ACTIONS SPEAK LOUDER THAN WORDS: COMPELLED BIOMETRIC DECRYPTION IS A TESTIMONIAL ACT

ABSTRACT

Most Americans can open their personal device using only their finger, not to type the password, but as the password itself. Using features like Touch ID or Face ID—forms of biometric decryption—to unlock a personal device provides several benefits, including heightened information security. Yet biometric decryption has also created a modern loophole for law enforcement to erode citizens' Fifth Amendment safeguards. In the absence of Supreme Court precedent, some lower courts afford more constitutional protection to owners of password-protected devices than owners of devices protected by a biometric identifier. Consumers are thus forced to assess whether it is more important to protect their personal information or civil liberties. This Note provides legal, public policy, and constitutional theory arguments that, consistent with the original meaning of the Fifth Amendment, the public deserves both. This, however, can be secured only if courts—and, namely, the Supreme Court—afford Fifth Amendment protection to compelled biometric decryption.

INTRODUCTION

Suppose during a criminal investigation, the police lawfully seize a suspect's iPhone and have a valid warrant to search it for evidence. The police, however, are unable to execute the search warrant because the iPhone is encrypted—it requires a password to unlock the device. In response, law enforcement obtains a court order compelling the suspect to unlock the phone. The suspect then attempts to invoke her Fifth Amendment right against self-incrimination, arguing that unlocking the device would force her "to be a witness against h[er]self."[1] Is the suspect protected by the Fifth Amendment? As the law currently stands, a court's answer would depend on whether she uses her finger to type in the passcode or if her finger is the passcode itself.

Biometric decryption first integrated itself into consumer technology in 2013 when Apple's iPhone 5S offered a new security feature called Touch ID.[2] With Touch ID, the iPhone could capture high resolution photos of the user's fingerprints and then use those to unlock the device in lieu of a traditional alphanumeric password consisting of numbers, letters, and symbols.[3] Four years later, Apple unveiled Touch ID's cousin, Face ID, which uses a "TrueDepth" camera to project thousands of infrared dots onto a user's face, mapping out their unique combination of facial curvatures and creases.[4] Today, over 85% of Americans own a smartphone,[5] and most of those smartphones enable biometric security features like Touch ID or Face ID.[6] In a relatively short time span, biometric-based decryption (i.e., using a fingerprint, facial scan, iris/retina scan, voice recognition, etc. to unlock a

1. U.S. CONST. amend. V. Scenario adapted from Orin S. Kerr, *Decryption Originalism: The Lessons of* Burr, 134 HARV. L. REV. 905, 907 (2021) [hereinafter Kerr, *Decryption Originalism*].

2. Michael Price & Zach Simonetti, *Defending Device Decryption Cases*, CHAMPION, July 2019, at 42, 44.

3. Rene Ritchie, *How Touch ID Works: Making Sense of Apple's Fingerprint Identity Sensor*, IMORE (April 24, 2018), https://www.imore.com/how-touch-id-works [https://perma.cc/Z4DJ-V3Z6]; David Naar, *What Are Alphanumeric Characters? The Meaning of Alphanumeric & Some Common Examples of Alphanumeric Code*, REFERENCE* (May 17, 2021), https://www.reference.com/world-view/examples-alphanumeric-characters-86117e89a44d1322 [https://perma.cc/9WGV-QDT5].

4. Katie Collins, *iPhone 12 Failed to Address How Face ID is Useless in the Age of Coronavirus*, CNET (Oct. 20, 2020, 12:24 PM), https://www.cnet.com/tech/mobile/apple-iphone-12-no-touch-id-button-face-id-useless-in-age-of-coronavirus-wearing-masks/#:~:text=Apple%20first%20introduced%20Face%20ID,made%20up%20of%20several%20components [https://perma.cc/CH3P-6N4W].

5. *Mobile Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/ [https://perma.cc/7ZEE-7H44].

6. Justina Alexandra Sava, *Biometric-Enabled Active Phones in North America, Western Europe & APAC 2016–2020*, STATISTA (Oct. 6, 2022), https://www.statista.com/statistics/1226088/north-america-western-europe-biometric-enabled-phones/ [https://perma.cc/PD99-BVK9].

device[7]) has become ubiquitous in consumer technology, meaning many Americans now unlock their phone with their finger, not by typing in a passcode, but as the passcode itself.

The benefits biometric passwords provide in the way of convenience and enhanced data security have come at an unexpected cost.[8] In the previous hypothetical scenario, if the suspect's iPhone requires an alphanumeric password, she is likely eligible for Fifth Amendment protection.[9] If the suspect's iPhone requires a biometric password, however, in many jurisdictions, she would be ineligible for Fifth Amendment protection.[10] Legislative Attorney Michael A. Foster encapsulates the situation well: "Courts have reached conflicting conclusions [regarding] compelled decryption [and] the Fifth Amendment. And perhaps counterintuitively, the trend appears to favor recognizing more constitutional protection for password-protected devices than for devices protected by a biometric identifier."[11] As a result, the legal issue of compelled biometric decryption—where a suspect is forced (e.g., by court order) to unlock her device using a biometric identifier (e.g., a fingerprint)—"presents the twenty-first-century citizen with a disclosure quandary: . . . information security or constitutional protection . . . ."[12]

In the absence of Supreme Court precedent, lower courts have struggled to apply outdated caselaw to these novel legal issues, and they must operate without a "consistent unified theory" to settle disagreements on "how these cases should be decided."[13] Because this technology has been "integrated into everyday life"[14] and has created modern loopholes in traditional constitutional safeguards, the need for Supreme Court guidance grows increasingly urgent. This Note argues that the public deserves both information security and constitutional protection, which can be secured only if courts—and, namely, the Supreme Court—afford Fifth Amendment protection to compelled biometric decryption.

---

7. *What Is Biometrics?: FAQs*, BIOMETRICS INST., https://www.biometricsinstitute.org/what-is-biometrics/faqs/ [https://perma.cc/X28A-CQSS] (last visited Jan. 24, 2023).

8. BIOMETRIC SECURITY vii (David Check Ling Ngo, Andrew Beng Jin Teoh & Jiankun Hu eds., 2015).

9. *See* discussion *infra* Section II.A.

10. *See* discussion *infra* Section II.B.

11. MICHAEL A. FOSTER, CONG. RSCH. SERV., LSB10416, CATCH ME IF YOU SCAN: CONSTITUTIONALITY OF COMPELLED DECRYPTION DIVIDES THE COURTS 1 (2020).

12. Ariel N. Redfern, Comment, *Face It—The Convenience of a Biometric Password May Mean Forfeiting Your Fifth Amendment Rights*, 125 PENN ST. L. REV. 597, 624 (2021) (citing Seo v. State, 109 N.E.3d 418, 438–39 (Ind. Ct. App. 2018), *transfer granted*, *opinion vacated*, 119 N.E.3d 90 (Ind. 2018)).

13. Aloni Cohen & Sunoo Park, *Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries*, 31 HARV. J.L. TECH. 169, 174 (2018); *see* discussion *infra* Part II.

14. Redfern, *supra* note 12, at 601.

Following the Introduction, Part I provides an overview of Fifth Amendment jurisprudence. This includes the three required elements to invoke one's Fifth Amendment privilege (compelled, incriminating, and, most importantly, testimonial);[15] two key Supreme Court precedents—act of production doctrine (testimonial) (*Fisher v. United States*)[16] and physical-trait evidence (nontestimonial) (*Schmerber v. California*)[17]; a highly influential analogy (*United States v. Hubbell*)[18] that compares compelled decryption to either producing a "combination to a safe" (testimonial) or a "key to a [lock]" (nontestimonial);[19] and the gaps in Supreme Court precedent that currently leave lower courts struggling to apply outdated legal tools to novel constitutional issues.

Part II illustrates how the legal issue of compelled biometric decryption lies at the intersection of *Fisher*'s act of production doctrine (testimonial) and *Schmerber*'s physical-trait evidence precedent (nontestimonial). While lower courts generally hold compelled production of an alphanumeric password to be testimonial,[20] lower courts are split on compelled biometric passwords, differing in how they apply *Schmerber*.[21] Some courts hold that compelled biometric decryption is nontestimonial, characterizing the biometric identifier as *Schmerber*'s physical-trait evidence and likening it to *Hubbell*'s lock-and-key analogy.[22] Other courts maintain that a biometric identifier, in the context of compelled decryption, is testimonial and distinguishable from both *Schmerber* and *Hubbell*.[23] This Note argues that courts—both lower courts and the Supreme Court—should employ the latter reasoning in deciding cases of compelled biometric decryption.

Given the lag in Supreme Court precedent, the mounting tension between constitutional rights and consumer technology, and jurisdictional splits forming along legal interpretations of biometric identifiers, it is reasonable to believe a case involving compelled biometric decryption could make its way to the Supreme Court in the near future. Part III therefore presents legal, public policy, and originalist constitutional theory arguments for why the Court should uphold the testimonial nature of compelled biometric decryption. From a legal standpoint, this Note argues three points: first, in the context of decryption, a biometric identifier is distinguishable from

15. Hiibel v. Sixth Jud. Dist. Court, 542 U.S. 177, 189 (2004).
16. 425 U.S. 391 (1976).
17. 384 U.S. 757 (1966).
18. 530 U.S. 27 (2000).
19. *Id.* at 43.
20. S*ee* discussion *infra* Section II.A.
21. *See* discussion *infra* Section II.B.
22. *See e.g.*, *In re* Search of [Redacted] Washington, D.C., 317 F. Supp. 3d 523, 535–36 (D.D.C. 2018); *see* discussion *infra* Section II.B.
23. *See, e.g.*, *In re Search of a Residence in Oakland, California*, 354 F. Supp. 3d 1010, 1016 (N.D. Cal. 2019); *see* discussion *infra* Section II.B.

physical-trait evidence because it is not the actual evidence law enforcement seeks but rather provides *access* to the evidence; second, *Hubbell*'s lock-and-key analogy is an inapposite comparison to a biometric identifier regarding its functionality and stronger connections to individual identification; and third, the act of producing a biometric identifier not only contains implicit communications, but it communicates even more than the act of producing an alphanumeric password.[24] From a public policy perspective, this Note argues three points: first, the law should not force the public to bargain away constitutional rights for enhanced information security provided by biometric passwords; second, an individual's constitutional protections should not hinge on decryption format (i.e., whether unlocking a device uses a passcode or fingerprint); and third, affirming the testimonial nature of biometric decryption restores, or at least mitigates, the disrupted "equilibrium of government power" caused by this "seismic shift[] in . . . technology."[25]

Finally, Part III also addresses the fact that if—or, rather, when—a case of compelled biometric decryption makes its way to the Supreme Court, the current makeup of the Court indicates originalism will likely drive the legal analysis.[26] This section of the Note provides an overview of originalism, the "enshrined principle" of the Fifth Amendment (*nemo tenetur prodere seipsum*, or "no one is obliged to accuse himself"[27]), and how enshrined principles are designed to capture evolving social norms. As such, the Court should reevaluate the testimonial nature of a fingerprint in the context of twenty-first-century technology and afford Fifth Amendment protection to compelled biometric decryption.[28] Ultimately, the Supreme Court should find that actions speak louder than words, and compelled biometric decryption is a testimonial act.

