the issue and explaining why a new doctrine is needed now).

government intrusion.[295] Further, the doctrine of testimonial biometrics does not overreach or overprotect criminal suspects and defendants.[296]

The main counterargument to this doctrine is likely that it provides too much protection to criminal suspects and defendants.[297] Some will argue that this doctrine creates a total bar to the government's access to encrypted devices.[298] However, this doctrine does not seek to totally prohibit access to individuals' devices through biometrics.[299] This doctrine only seeks to extend the protection of the privilege to a point where the government must carry the same level of proof as normal encryption.[300] Specifically, the government can still gain access to the device through compulsion of biometrics if it can prove the foregone conclusion doctrine.[301] If the government can meet the standards of the foregone conclusion doctrine, it will be able to obtain a valid warrant for the information sought through the use of the suspect's biometric data.[302] The doctrine still provides viable routes for the government to gain access to the information sought.[303]

Similarly, opponents are likely to argue that this doctrine hamstrings law enforcement agencies and prevents them from effectively pursuing criminals by preventing access to biometrically encrypted devices.[304]

---

295 *See supra* Part IV.A (explaining the doctrine and its goals).

296 *See infra* note 297 and accompanying text (discussing how the doctrine still gives the government viable routes around the privilege).

297 *See, e.g.*, Lev Grossman, *Inside Apple CEO Tim Cook's Fight with the FBI*, N.Y. TIMES (Mar. 17, 2016), http://time.com/4262480/tim-cook-apple-fbi-2/ [http://perma.cc/F7SC-UKMY] (exploring Apple's public legal fight with the FBI over encryption following the San Bernardino attack). While the issue here is different than the issue raised in Apple's spat with the FBI, Apple was portrayed as interfering with and hindering law enforcement by refusing to make it easier for law enforcement to decrypt its devices. *Id*. A similar situation arises here: this doctrine seeks to make it more difficult for law enforcement to access encrypted devices. *See supra* Part IV.A. It is likely that this doctrine will be viewed in much the same manner as Apple was viewed when it refused to help the FBI. *See* Grossman, *supra* (covering how Apple was viewed and portrayed following its refusal to help the FBI decrypt the San Bernardino attacker's phone).

298 *See* Grossman, *supra* note 297.

299 *See supra* note 107 (expounding what the foregone conclusion doctrine is and how it applies to encryption).

300 This doctrine does not seek to be a total bar to government access to devices protected by biometric encryption. It seeks to provide biometric encryption the same protection other testimonial issues are afforded.

301 *See supra* Part II (describing how the government can gain access to a device through proving a foregone conclusion).

302 *See supra* note 107 (explaining what the foregone conclusion doctrine is and how it allows the government to access devices if it can meet the standard).

303 *See supra* note 107.

304 *See* Grossman, *supra* note 297. Former FBI Director James Comey publicly expressed his frustration with Apple because he felt the hindrance of being unable to access encrypted devices kept him from doing his job. *See id*. (giving Comey's statements in regard to how

However, as previously noted, this doctrine does not seek to create a total bar to accessing biometrically encrypted devices.[305] This doctrine merely seeks to ensure that law enforcement accesses information on a biometrically encrypted device in a constitutional manner.[306] Admittedly, this creates a higher burden on law enforcement; however, the creation of a slight burden on law enforcement does not outweigh the need for law enforcement to act within the confines of the Constitution.[307] While law enforcement may not be happy about the added step necessary to access biometrically encrypted devices, this doctrine seeks to require law enforcement to act within the Constitution and still provides avenues for accessing information on those devices.[308]

This doctrine is also unlikely to be preempted in the near future.[309] Thus far, only several cases in the country have faced the issue of compulsion of a person's biometrics to unlock that person's device.[310] So far, none of those cases have continued to appeal the ruling against the doctrine.[311] Of the three cases facing the issue, only *Diamond* made it to the state appellate level, and that ruling has not been appealed.[312] *Baust* did not appeal the ruling and is unlikely to see an appeal three years after the ruling.[313] Due to the low level of litigation on the issue, and the lack of appeals, it is unlikely the Supreme Court will face this issue for at least several years.[314] It is also unlikely that Congress passes legislation dealing with the issue in a timely fashion, considering the current political

---

Apple was preventing him from fully investigating the San Bernardino attack). Here, a similar situation occurs because the doctrine creates an obstacle that law enforcement must overcome before accessing a device. *See supra* Part IV.A.

305 *See supra* Part IV.A.

306 *See supra* Part IV.A.

307 *See, e.g.*, U.S. DEP'T OF JUSTICE, POLICING 101 (2017), https://www.justice.gov/crs/file/836401/download [https://perma.cc/BL9W-QADM] (stating what constitutional policing is and its fundamental nature).

308 *See* Part IV.A.

309 *See infra* text accompanying notes 310–15.

310 *See supra* Part III.D (analyzing the cases that have dealt with compulsion of biometrics to unlock a device).

311 *See supra* Part III.D.

312 *See supra* Part III.D.

313 *See supra* Part III.D.