I. FIFTH AMENDMENT JURISPRUDENCE

The Fifth Amendment of the United States Constitution provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself."[29] While the Fifth Amendment often conjures imagery of a courtroom drama where a witness testifies on the stand during a criminal

24. *See* discussion *infra* Section III.A.

25. Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767, 791 (2019) [hereinafter Kerr, *Compelled Decryption*] ("equilibrium of government power"); Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) ("seismic shift[] in . . . technology"); *see* discussion *infra* Section III.B.

26. *See infra* note 184.

27. John H. Langbein, *The Historical Origins of the Privilege Against Self-Incrimination at Common Law*, 92 MICH. L. REV. 1047, 1072 (1994); *See* discussion *infra* Section III.C.2.

28. *See* discussion *infra* Section III.C.3.

29. U.S. CONST. amend. V.

trial, a person may invoke Fifth Amendment protection in other circumstances, such as while testifying during an investigatory proceeding (e.g., a grand jury hearing), when taken in for police questioning, and even during a deposition.[30] The Amendment's privilege against self-incrimination extends not only to "answers that would in themselves support a conviction" but also covers information that would "furnish a link in the chain of evidence" necessary to prosecute an individual for a crime.[31] Essentially, the mere possibility of criminal prosecution triggers the circumstances necessary to invoke the privileges and protections of the Fifth Amendment.[32]

A. Invoking the Fifth Amendment

After the necessary circumstances are triggered, three conditions must be satisfied for an individual to successfully assert the Fifth Amendment's privilege against self-incrimination: the individual must demonstrate that the information sought by the government is (1) compelled, (2) incriminating, and (3) testimonial.[33] First, the person must face legal compulsion to cooperate with the government.[34] Second, the compelled testimony must be incriminating, meaning that providing the requested information "could lead to the discovery of inculpatory evidence."[35] Third, the compelled conduct must be testimonial, meaning it forces a person "to disclose the contents of his own mind," thereby communicating a "factual assertion" or "convey[ing] any information to the Government."[36] While actions could be both compelled and incriminating, if the action does not assert facts, convey information, or disclose inner thoughts, the actions are considered nontestimonial and ineligible for Fifth Amendment protection.

30. "[T]he location of the self-incrimination clause in the Fifth Amendment rather than the Sixth proves that the [drafters] did not intend to restrict that clause to the criminal defendant only nor only to his trial." LEONARD W. LEVY, ORIGINS OF THE FIFTH AMENDMENT: THE RIGHT AGAINST SELF-INCRIMINATION 427 (1968). "[I]ndividuals can assert this right during a civil case" where they "believe[] that the testimony can result in self-incrimination that could expose him or her to criminal prosecution" and not just civil liability. *When Can I Assert my Fifth Amendment Right?* HG.ORG LEGAL RESOURCES, https://www.hg.org/legal-articles/when-can-i-assert-my-fifth-amendment-right-34464 [https://perma.cc/H8UD-7H5S] (last visited Jan. 25, 2023). Additionally, "[t]he right applies to both state and federal cases." *Id.*

31. Hoffman v. United States, 341 U.S. 479, 486 (1951).

32. In re Seper, 705 F.2d 1499, 1501 (9th Cir. 1983).

33. Hiibel v. Sixth Jud. Dist. Court, 542 U.S. 177, 189 (2004).

34. *Id.* at 189–90.

35. Price & Simonetti, *supra* note 2, at 43. Information is incriminating when the prospect of complying with the order "establish[es] 'reasonable ground to apprehend danger to the witness from his being compelled to answer.'") *Hiibel*, 542 U.S. at 190 (quoting Brown v. Walker, 161 U.S. 591, 599–600 (1896)).

36. Doe v. United States, 487 U.S. 201, 208, 210–11 (1988).

B. Only "Testimonial" Evidence is Eligible for Fifth Amendment Protection

Because compelled production of incriminating evidence is necessary, but not sufficient, to invoke one's Fifth Amendment privilege, Fifth Amendment jurisprudence does not "proscribe the compelled production of *every* sort of incriminating evidence."[37] The Amendment's protection "applies only when the accused is compelled to make a *testimonial* communication that is incriminating."[38] The "compelled" and "incriminating" prongs are rarely in dispute.[39] Testimonial, however, is more ambiguous, lacks bright-line rules, and "has been the focus of much debate by scholars and in the courts."[40]

1. Act of Production Doctrine: Testimonial Evidence

Testimony is not just limited to oral statements such as speaking to law enforcement or answering an attorney's questions on the courtroom stand; an action can also be testimonial in nature if the act implies "tacit averments" that have "communicative aspects."[41] In other words, "complying with an order to *do* something can send a message just like complying with an order to *say* something."[42] For example, the act of raising a hand or shaking/nodding a head can communicate an answer of "yes" or "no."[43] Producing documents to comply with a court order "implicitly states, 'I think these are the documents you seek[,]' . . . expos[ing] [a] person's thoughts about the documents' existence, possession, and authenticity."[44] In the context of personal devices, entering an alphanumeric password to unlock a smartphone in compliance with a search warrant

37. Fisher v. United States, 425 U.S. 391, 408 (1976) (emphasis added).

38. *Id.*

39. "'Compelled' simply means not voluntarily given. 'Incriminating' means that the information demanded tends to show guilt or furnishes a link in a chain of evidence needed to prosecute." Peter Thomson, *The Fifth Amendment's Act of Production Doctrine: An Overlooked Shield Against Grand Jury Subpoenas Duces Tecum*, 20 FEDERALIST SOC'Y REV. 4, 5 (2019).

40. *Id.*; *see In re* Search of [Redacted] Washington, D.C., 317 F. Supp. 3d 523, 535 (D.D.C. 2018) ("[T]he line between testimonial and non-testimonial communications under the Fifth Amendment is not crystal clear.")

41. *Fisher*, 425 U.S. at 410. Professor Orin Kerr explains that complying with a government order implies "[f]irst, . . . beliefs that are necessary to comply with the order" and "[s]econd, . . . belief that the act amounts to compliance." Kerr, *Compelled Decryption*, *supra* note 25, at 772.

42. Kerr, *Compelled Decryption*, *supra* note 25, at 772. *But see* Laurent Sacharoff, *What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr*, 97 TEX. L. REV. ONLINE 63, 66 (2019) [hereinafter Sacharoff, *Response to Kerr*] (arguing "testimony" requires intentional communications and not "draw[ing] ordinary inferences" as an "inadvertent by-product of the act").

43. Kerr, *Compelled Decryption*, *supra* note 25, at 772.

44. *Id.* at 773.

implicitly communicates, "I know the password to the device," or "I know how to unlock the device."[45]

In *Fisher v. United States*, the Supreme Court developed an "act of production" doctrine to assess the level of implicit communication in a compelled act and whether such communication is testimonial in nature.[46] *Fisher* consolidated two cases in which the government compelled the production of tax documents that were held by the parties' attorneys. The attorneys then attempted to invoke attorney-client privilege as a basis for refusing to comply with the order.[47] In evaluating whether attorney-client privilege could preclude the compelled document production at issue, the Court posed a parallel hypothetical. The Court contemplated "whether the client [taxpayer] would have had a valid Fifth Amendment privilege against complying with the summons if, hypothetically, he had possessed the documents and if the summons had been directed at *him*."[48]

Initially, the answer appeared to be "no." After all, Fifth Amendment protection does not extend to previously created documents.[49] In the Court's hypothetical, the government had not compelled the taxpayer to *create* the tax documents; it was merely requiring the taxpayer to physically surrender them.[50] The Court did note, however, in this scenario, the taxpayer's compliance with the summons contained implicit communications.[51] To physically surrender the requested documents, the taxpayer implicitly communicated that (1) the requested documents did exist, (2) the requested documents were in the taxpayer's possession, and (3) the documents surrendered were, in fact, the documents requested.[52] In short, the Court found that the compelled production "expose[d] the [taxpayer]'s thoughts about the documents' existence, possession, and authenticity."[53] The Court thus carved out an exceptional circumstance: "[I]f the very act of producing the [previously created] document would itself be testimonial (and

45. *Id.* at 779.

46. *Fisher,* 425 U.S. at 410; Kerr, *Compelled Decryption*, *supra* note 25, at 772, 772 n.32.

47. *Fisher*, 425 U.S. at 393–95 (defendant taxpayers gave tax documents prepared by their accountants to their respective defense attorneys).

48. Kerr, *Compelled Decryption*, *supra* note 25, at 772 n.28 (citing *Fisher*, 425 U.S. at 402–05, 402 n.8 (Court stating it felt "obliged to inquire whether the attorney-client privilege" could apply to the documents while in the attorney's possession that would otherwise be privileged in the client's possession, and noting that "[t]he parties disagree on . . . whether an attorney may claim the [client's] Fifth Amendment privilege")).

49. Thomson, *supra* note 39, at 5 ("[T]he contents of privately held documents are not protected by the Fifth Amendment, unless the government compels their creation or requires the witness to endorse the truth of their incriminating contents."); *see Fisher*, 425 U.S. at 400–01 (clarifying that the Fifth Amendment is not a privacy safeguard; it "protects against 'compelled self-incrimination, not [the disclosure of] private information'") (quoting United States v. Nobles, 422 U.S. 225, 233 n.7 (1975)).

50. *Fisher*, 425 U.S. at 411–12.

51. *Id.* at 410.

52. *Id.*

53. Kerr, *Compelled Decryption*, *supra* note 25, at 773.

incriminating), then the suspect or witness may be able to assert a Fifth Amendment right and decline to produce the documents."[54] This became known as the act of production doctrine.

The "contours"[55] of *Fisher*'s act of production doctrine are largely defined by two subsequent Supreme Court cases: *Doe v. United States*[56] and *United States v. Hubbell*.[57] In *Doe*, the government subpoenaed records for the defendant's various offshore bank accounts.[58] The foreign banks, citing their own "bank-secrecy laws," refused to disclose the account records without the customer's consent.[59] The government then sought a court order that would compel the defendant to sign multiple consent forms to release the records.[60] The Court held that the defendant's signature, while compelled and incriminating, ultimately did not "disclose the contents of [the defendant's] mind."[61] The signature was, therefore, nontestimonial and fell outside the scope of Fifth Amendment protection.[62] *Doe* proffered two important contributions to the legal analysis of compelled biometric decryption. First, it established a Supreme Court precedent that the Fifth Amendment protects the contents of an individual's mind from compelled disclosure.[63] Second, it laid the foundation for *Hubbell*'s lock-and-key analogy that several lower courts use today to hold compelled biometric decryption as a nontestimonial act.

The lock-and-key analogy first originated in *Doe*. In his dissent, Justice Stevens argued the defendant should not have been compelled to sign the form.[64] He wrote: "[The defendant] may in some cases be forced to

54. Sacharoff, *Response to Kerr*, *supra* note 42, at 65; *see Fisher*, 425 U.S. at 428–29 (Brennan, J., concurring); Thomson, *supra* note 39, at 4 (explaining that, under the Fifth Amendment, an individual may "refuse to produce subpoenaed documents where the act of producing them is incriminating in itself, regardless of the contents of the documents")

55. James G. Thomas, *The Act of Production Doctrine*, NEAL & HARWELL ATTORNEYS AT LAW (Feb. 14, 2017), https://www.nealharwell.com/blog/the-act-of-production-doctrine/ [https://perma.cc/35CA-6FDJ].

56. 487 U.S. 201 (1988).

57. 530 U.S. 27 (2000).

58. *Doe*, 487 U.S. at 202–03.

59. *Id.* at 203.

60. *Id.*

61. *Id.* at 211 (quoting Curcio v. United States, 354 U.S. 118, 128 (1957)). The Court remarked the court order ("consent directive") was "carefully drafted" in that it spoke only "in the "hypothetical." *Id.* at 215. For example, the order "did not assert any facts by requesting information on any accounts Doe 'may' be associated with, [or] specify[] from which bank [the records may have been obtained]." Raila Cinda Brejt, Note, *Abridging the Fifth Amendment: Compelled Decryption, Passwords, & Biometrics*, 31 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1154, 1173 (2021). Brejt argues that *Doe* is distinguishable "from the direct and personal surrender of evidence provided by biometric decryption, which communicates that the evidence on the device was placed there by the individual with matching physical features." *Id.* at 1173.

62. *Doe*, 487 U.S. at 215.

63. *Id.* at 210–11.

64. *Id.* at 219–21 (Stevens, J., dissenting).

surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe—by word or deed."[65] This sentiment—that surrendering a physical key was nontestimonial but disclosing a safe combination was testimonial—was echoed by the majority in dicta in a footnote.[66] Twelve years later, when writing the majority opinion in *Hubbell*, Justice Stevens cited the same *Doe* footnote: "The assembly of those documents was like telling an inquisitor the *combination to a wall safe* [testimonial], not like being forced to *surrender the key* to a strongbox [nontestimonial]."[67] While the Court's decision in *Hubbell* is cited more for expanding and shaping government workarounds to Fifth Amendment protection,[68] the opinion also cemented as Supreme Court precedent Justice Stevens's lock-and-key analogy for evaluating the testimonial nature of acts of compelled production.

Lower courts today often cite the *Hubbell* analogy when holding compelled biometric decryption as nontestimonial.[69] According to these courts, disclosing an alphanumeric password is akin to disclosing the combination to a safe, and therefore testimonial, because it entails disclosing the contents of one's mind.[70] These courts hold that disclosing a biometric feature, on the other hand, is akin to disclosing the key to a lock, making it nontestimonial and outside Fifth Amendment protection.[71]

2. Act of Production Doctrine: Gap in Supreme Court Precedent

While *Fisher*, *Doe*, and *Hubbell* grappled with the compelled production of documents, the legal issue before courts today is the compelled production of *the means to decrypt* a personal device. And yet, the primary tool available—the act of production doctrine—was developed over forty-five years ago and has not been updated in over twenty years. Furthermore,

65. *Id.* at 219 (Stevens, J., dissenting).

66. *Id.* at 210 n.9. The majority maintained that the defendant's "compulsion is more like 'be[ing] forced to surrender a key to a strongbox containing incriminating documents' than it is like 'be[ing] compelled to reveal the combination to [petitioner's] wall safe.'" *Id.* (alterations in original).

67. United States v. Hubbell, 530 U.S. 27, 43 (citing *Doe*, 487 U.S. at 210 n.9) (emphasis added).

68. *See* discussion on the "foregone conclusion" doctrine *infra* Section III.B.3.

69. *See, e.g.*, *In re* Search Warrant No. 5165, 470 F. Supp. 3d 715, 729 (E.D. Ky. 2020) ("Files found on a device accessed by a target's biometrics [has no] greater legal effect than files found in a target's desk drawer accessed by a key on the target's keyring."); *In re* Search Warrant Application for the Cellular Telephone in United States v. Barrera, 415 F. Supp. 3d 832, 839 (N.D. Ill. 2019) (establishing that a "key question[]" was "whether the biometric unlock is more like a key than a combination," and then holding that "the biometric unlock procedure is more akin to a key than a passcode combination"); *In re* Search of: A White Google Pixel Cellphone in a Black Incipio Case, 398 F. Supp. 3d 785, 791 (D. Idaho 2019) ("The same principle applies here: a person generally cannot be compelled to disclose the passcode (like the safe's combination) but can be compelled to provide the fingerprint (like the key to the safe).").

70. *See* discussion *infra* Section II.A.

71. *See* discussion *infra* Section II.B.

that tool is limited to only document production, rather than the production of an alphanumeric password, let alone a biometric identifier. Lower courts need updated, relevant Supreme Court guidance.

The gap in Supreme Court precedent, however, is not for lack of eligible cases and opportunity. In fact, a 2020 New Jersey Supreme Court case, *State v. Andrews*,[72] provided the United States Supreme Court with an opportunity to clarify how the act of production doctrine applies to compelled production of alphanumeric passwords to decrypt personal devices. In *Andrews*, the State could not execute its search warrant to retrieve incriminating text messages and call records from the defendant's iPhone 5S and iPhone 6 Plus because it lacked the passcodes to decrypt the devices.[73] When the State moved to compel Andrews (the defendant) to share his passcodes, Andrews tried to invoke "privilege against self-incrimination."[74] The trial court held, however, that compelled password disclosure was nontestimonial and therefore outside the scope of Fifth Amendment protection.[75] Andrews subsequently appealed.[76]

On each of Andrews's appeals, both the Appellate Division and the Supreme Court of New Jersey drew upon *Fisher* to hold that password production was indeed testimonial.[77] The Appellate Court reasoned "[t]he act of produc[tion] itself"—like entering a passcode—can be testimonial because it "may communicate incriminatory statements."[78] The Supreme Court of New Jersey reiterated that testimonial communications "may take any form"[79] so long as they "imply assertions of fact."[80] In the defendant's case, "[c]ommunicating or entering [his] passcode" was a "testimonial act of production" in that it disclosed the contents of his mind.[81] Yet both courts ultimately held the password production fell outside Fifth Amendment protection under the foregone conclusion exception—a Fifth Amendment government workaround discussed later in the Note.[82]

72. 234 A.3d 1254 (N.J. 2020), *cert. denied*, 141 S. Ct. 2623 (2021).
73. State v. Andrews, 197 A.3d 200, 203 (N.J. Sup. Ct. App. Div. 2018), *aff'd*, 234 A.3d 1254 (2020).
74. *Andrews*, 197 A.3d at 203.
75. *Id.* at 203–04.
76. *Id.* at 204.
77. *Andrews*, 197 A.3d at 205; 234 A.3d at 1274.
78. *Andrews*, 197 A.3d at 204 (quoting Fisher v. United States, 425 U.S. 391, 410 (1976)) (alterations in original).
79. *Andrews*, 234 A.3d at 1265 (citing Schmerber v. California, 384 U.S. 757, 763–64 (1966)).
80. *Id.* (quoting Doe v. United States, 487 U.S. 201, 209 (1988)).
81. *Id.* at 1273 (drawing upon *Hubbell* to hold a "cellphone's passcode" as testimonial because it is "analogous to the combination to a safe, not a key").
82. *Andrews*, 197 A.3d at 205, 207, 209; *Andrews*, 234 A.3d at 1262, 1274–75. For discussion of the foregone conclusion doctrine, see *infra* Section III.B.3.