314 *See supra* Part III.D (showing the minimal litigation that has occurred in relation to the issue of testimonial biometrics).

climate.[315] Therefore, it is unlikely that testimonial biometrics will be preempted.[316]

Some may also argue that an amendment to the Fifth Amendment of the Constitution is a more appropriate route.[317] The issue with this approach is the sheer difficulty and rarity of the passage of an amendment or addition to a preexisting amendment.[318] Even if an amendment or an addition to an amendment makes it past the first stage of a two-thirds majority vote in Congress, it must be ratified by two-thirds of the states.[319] The process of ratification by the states can take years longer than even the route of litigation.[320] The political climate in recent years has led to large difficulties in passing bills, let alone passing and ratifying a constitutional amendment.[321] To be sure, while an amendment is more concrete and stable, the passage of one is far less certain to happen and far too distant in the future for such a pressing issue.[322]

---

315 *See, e.g.*, Mike DeBonis, Ed O'Keefe, Erica Werner & Elise Viebeck, *Government Shutdown Looms as Senate Democrats Dig in Against GOP Spending Plan*, WASH. POST (Jan. 19, 2018), https://www.washingtonpost.com/powerpost/shutdown-looms-as-senate-democrats-dig-in-against-gop-spending-plan/2018/01/19/f4370868-fccd-11e7-a46b-a3614530bd87_story.html?hpid=hp_hp-banner-main_shutdown-740am%3Ahomepage%2Fstory&utm_term=.47599fbe5a88 [https://perma.cc/4B4L-QSJW] (giving one example of the impasse that has plagued the U.S. government in recent years).

316 *See supra* notes 310–15.

317 This counterpoint to the testimonial biometrics doctrine came about through discussions with colleagues.

318 *See* Mary Frances Berry, *Amending the Constitution; How Hard It Is to Change*, N.Y. TIMES (Sept. 13, 1987), http://www.nytimes.com/1987/09/13/magazine/amending-the-constitution-how-hard-it-is-to-change.html [https://perma.cc/NB23-KHZV] (discussing how difficult it is to pass an amendment to the Constitution and the process for doing so). *See also* Eric Posner, *The U.S. Constitution Is Impossible to Amend*, SLATE (May 5, 2014), http://www.slate.com/articles/news_and_politics/view_from_chicago/2014/05/amending_the_constitution_is_much_too_hard_blame_the_founders.html [https://perma.cc/QSG3-KYUL] (opining that the Constitution is extremely difficult to amend). While Posner's interpretation may be extreme, he makes the point that our Constitution is very difficult to change, and any changes could take untold years to be ratified. The Twenty-Seventh Amendment to the Constitution took 203 years to be ratified. *See An Overview of the 27th Amendment*, LAWS.COM (2017), https://constitution.laws.com/27th-amendment [https://perma.cc/5UUN-KMXV] (providing a brief history of the Twenty-Seventh Amendment to the Constitution).

319 *See* Posner, *supra* note 318 (explaining the voting process on new amendments to the Constitution).

320 *See* sources cited *supra* note 318.

321 *See, e.g.*, DeBonis et al., *supra* note 315 (discussing the looming government shutdown as a result of Congress's inability to pass a spending bill).

322 *See* Berry, *supra* note 318 (explaining the difficulty and length of time required to pass an amendment to the Constitution).

V. CONCLUSION

Under the testimonial biometrics doctrine, a defense attorney has a strong argument to use in court. The suspect in the hypothetical posed in the introduction will be protected by the privilege against self-incrimination. The rising popularity of biometric encryption demands the need for protection from compulsion to provide a person's biometrics to unlock that person's device. The traditional role of the Fifth Amendment privilege against self-incrimination is to protect from government overreach, protect from improper means of incrimination, and maintain an adversarial system of justice. Allowing authorities to force the production of a device and its contents via the compulsion of biometric data brushes dangerously close to an inquisitorial system of justice. Not requiring the government to meet its burden of proof beyond meeting the standard for probable cause for a search warrant fails to protect individuals from government overreach.

The law is slow to react to the rapid changes in technology. This doctrine provides an opportunity for the law to maintain pace with technology. If biometric encryption continues its trend in popularity, there needs to be some limitation on the government's power to compel biometrics from a person to unlock that person's device. The testimonial biometrics doctrine provides that chance. Defense attorneys can turn to this doctrine to begin pushing courts to recognize and protect the new context in which biometrics are used. While the doctrine faces many hurdles, a talented defense attorney can begin the push to the Supreme Court's recognition of this new doctrine.

Harrison Metz[*]

---

[*] J.D. Candidate, Valparaiso University Law School (2019); B.A., Law and Society, Minors, History, Classical Studies, Purdue University (May 2016). I would first like to thank my fiancée, Bekah, for her love and support during my time at law school and the publication of this Note. I could not have gotten through these three years without her. Second, I would like to thank my family and friends for their support in this endeavor. Last, I would like to thank my colleagues in Volume 53 of the Valparaiso University Law Review. Their friendship and support made this demanding journey an enjoyable and memorable experience.