On January 7, 2021, Andrews filed a petition for certiorari to the Supreme Court of the United States.[83] While the ultimate legal issues in *Andrews* turned on applying the foregone conclusion, to even make a ruling on the foregone conclusion would have required the Supreme Court to make a preliminary ruling on the threshold issue of whether compelled password production to decrypt a personal device constituted a testimonial act.[84] Though such a ruling would not have eliminated the legal confusion surrounding compelled biometric decryption, it could have at least laid a relevant foundation and provided more context for lower courts in furthering the legal analysis of compelled biometric decryption. The Supreme Court, however, denied certiorari on May 17, 2021.[85]

3. Physical Traits: Non-Testimonial Evidence

For information to be protected by the Fifth Amendment, it must be compelled, incriminating, and testimonial. While certain communications may be both compelled and incriminating, if such communications do not make an assertion of fact or disclose the contents of one's mind, the communications are considered nontestimonial and ineligible for Fifth Amendment protections.[86] While compelled document production can be testimonial under the act of production doctrine, the Supreme Court has also held that the Fifth Amendment does not bar the government from compelling a person to wear a particular piece of clothing;[87] furnish a blood sample;[88] provide a handwriting exemplar or a voice exemplar;[89] or stand in a lineup.[90] In other words, if a person's body is the source of the physical

83. Petition for Writ of Certiorari, Andrews v. State, 141 S. Ct. 2623 (2021), 2021 WL 135207.

84. *Id.* The Appellate Division and the Supreme Court of New Jersey both held that password production ultimately fell outside Fifth Amendment protection under the foregone conclusion doctrine. Because the foregone conclusion doctrine is a carve-out exception to the act of production doctrine (which maintains compelled production is testimonial), both courts had to first answer the threshold question of whether the act of production even applied to producing a personal device password (which they both held it did). If the act of production didn't apply, both courts would have had no need to go through a foregone conclusion analysis. The United States Supreme Court has never ruled on the act of production as it applies to producing a personal device password; it has only addressed document production. By denying certiorari to review *Andrews*, the Supreme Court rejected an opportunity to update act of production coverage to include the production of personal device passwords.

85. *Id.*

86. *See* discussion *supra* Section I.B.

87. Holt v. United States, 218 U.S. 245 (1910).

88. Schmerber v. California, 384 U.S. 757 (1966).

89. Gilbert v. California, 388 U.S. 263 (1967); United States v. Wade, 388 U.S. 218 (1967).

90. *Wade*, 388 U.S. 218 (1967).

evidence, courts find the production of those physical traits to be nontestimonial.[91]

In an early twentieth-century case, *Holt v. United States*,[92] the Supreme Court overruled the defendant's objections to trying on a blouse during the trial as constituting self-incrimination.[93] The Court reasoned that putting the blouse on at trial was nontestimonial because Holt was furnishing his body—a physical trait—as evidence, not his thoughts.[94] The Court maintained that the Fifth Amendment prohibited "extort[ing] communications from him, not . . . his body . . . ."[95] Over fifty years later, the Supreme Court reinforced the nontestimonial nature of physical-trait evidence in *Schmerber v. California*.[96] There, the Court held forcing a suspect to furnish a blood sample did not violate the Fifth Amendment because when "compulsion . . . makes a suspect or accused the source of 'real or physical evidence,'" such compulsion is nontestimonial.[97] The Court upheld the physical-trait precedent the following year in both *Gilbert v. California*[98] and *United States v. Wade*.[99]

---

91. Kendall Howell, *The Fifth Amendment, Decryption and Biometric Passcodes*, LAWFARE (Nov. 27, 2017), https://www.lawfareblog.com/fifth-amendment-decryption-and-biometric-passcodes [https://perma.cc/ALU7-54KH] ("Courts are in relative accord that the Fifth Amendment doesn't protect against the production of physical features . . . .").

92. 218 U.S. 245 (1910). While the defendant, Holt, was on trial for murder, a question arose as to whether a blouse belonged to him. A witness testified at trial that, during the crime, the defendant put on the blouse, and it had fit him. *Id.* at 252.

93. The Court held the defendant's objection to trying on the blouse at trial to be "an extravagant extension of the Fifth Amendment." *Id.*

94. *Id.* at 252–53.

95. *Id.* at 253.

96. 384 U.S. 757 (1966). The defendant, Schmerber, crashed his car, and when police arrived, they saw signs of Schmerber's intoxication—specifically, alcohol on his breath and bloodshot, glassy eyes. While at the hospital for treatment, Schmerber refused to give a blood sample for chemical analysis. The police officer directed a doctor to take one anyway. The analysis then showed Schmerber was intoxicated beyond the legal limit, and he was tried for driving while under the influence. *Id.* at 758–59, 769.

97. *Id.* at 764.

98. 388 U.S. 263 (1967). The defendant, Gilbert, was a suspect in several robberies. During interrogation, Gilbert mentioned other robberies in which the robber used handwritten notes to demand his ransom. Gilbert then gave the agent handwriting exemplars, and they were admitted into evidence at trial. The Supreme Court held that taking a handwriting exemplar did not violate the privilege against self-incrimination because "[a] mere handwriting exemplar, in contrast to the content of what is written . . . is an identifying physical characteristic outside [Fifth Amendment] protection." *Id.* at 264–67.

99. 388 U.S. 218 (1967). The defendant, Wade, was arrested for his involvement in a bank robbery. The lineup required Wade to speak, and witnesses identified Wade as the bank robber. *Id.* at 219–20. While Wade argued the lineup violated his privilege against self-incrimination, the Supreme Court held Wade's voice exemplar did not violate the Fifth Amendment because "compelling Wade to speak within hearing distance of the witnesses . . . was not compulsion to utter statements of a 'testimonial' nature; [rather] he was required to use his voice as an identifying physical characteristic, not to speak his guilt." *Id.* at 222–23.

The Court did so, however, with both caveats and concerns. In explaining its rationale, the *Schmerber* Court distinguished in dicta the defendant's compelled blood test from other tests designed to elicit "essentially testimonial" responses.[100] Because a lie detector test, for example, ascertains "guilt or innocence on the basis of physiological responses," it would "evoke the spirit and history of the Fifth Amendment."[101] In his *Schmerber* dissent, Chief Justice Warren sharply criticized the physical-trait evidence rule's "restrictive reading of the Fifth Amendment" that not only "deprives citizens of their rights" but also creates an "instrument" to further "narrow more constitutional protections."[102] Warren then joined Justice Fortas's partial dissent in *Wade*, who also expressed disdain for *Schmerber*'s "insidious doctrine," which "encroach[ed] upon the rights of the individual."[103] These concerns ring true now more than ever in the context of compelled biometric decryption.

II. COMPELLED DECRYPTION JURISPRUDENCE

In cases of compelled biometric decryption, suspects are not only compelled to produce a means of decryption, but that means of decryption (e.g., fingerprint) also happens to be a physical trait. These cases therefore find themselves at the intersection of *Fisher*'s act of production doctrine—stating that compelled acts of production can implicitly communicate testimonial information—and *Schmerber*'s physical-trait evidence precedent—stating that, when the source of evidence is a physical trait, versus contents of the mind, that evidence is nontestimonial. Yet, lower courts have no Supreme Court guidance to navigate this legal predicament. Instead, they are left to adapt outdated doctrines—developed decades before a smartphone with Touch ID even existed—to compelled decryption of personal devices in general, let alone compelled biometric decryption.

A. Alphanumeric Passwords: Generally Testimonial

Although compelled biometric decryption is a modern dilemma, the tension between compelled decryption and the Fifth Amendment is nearly as old as our nation's founding, dating back to Aaron Burr's 1807 trial for

100. *Schmerber*, 384 U.S. at 764.
101. *Id.*
102. Redfern, *supra* note 12, at 611 n.128 (citing Schmerber v. California, 384 U.S. 757, 773–78 (1966) (Warren, C.J., dissenting)) (internal quotations omitted).
103. *Wade*, 388 U.S. at 260–62 (Fortas, J., concurring in part and dissenting in part).

charges of treason.[104] More than 200 years and several technological innovations later, Supreme Court caselaw on compelled production is not only sparse, but the Court still has yet to specifically rule on the issue of compelled decryption beyond document production and address personal devices.[105] As a result, lower courts' best attempts at applying "outdated case law" to "novel issue[s]" of modern technology[106] has produced decisions "all over the map."[107] For purposes of this Note, though, in the context of decrypting personal devices, most courts generally hold that compelled production of an alphanumeric password is testimonial within the meaning of the Fifth Amendment.[108]

B. Biometric Decryption: Lower Courts Split

Unsurprisingly, lower courts' decisions regarding compelled *biometric* decryption are even more conflicting, and a jurisdictional split has emerged. One category of courts has analogized producing a biometric identifier to

104. *See* United States v. Burr *(In re* Willie), 25 F.Cas. 38 (Marshall, Circuit Justice, C.C. Va. 1807) (No. 14692). In 1807, former Vice-President Aaron Burr was charged with treason under the Crimes Act, which enacted both the offenses of treason and misprision. *See* Crimes Act of 1790, ch. 9, § 2, 1 Stat. 112, 112 (codified as amended at 18 U.S.C. § 2382). Burr's alleged treason occurred shortly after Burr departed the Vice-Presidency, when, as a private citizen, he devised plans to lead a small army to the American frontier. President Jefferson, "convinced . . . Burr was planning to levy war against the United States . . . ordered Burr's arrest for treason." Kerr, *Decryption Originalism*, *supra* note 1, at 915. The key evidence in the trial was a letter the government believed Burr had written to his co-conspirators encrypted in cipher. The government also believed Burr's secretary, Charles Willie, had copied it and knew how to decrypt it. When asked during trial whether he had copied the letter and understood its contents, Willie asserted his Fifth Amendment privilege against self-incrimination. For if Willie could decrypt the letter, then he understood its treasonous contents, and he could be found guilty of misprision under the Crimes Act. For further analysis of the case's legal arguments and impact on American Fifth Amendment jurisprudence see Kerr, *Decryption Originalism*, *supra* note 1, at 915–24, 935–63.

105. Andrews v. State, 234 A.3d 1254 (N.J. 2020), *cert. denied*, 141 S. Ct. 2623 (2021).

106. Redfern, *supra* note 12, at 615.

107. Kerr, *Decryption Originalism*, *supra* note 1, at 907; *see also* Price & Simonetti, *supra* note 2, at 42 (noting that compelled decryption caselaw is not only "frustratingly sparse," but "the decisions that do exist deploy a variety of standards and have created a divide" in courts' decisions at both the state and federal level); Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 FORDHAM L. REV. 203, 207 (2018) (describing the application of Fifth Amendment to compelled decryption as generating a "fundamental question bedeviling courts and scholars" (footnote omitted)) [hereinafter Sacharoff, *Unlocking the Fifth Amendment*].

108. "Most courts have now concluded that [compelled password production] runs afoul of the Fifth Amendment's privilege against self-incrimination." Evan T. Barr, *Compelled Use of Biometric Identifiers to Unlock Electronic Devices*, 261 N.Y.L.J., no. 121, June 25, 2019; *see, e.g.*, State v. Johnson, 576 S.W.3d 205, 225 (Mo. Ct. App. 2019) (acknowledging that while no Missouri court had addressed whether compelled decryption of a personal device was testimonial, "the majority of cases" that "have addressed this issue" determined this act to be testimonial). *But see* FOSTER, *supra* note 11, at 2 (noting that "[c]ourts and commentators have disagreed, however, on the precise nature of those implied statements of fact [inherent in the testimonial act] . . . .").

Schmerber's nontestimonial act of furnishing a physical trait.[109] Another category, however, has used *Schmerber* to reach a different conclusion.[110] These courts distinguish furnishing a fingerprint as biometric identifier from furnishing a fingerprint as physical-trait evidence because law enforcement is not actually after the fingerprint; it is after evidence on the personal device that only the fingerprint can *make accessible*.[111] These courts further maintain that furnishing a biometric identifier contains implicit communications "routinely considered testimonial" and eligible for Fifth Amendment protection.[112] Two cases in particular reflect the divergent views on this issue.

In a 2018 case in the U.S. District Court for the District of Columbia, Magistrate Judge Harvey treated biometric identifiers as nontestimonial physical-trait evidence when the government sought a court order compelling a suspect to biometrically decrypt personal devices subject to the government's search warrant.[113] Relying on *Hubbell*'s lock-and-key analogy, Judge Harvey held compelled production of a biometric identifier was "more akin to the surrender of a safe's key than its combination" because the act would require no "revelation of the contents of the Subject's mind . . . ."[114] Judge Harvey held biometric decryption to be, "from a legal standpoint," the "functional equivalent" of furnishing nontestimonial physical-trait evidence, no different than the government taking a blood or handwriting sample.[115]

109. *See In re* Search Warrant No. 5165, 470 F. Supp. 3d 715, 734 (E.D. Ky. 2020); *In re* Search Warrant Application for the Cellular Telephone in United States v. Barrera, 415 F. Supp. 3d 832, 839 (N.D. Ill. 2019); *In re* Search of: A White Google Pixel Cellphone in a Black Incipio Case, 398 F. Supp. 3d 785, 793 (D. Idaho 2019); State v. Diamond, 905 N.W.2d 870, 875 (Minn. 2018); *In re* Search of [Redacted] Washington, D.C., 317 F. Supp. 3d 523, 535–36 (D.D.C. 2018); *In re* Search Warrant Application for [Redacted Text], 279 F. Supp. 3d 800, 803, 806–07 (N.D. Ill. 2017); Commonwealth v. Baust, 89 Va. Cir. 267, 2014 WL 10355635 (2014), at *4.

110. *See* United States v. Wright, 431 F. Supp. 3d 1175, 1187–88 (D. Nev. 2020); *In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1015–16 (N.D. Cal. 2019); United States v. Warrant, No.19-mj-71283-VKD-1, 2019 WL 4047615, at *3 (N.D. Cal. Aug. 26, 2019); *In re* Search of: A White Google Pixel 3 XL Cellphone in a Black Incipio Case, No. 1:19-mj-10441-REB, 2019 U.S. Dist. LEXIS 83300, at *8–9 (D. Idaho, June 6, 2019); *In re* Single-Family Home & Attached Garage, No. 17 M 85, 2017 WL 4563870, at *7 (N.D. Ill. Feb. 21, 2017); *In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073 (N.D. Ill. 2017).

111. *See, e.g.*, *In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1015–16 (N.D. Cal. 2019).

112. Some courts also liken the compelled production of biometric identifiers to participation in a polygraph test, which elicits "nonverbal, physiological responses." Barr, *supra* note 108 (quoting *In re* Search of a Residence in Oakland, 354 F. Supp. 3d at 1016).

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

114. *Id.* at 535–36.

115. Barr, *supra* note 108; *In re* Search of [Redacted] Washington, D.C., 317 F. Supp. 3d at 538–40.

A 2019 case in the U.S. District Court for the Northern District of California[116] reached a different conclusion. There, law enforcement sought a court order compelling any individual present at the time of the search to biometrically decrypt personal devices subject to the search warrant.[117] Magistrate Judge Westmore found that compelling a suspect "to affix their finger or thumb to a digital device" was "fundamentally different than requiring a suspect to submit to fingerprinting" because the act "far exceed[ed]" comparing a fingerprint against already existing physical evidence (e.g., fingerprints in a database or those found at a crime scene).[118] Like the 2018 D.C. District Court case, Judge Westmore also cited *Schmerber*, but did so to analogize biometric features to the exception carved out in the opinion's dicta: those "nonverbal, physiological responses elicited . . . which are used to determine guilt or innocence" and are therefore "considered testimonial."[119] When a biometric identifier successfully decrypts a device, that act testifies to the "ownership or control of the device, . . . [which] cannot be reasonably refuted."[120] This Note argues that the reasoning employed by Judge Westmore should drive courts' legal analysis when deciding cases of compelled biometric decryption.

III. COMPELLED BIOMETRIC DECRYPTION IS A TESTIMONIAL ACT AND SHOULD RECEIVE FIFTH AMENDMENT PROTECTION

When data is encrypted, the encryption process uses algorithms to encode "plaintext" information into "ciphertext"—an "unintelligible," "incomprehensible" form.[121] A decryption key then returns data back to "useable, readable form."[122] In the case of biometric decryption, when someone presses their thumb to their phone, the fingerprint does more than merely unlock the device; it also serves as the decryption key, translating the encrypted ciphertext back into plaintext.[123] Biometric decryption first embedded itself into mainstream consumer technology in 2013 when Apple's iPhone 5S offered a new security feature called Touch ID—the first of many biometric decryption keys now standard in modern personal devices.[124] The following year, Apple released its "iOS 8" operating system,

116. *In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010 (N.D. Cal. 2019).
117. *Id.* at 1013.
118. *Id.* at 1016.
119. *Id.* at 1016 (citing Schmerber v. California, 384 U.S. 757, 764 (1966)).
120. *Id.* at 1016 (reiterating that a successful biometric decryption "concedes that the phone was in the [suspect's] possession and control . . . and authenticates [the suspect's] ownership or access to the phone and all of its digital contents").
121. Price & Simonetti, *supra* note 2, at 42; Cohen & Park, *supra* note 13, at 176–77.
122. Price & Simonetti, *supra* note 2, at 42.
123. *Id.*
124. *Id.* at 44.

which provided "encryption by default"—a feature included in all "subsequent iteration[s]" of Apple products and now standard for Android devices as well.[125] While biometric decryption has now become ubiquitous in consumer technology, its legal implications on individual rights are traversing unchartered waters, since lower courts still lack Supreme Court guidance on compelled production of all passwords, both alphanumeric and biometric. Given the lag in Supreme Court precedent, the mounting tension between constitutional rights and consumer technology, and jurisdictional splits forming along legal interpretations of biometric identifiers, it is reasonable to believe a case involving compelled biometric decryption could make its way to the Supreme Court in the near future. And when it does, there are strong legal, public policy, and constitutional arguments for why the Court should adopt Judge Westmore's reasoning in holding compelled biometric decryption to be a testimonial act.

A. Legal Arguments

Given the unique elements of biometric identifiers when serving as decryption keys, from a legal standpoint, compelled biometric decryption warrants Fifth Amendment protection. First, biometric identifiers are distinguishable from *Schmerber*'s physical-trait evidence. Second, biometric identifiers fall outside the scope of *Hubbell*'s lock-and-key analogy. And third, biometric decryption does in fact reveal contents of the mind, making it a testimonial act.

1. Biometric Identifiers Are Not Physical-Trait Evidence

As Judge Westmore astutely noted, a fingerprint as a password is distinct from a fingerprint as physical evidence.[126] When law enforcement compels a suspect to produce a biometric identifier, they do not classify the identifier itself as evidence; the identifier supplies *access* to the evidence that law enforcement seeks.[127] In the context of biometric decryption, reliance on *Schmerber* to hold a biometric identifier as physical-trait evidence is misplaced. The Court should heed those decisions that recognize "compelled biometric decryption surpasses [the] pure physicality" that would traditionally exclude it from Fifth Amendment protection.[128]

125. *Id.* at 43; *see* Cohen & Park, *supra* note 13, at 171 n.5 ("Encryption by default is an increasingly common feature on popular devices.").

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

127. *Id.*

128. Redfern, *supra* note 12, at 626; *see* discussion *supra* Section II.B; sources cited *supra* note 110.

2. The Hubbell Lock-and-Key Analogy Is an Inapposite Comparison for Compelled Biometric Decryption

Admittedly, the aforementioned distinction—a physical trait as evidence versus a physical trait as a *means to retrieve* evidence—is insufficient to overcome the *Hubbell* lock-and-key analogy in finding compelled biometric decryption to be nontestimonial. One could simply argue that, like the biometric identifier, the key is also not the evidence law enforcement seeks and merely provides access to the storage unit containing the evidence. But the rudimentary and antiquated nature of the lock-and-key analogy—first conceived in 1988 and solidified as Supreme Court precedent in 2000[129]—fails to capture the modern complexity of biometric decryption.[130] First, a biometric identifier's functionality surpasses that of a key in a lock. While a key unlocks a vessel containing evidence, it has no impact on the evidence inside. In contrast, a biometric identifier both unlocks and decrypts a personal device; the identifier not only grants law enforcement access to the evidence but it also translates the evidence into readable form for law enforcement's use. Second, a biometric identifier indicates a much stronger correlation to identity, possession, and control than a key does. Keys can be easily duplicated and freely exchanged. Possessing the key to unlock a storage unit has little to no bearing on owning or controlling the evidence inside. Biometric identifiers, on the other hand, are non-repudiable and serve as "proof of property."[131] Though in practice, the correlation is not always 1:1; Touch ID does allow a device to register up to five fingerprints.[132] Yet even under those circumstances, law enforcement could still use a biometric identifier to develop a discrete set of possible identities with a level of certainty that would rarely, if ever, be achieved through a traditional key.[133] Today's devices and biometric technology are not

129. Doe v. United States, 487 U.S. 201, 210 n. 9, 219 (Stevens, J., dissenting); United States v. Hubbell, 530 U.S. 27, 43 (2000).

130. Cohen & Park, *supra* note 13, at 178–79 (noting that analogies, "when applied across disciplines," can "obscure certain details of a technical rather than legal nature" or fail to "capture every subtlety of the technical reality"); *see* discussion *supra* Part III.

131. BIOMETRIC SECURITY, *supra* note 8, at vii ("[T]he identity of the user is much more difficult to duplicate or share with others, owing to the uniqueness and non-repudiation nature of biometrics."). *But see* Price & Simonetti *supra* note 2, at 43 (acknowledging "it is possible to replicate or steal [biometric identifiers]").

132. Glenn Fleishman, *How to Add Other People's Fingerprints to Touch ID*, MACWORLD (Mar. 17, 2019, 9:00 PM), https://www.macworld.com/article/232548/how-to-add-other-peoples-fingerprints-to-touch-id.html#:~:text=Touch%20ID%20allows%20you%20to,a%20Fingerprint%20to%20enroll%20more [https://perma.cc/8RY8-P785].

133. *See* Ritchie, *supra* note 3 (noting that the additional registered fingerprints would likely belong to people in a user's inner circle such as "family members, friends, colleagues, etc.").

comparable to the basic storage equipment underlying *Hubbell*'s lock-and-key analogy and are "entitled to greater . . . protection."[134]

3. Biometric Decryption Contains Implicit Communications

Still, one could argue that biometric decryption does not entail the "contents of the mind"[135] or "mental processes"[136] inherent in testimonial acts protected by the Fifth Amendment. Courts generally hold that compelled production of an alphanumeric password does satisfy this standard[137] even if the "act of decryption does not reveal the password."[138] For example, law enforcement could hand a suspect the phone to type in the password, and the suspect could hand back the unlocked phone, never disclosing the actual password.[139] The standard—"contents of the mind" or "mental processes"—does not refer to the brain synapses that must fire to recall and enter a password; it refers to the messages that are implicitly communicated when a password successful decrypts a device. Yet, courts often misconstrue the standard in just that way, conflating it with mental exertion and decision-making.[140] Under an accurate interpretation of "contents of the mind" and "mental processes," biometric decryption contains implicit communications making it a testimonial act.

To evaluate the implicit communication in compelled biometric decryption, one must first evaluate, as a reference point, the implicit communication of entering an alphanumeric password. The act of entering an alphanumeric password has "simple testimonial significance," in that the only definitive testimony it can assert is that "the person knows the password."[141] Unlike fingerprints, a password can be shared, meaning multiple people could know the password to decrypt a device even if they

134. *In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1017 (N.D. Cal. 2019) (first citing Riley v. California, 573 U.S. 373, 384–86, 393–95 (2014); then citing Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018)).

135. *See, e.g.*, *In re* Search of: A White Google Pixel 3 XL Cellphone in a Black Incipio Case, 398 F. Supp. 3d 785, 791 (D. Idaho 2019) ("[T]he fingerprint seizure itself does not reveal the contents of the person's mind in the way that disclosure of a [passcode] would.").

136. *See, e.g.*, Commonwealth v. Baust, 89 Va. Cir. 267, 2014 WL 10355635 (2014), at *4 ("The fingerprint . . . does not require the witness to divulge anything through his mental processes.").

137. *See* discussion *supra* Section II.A.

138. Kerr, *Compelled Decryption*, *supra* note 25, at 782; *see* Sacharoff, *Response to Kerr*, *supra* note 42, at 65 (noting that neither Kerr nor the courts have disqualified that type of scenario from receiving Fifth Amendment protection).

139. Kerr, *Compelled Decryption*, *supra* note 25, at 782.

140. *See, e.g.*, *In re* Search Warrant Application for [Redacted Text], 279 F. Supp. 3d 800, 804–05 (N.D. Ill. 2017) (holding a biometric identifier could "make use of the content of the person's mind" if "the warrant required the *person* to decide which finger (or fingers) to apply. But when agents pick, the person's performance of the compelled act is not an act of communication by that person.")

141. Kerr, *Compelled Decryption*, *supra* note 25, at 779.

do not own the device or control its contents.[142] Entering a password could, at most, communicate that "the device *likely* belongs to the person [entering the password] and that the person possesses, perhaps knowingly, the files on the device."[143] In contrast, an individual's fingerprint cannot be shared under normal circumstances;[144] and only that individual (or up to five individuals) can decrypt the device,[145] meaning that particular individual more than likely owns, possesses, controls, and authenticates that device.[146] Biometric decryption therefore communicates *more* than alphanumeric password decryption. If the latter is eligible for Fifth Amendment protection, then it logically follows that the former should be as well.

B. Public Policy Arguments

As evidenced by the 1807 Burr trial, tension between compelled decryption and the Fifth Amendment is not a just a modern dilemma.[147] Chief Justice Marshall not only presided over the Burr trial but was also prominent in resolving constitutional ambiguities from the outset of our nation's founding.[148] In studying Marshall's constitutional interpretations, Professor Mike Rappaport asserts that a guiding principle underlying Marshall's reasoning is to "follow[] the unambiguous text unless an absurdity would result."[149] The following scenario provides an example:

> [T]he government obtains a search warrant to search a home for computer-stored [contraband]. . . . The search yields one computer, and that computer has an encrypted hard drive that requires a password to use . . . . [I]nvestigators obtain court orders requiring each of the three residents to [unlock the device].[150]

142. *Id.* (explaining it is entirely possible that "[o]ne person might know the device's contents but not know the password. Another person might know the password but not know the device's contents.").

143. Sacharoff, *Response to Kerr*, *supra* note 42, at 67, 69 (emphasis added) (reiterating that when someone opens a device with an alphanumeric password, the person's possession of that device is "likely—though not certain[]").

144. Hackers have, however, developed methods of forging prints, such as "reverse-engineer[ing]" them from photos or using residual prints left behind on a scanner or phone screen. Alex Hern, *Hacker Fakes German Minister's Fingerprints Using Photos of Her Hands*, GUARDIAN (Feb. 21, 2017, 1:17 PM), https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands [https://perma.cc/LBA3-37BL].

145. *See* Fleishman, *supra* note 132.

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

147. *See supra* note 104.

148. Peter J. Smith, *The Marshall Court and the Originalist's Dilemma*, 90 MINN. L. REV. 612, 614–15 (2006).

149. Mike Rappaport, Essay, *Chief Justice Marshall's Textualist Originalism*, L. & LIBERTY (Mar. 21, 2019), https://lawliberty.org/chief-justice-marshalls-textualist-originalism/ [https://perma.cc/7HEC-BVHR].

150. Kerr, *Compelled Decryption, supra* note 25, at 783.

Under some caselaw, the residents *could* invoke Fifth Amendment privilege if the device required an alphanumeric password, but they *could not* if the device required a biometric identifier. All things being equal, their constitutional protection would turn on whether the role of the finger is to type an alphanumeric password or be the password itself—an absurd result, indeed. From a public policy standpoint, caselaw will continue to produce absurd results unless biometric decryption is uniformly regarded a testimonial act.

1. Increased Information Security Should Not Decrease Constitutional Protection

Biometric passwords are superior to their alphanumeric counterparts because they provide greater privacy and security through a standardized, user-friendly platform.[151] And yet, biometric passwords can receive less constitutional protection against government intrusion than the password 123456, which consistently ranks as the least secure password and fails to protect against cybercriminal invasion.[152] To continue holding biometric decryption as nontestimonial, and thus outside the scope of the Fifth Amendment, would perpetuate an inverse relationship, whereby an individual's enhanced information security consequently weakens her constitutional protections. Citizens who wish to "use the newest technologies" to better protect their privacy and secure their information "should not have to forfeit their constitutional rights" to do so.[153]

2. Decryption Format Does Not Provide a Meaningful Legal Distinction

When courts classify compelled biometric decryption as nontestimonial, their reasoning often turns on the format of decryption.[154] But this fails to provide a meaningful legal distinction. At least one court has accounted for this in its reasoning: in holding compelled production of an alphanumeric password to be *non*testimonial, the court in *State v. Stahl* explained it did so

151. Louis Columbus, *Why Your Biometrics Are Your Best Password*, FORBES (Mar. 8, 2020, 12:38 PM), https://www.forbes.com/sites/louiscolumbus/2020/03/08/why-your-biometrics-are-your-best-password/?sh=47981f0a6c01 [https://perma.cc/KY3M-WP95]. "[S]omething you know," such as a password or PIN can be "easily stolen, guessed, or phished for," whereas "something you are"—biometrics—is "very hard to fake or duplicate." *Id.* The vulnerabilities of passwords are also exacerbated by human error, in that people use weak passwords across multiple accounts. *Id.* Ultimately, the best protection is a Multi- or Two-Factor Authentication system that incorporates biometrics. *Id.*

152. *Do Not Use: Top 15 'Worst Passwords'*, SECUREWORLD (Oct. 10, 2019, 7:50 AM), https://www.secureworld.io/industry-news/top-15-worst-passwords-list [https://perma.cc/PED7-P9J2].

153. Redfern, *supra* note 12, at 618 (citing to *In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1015 (N.D. Cal. 2019).

154. *See* discussion *supra* Section II.B; sources cited *supra* note 109.

to prevent biometrically encrypted cell phones from receiving less protection under the Fifth Amendment than alphanumeric passwords.[155] While this Note advocates that both alphanumeric and biometric passwords should receive Fifth Amendment protection, the *Stahl* court acknowledged that the two encryption methods are not so meaningfully distinct so as to receive different levels of constitutional protection.[156] To do otherwise would produce "arbitrary" and "inequitable results,"[157] leaving consumers with disparate levels of constitutional protection for reasons devoid of meaningful legal distinction.

Many courts also overlook or fail to recognize that passwords are involved in both alphanumeric and biometric decryption methods. Setting up Touch ID, for example, requires users to set a password from the outset.[158] The device then links that password to the user's unique combination of physiological features (e.g., fingerprint), which in turn decrypts the device.[159] Furthermore, when a device is restarted, Touch ID requires the owner to reenter the baseline alphanumeric password,[160] which would then make the owner eligible to invoke her Fifth Amendment privilege. A device's on/off switch serving as the gatekeeper of constitutional protection yields an absurd result as well.

3. Courts Should Seek to Restore the "Equilibrium of Government Power"

New technologies frequently disturb the "equilibrium of government power"[161] by expanding or restricting the government's reach.[162] When courts "mechanically" apply constitutional doctrine to "seismic shifts in digital technology,"[163] it leaves consumers vulnerable to the

155. 206 So. 3d 124, 135 (Fla. Dist. Ct. App. 2016) ("[W]e are not inclined to believe that the Fifth Amendment should provide greater protection to individuals who passcode protect their iPhones with letter and number combinations than to individuals who use their fingerprint as the passcode.")

156. *Id.*

157. Brejt, *supra* note 61, at 1195–96.

158. *See Use Touch ID on iPhone and iPad*, APPLE (Mar. 17, 2022), https://support.apple.com/en-us/HT201371 [https://perma.cc/NV6B-NKG9] (explaining that a user must first create a passcode before setting up TouchID on their iPhone).

159. Brejt, *supra* note 61, at 1197.

160. Vicky Carter, *What to Do If Your Passcode Is Required When iPhone Restarts*, IMOBIE (Aug. 30, 2022), https://www.imobie.com/iphone-unlocker/touch-id-requires-passcode-when-iphone-restarts.htm [https://perma.cc/65E3-HYQX].

161. Kerr, *Compelled Decryption*, supra note 25, at 791.

162. *See* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 485–89 (2011) [hereinafter Kerr, *Equilibrium*] Kerr provides several examples of how new technologies and social developments have changed "the facts . . . and therefore the facts that the [Constitution] regulates . . . ." *Id.* at 485. He argues these "new facts threaten the balance of power by changing the consequences of old rules." *Id.*

163. Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

government's "stealthy encroachment"[164] upon fundamental rights through a modern loophole. It undermines the inherent principles of that very doctrine courts purport to uphold.[165]

The concern that modern encryption technology can obstruct law enforcement from performing "its axiomatic functions of solving crime and maintaining public safety"[166] is not entirely unfounded.[167] After all, modern technology has inserted a "remarkably powerful password gate" between law enforcement and its ability to conduct routine searches founded upon probable cause, restricting the government's reach.[168] Adopting Judge Westmore's approach, however, precludes law enforcement from gaining only "*immediate* non-consensual access" to a device's contents.[169] The government still retains "a formidable array of [legal] tools," or workarounds, to expand its reach and access the information it seeks,[170] the most powerful of which is the foregone conclusion doctrine.[171]

In the same opinion that debuted the act of production doctrine, the *Fisher* Court also carved out an exception for instances of a "foregone conclusion."[172] Under the exception, if the government has enough substantive evidence—so much so that the compelled information adds nothing to the government's collective information and provides no prosecutorial advantage—the acquisition of that testimony becomes merely a matter of "surrender" and outside Fifth Amendment protection.[173] Aspects

164. Fisher v. United States, 425 U.S. 391, 417 (1976) (Brennan, J., concurring) (citing Gouled v. United States, 255 U.S. 298, 304 (1921)).

165. *Id.* (Brennan, J., concurring) ("History and principle, not the mechanical application of its wording, have been the life of the [Fifth] Amendment.").

166. Redfern, *supra* note 12, at 629.

167. *See* Kerr, *Compelled Decryption*, *supra* note 25, at 770 ("Strong encryption for everyone shifts the balance of power towards the citizen and away from the state . . . ."). *See generally* Kerr, *Equilibrium*, *supra* note 162.

168. Kerr, *Compelled Decryption*, *supra* note 25, at 790; *see* Cohen & Park, *supra* note 13, at 172–73.

169. Barr, *supra* note 108 (emphasis added); *see In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1018 (N.D. Cal. 2019).

170. Examples include the Stored Communications Act, search warrants, subpoenas, and third party doctrine. *See* Barr, *supra* note 108. Professors Kerr and Schneier also outline six categories of encryption workarounds still available to law enforcement. Orin Kerr & Bruce Schneier, *Encryption Workarounds*, 106 GEO. L.J. 989, 996–1011 (2018).

171. For a general overview of the foregone conclusion doctrine and how it applies in various contexts, see Fern L. Kletter, *Construction and Application of "Foregone Conclusion" Exception to Fifth Amendment Privilege against Self-Incrimination*, 25 A.L.R. Fed. 3d Art. 10 (2017). For an analysis of how the forgone conclusion doctrine specifically applies to smartphones, see DAVID M. NISSMAN & ED HAGEN, LAW OF CONFESSIONS § 3:19 (2d ed. 2019).

172. Fisher v. United States, 425 U.S. 391, 411 (1976); Kerr, *Compelled Decryption*, *supra* note 25, at 777 ("[T]he foregone conclusion doctrine exists to prevent suspects from exploiting the act of production doctrine . . . .").

173. *See Fisher*, 425 U.S. at 411 (citing *In re* Harris, 221 U.S. 274, 279 (1911)). *See* Kerr, *Compelled Decryption*, *supra* note 25, at 774, 778, 782 (explaining that because "the doctrine focuses

of the foregone conclusion doctrine remain uncertain,[174] and significant legal and scholarly debate exists in defining the doctrine's exact parameters.[175] While a full examination of that debate ultimately falls outside of the scope of this Note, in general, the doctrine maintains that providing a passcode can be a foregone conclusion if the State can independently show it "knows with reasonable particularity the passcode exists, is within the accused's possession or control, and is authentic."[176] By independently establishing this information, compelled production of the password offers no prosecutorial advantage to the State, which "render[s] the testimonial aspect of production—knowledge of the password—a foregone conclusion," and thereby "disarms the [Fifth Amendment's] privilege against self-incrimination."[177]

The more troubling—and often overlooked—expansion in government power has been the "stealthy encroachment" occurring not in the courtroom over search warrants, but rather during unofficial and informal interactions with law enforcement. Take the following scenario: during a peaceful protest, law enforcement detains or arrests a protestor and then asks the protestor for her phone. In the absence of a search warrant, the protestor is legally entitled to refuse consent to a search of her smartphone for information.[178] But, as some reporters note, "things [can] get legally dicey from there."[179] If an officer forces the protestor to biometrically unlock the

---

on prosecutorial advantage," the threshold question in applying the doctrine is to ask whether "the government gained a prosecutorial advantage by obtaining the [compelled] testimony").

174. *See* Kerr, *Compelled Decryption*, *supra* note 25 at 775 (noting the doctrine's "burden of proof . . . to compel documents remains surprisingly unclear").

175. Courts are clear that the burden rests with the government. *See, e.g.*, *In re* Grand Jury Proceedings, Subpoenas for Documents, 41 F.3d 377, 380 (8th Cir. 1994) ("The government . . . bears the burdens of production and proof on the questions of the authenticity, possession, and existence of the summoned documents.") (citing United States v. Rue, 819 F.2d 1488, 1493 n.4 (8th Cir. 1987)). But the cases are "murky" on "how much certainty the government must establish" and whether the burden is expressed "in terms of the specificity of the government's description . . . rather than the certainty of the government's knowledge." Kerr, *Compelled Decryption*, *supra* note 25, at 774–75.

176. State v. Stahl, 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016). The Ninth, Eleventh, and D.C. Circuits have all adopted the "reasonable particularity" standard. *See In re* Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012), United States v. Ponds, 454 F.3d 313, 320–21 (D.C. Cir. 2006); *In re* Grand Jury Subpoena, Dated April 18, 2003, 383 F.3d 905, 910 (9th Cir. 2004). Some courts use instead a standard of "clear and convincing evidence." *See, e.g.*, U.S. v. Spencer, No. 17-cr-00259-CRB-1, 2018 WL 1964588, at *3 (N.D. Cal. Apr. 26, 2018).

177. Kerr, *Compelled Decryption*, *supra* note 25, at 799. Biometric identifiers, like a fingerprint, are even more vulnerable to the foregone conclusion because the State can more clearly show it independently knows the password (a) exists, (b) is within the accused's possession and control, and (c) is authentic. *See* discussion *supra* Section III.A.3. Even if biometric decryption were given Fifth Amendment protection, it may rarely survive the foregone conclusion threshold. This is troubling and should also be addressed by the Court.

178. Patrick Lucas Austin, *Going to a Protest? Here's How to Protect Your Digital Privacy*, TIME (June 17, 2020, 5:09 PM), https://time.com/5852009/protest-digital-privacy/ [https://perma.cc/A2JE-GWK6].

179. *Id.*

device (e.g., holds the device in front of her face to activate Face ID or presses her finger on the device to activate Touch ID),[180] given the altercation's unofficial nature and the inconsistencies in biometric decryption caselaw, the protestor could not reliably expect to achieve redress after the fact.[181] In fact, the strategy of turning off one's phone (to trigger the alphanumeric passcode entry when the device restarts), or disabling Touch ID altogether, has frequently been circulated among protestors to protect against law enforcement's infringement upon their rights.[182] Affording Fifth Amendment protection to biometric decryption is crucial to counteract government overreach into both Fourth Amendment and First Amendment rights as well.

C. Constitutional Theory Arguments

If (or rather, when) a case involving compelled biometric decryption is granted certiorari by the Supreme Court, the constitutional theories to which the Justices subscribe will be a determinative factor in the outcome of the case. A majority of the current Justices—namely Justices Clarence Thomas, Samuel Alito, Neil Gorsuch, Brett Kavanaugh, and Amy Coney Barrett—have avowed a commitment or "allegiance" to "originalism in its 'original meaning' incarnation."[183] Given the current makeup of the Supreme Court Justices and the imminency of the issue, it is highly likely that an originalist perspective will drive the legal analysis.[184]

---

180. *See Attending a Protest*, SURVEILLANCE SELF-DEFENSE (June 1, 2020), https://ssd.eff.org/module/attending-protest [https://perma.cc/C36T-JZGS] (even if a protestor exercised their "right to refuse" unlocking their device, "an officer may physically force [her] to biometrically unlock [the] device").

181. S*ee* Sara Morrison, *The Police Want Your Phone Data. Here's What They Can Get—and What They Can't*, VOX (Oct. 21, 2020, 1:48 PM), https://www.vox.com/recode/2020/2/24/21133600/police-fbi-phone-search-protests-password-rights [https://perma.cc/HH6S-D8TR] (even if unlawful compelled decryption occurred, and a lawyer argued the evidence "was illegally obtained and should be suppressed, there's no guarantee they'll win").

182. *See* Meghan Jones, *Why You Should Change Your Phone Settings Before Protesting*, READER'S DIGEST (Jul. 21, 2021), https://www.rd.com/article/change-phone-settings-before-protest/ [https://perma.cc/P39F-X363].

183. Harry Litman, *Originalism, Divided*, ATLANTIC (May 25, 2021), https://www.theatlantic.com/ideas/archive/ 2021/05/originalism-meaning/618953/ [https://perma.cc/6K53-SEHW]. Several other Justices are influenced by originalism. *See, e.g.*, *Confirmation Hearing on the Nomination of Elena Kagan to Be an Associate Justice of the Supreme Court of the United States: Hearing Before the S. Comm. on the Judiciary*, 111th Cong. 62 (2010) (statement of Solicitor General Elena Kagan) ("Either way we apply what [the Framers] say, what they meant to do. So in that sense, we are all originalists.").

184. *See* Lawrence B. Solum, *Originalism Versus Living Constitutionalism: The Conceptual Structure of the Great Debate*, 113 NW. U. L. REV. 1243, 1292 (2019) [hereinafter Solum, *Originalism Versus Living*] ("With three or four originalist Justices on the Court, it becomes more likely that originalist reasoning will play a substantial role in influencing outcomes and the reasoning of the Court."); Kerr, *Decryption Originalism*, *supra* note 1, at 906.

1. Originalism

Originalism broadly argues that the meaning of each constitutional provision at the time of enactment binds future actors.[185] Substantial disagreement exists, however, in defining the theory's exact specifications, and "no single definition commands the assent of constitutional scholars."[186] A full legal analysis of "the many . . . explicit [and] implicit definitions of originalism"[187] is ultimately beyond the scope of this Note. Nonetheless, Professor Lawrence Solum argues that while "originalism" can refer to a "family" of constitutional theories,[188] they all affirm the same two underlying elements: the "Fixation Thesis"—"the meaning of the constitutional text is fixed at the time each provision is drafted"—and the "Constraint Principle"—a "constitutional practice should, at a minimum, be consistent with the original meaning."[189] Furthermore, although originalism is often associated with ideologically conservative outcomes,[190] Professor Harry Litman cautions against the superficial impression that originalism commands rigid application of "frozen" meaning "to a present-day quandary."[191] In fact, he argues, originalism "fully conceived, . . . does not foreclose" but rather "requires the possibility that the provisions of the Constitution are best interpreted to produce 'progressive' outcomes."[192] This Note argues that affording Fifth Amendment protection to the "present-day quandary" of compelled biometric decryption would be consistent with the original meaning of the Fifth Amendment.

185. Solum, *Originalism Versus Living*, *supra* note 184, at 1244–45.

186. *Id.* at 1253.

187. *Id.* (internal quotations omitted); *see, e.g.*, Litman, *supra* note 183 (differentiating the "original intent" strain of originalism with "original meaning," which seeks to uncover "what the text would reasonably have been understood to mean at the time of its enactment").

188. Solum explains that members of the originalism family could include public meaning, original intentions, original methods, and original law. Solum, *Originalism Versus Living*, *supra* note 184, at 1253. While there is "family resemblance," Solum concedes that "no one set of characteristics is shared by all the members of the family." *Id.* at 1247, 1253, 1265.

189. *Id.* at 1245. Though "penumbral cases of originalism" may exist, "the core [theories] of originalis[m] . . . satisfy [four] criteria." *Id.* at 1270 (emphasis omitted). Two criteria are "they affirm the Fixation Thesis," and "they affirm some reasonable version of the Constraint Principle . . . ." *Id.* For a description of all criteria, see *id.* at 1270–71. For all three requirements and qualifications of the Constraint Principle, see Lawrence B. Solum, The Constraint Principle: Original Meaning and Constitutional Practice 20–21 (Apr. 6, 2019) (unpublished manuscript) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2940215).

190. "Originalism . . . in its contemporary form traces back to the advocacy of a few conservative judges, most prominently Antonin Scalia, in the mid-1980s . . . ." Litman, *supra* note 183.

191. *Id.*; *see* Solum, *Originalism Versus Living*, *supra* note 184, at 1248 ("fixed meaning does not entail static doctrine").

192. Litman, *supra* note 183.

2. The "Enshrined Principle" of the Fifth Amendment

Justice Amy Coney Barrett said (through the lens of originalism) in her confirmation hearing, "[an amendment] enshrines a principle"; we then seek to "understand [that] principle as it was at the time [of the founding]" and how it is "applied to new circumstances."[193] Therefore, an originalist approach to compelled biometric decryption would first seek to define the Fifth Amendment's original meaning—its enshrined principle. Though scholars have long disagreed on the original meaning of the Fifth Amendment privilege,[194] the Justices can still draw upon several sources to discern the Fifth Amendment's original meaning.[195] The issue is further

193. *Id.* (italics removed).

194. "Much of the disagreement focuses on what role the Fifth Amendment privilege was understood to serve and when modern concepts of the privilege were established." Kerr, *Decryption Originalism*, *supra* note 1, at 909 n.16. Kerr provides an overview of several sources illustrating the Fifth Amendment's evolution, many of which are reproduced below. *Id.* (collecting sources). *See, e.g.*, LEVY, *supra* note 30, at vii–viii, 428 (asserting that our modern notions of the privilege originated from common law and the right's history, "both in England and America, proves that it was not bound by rigid definition"); Eben Moglen, *Taking The Fifth: Reconsidering the Origins of the Constitutional Privilege Against Self-Incrimination*, 92 MICH. L. REV. 1086, 1087 (1994) (asserting that the privilege was more "rhetorical than practical" during the founding period and that "early American criminal procedure reflected less tenderness toward the silence of the . . . accused than [previously thought]"); Katharine B. Hazlett, *The Nineteenth Century Origins of the Fifth Amendment Privilege Against Self-Incrimination*, 42 AM. J. LEGAL HIST. 235, 240 (1998) (explaining that legal developments in the nineteenth century greatly shaped our modern notions of the privilege); Langbein, *supra* note 27, at 1048 (arguing that our notion of a defendant asserting the privilege to not testify at trial is a relatively modern development). For an in-depth examination of the development and scope of the Fifth Amendment's Self-Incrimination Clause, see *Self-Incrimination*, JUSTIA, https://law.justia.com/constitution/us/amendment-05/07-self-incrimination.html#fn-191 [https://perma.cc/UX69-5NS9] (last visited Jan. 24, 2023).

195. Examining the *Burr* trial can be particularly instructive because it shows how prominent lawyers and Chief Justice Marshall understood the Fifth Amendment sixteen years after its ratification. Kerr, *Decryption Originalism*, *supra* note 1, at 906. From the trial, the Justices can glean two key insights. First, the arguments in *Burr* illustrate that the original meaning of the Fifth Amendment was "hotly contested and vigorously argued" from the outset of our nation's founding. *Id.* at 912, 913; *see* 1 DAVID ROBERTSON, REPORTS OF THE TRIALS OF COLONEL AARON BURR, FOR TREASON, AND FOR A MISDEMEANOR 215 (1808) [hereinafter, 1 BURR'S TR.] (statement of Williams); *id.* at 216–17 (statement of Martin); *id.* at 220 (statement of Hay). Second, the sources cited in *Burr* provide further evidence of the Amendment's common law roots. "The great rule of law, of which the cases cited are illustrations, *is this*, that a witness is not to give evidence to accuse himself of a crime." 1 BURR'S TR. 220 (first citing 1 LEONARD MACNALLY, THE RULES OF EVIDENCE ON PLEAS OF THE CROWN 256 (1802); then citing 2 WILLIAM HAWKINS, A TREATISE OF THE PLEAS OF THE CROWN 609 (6th ed. 1788)). Although "MacNally's treatise was published eleven years after the Fifth Amendment's ratification, the relevant cases and authorities from the treatise that the lawyers discussed predated the ratification of the Fifth Amendment." Kerr, *Decryption Originalism*, *supra* note 1, at 926. Additionally, a comparative analysis showed MacNally's rule statements quoted Hawkins "verbatim," which was published six years before the Fifth Amendment's ratification. *Id.* Ultimately, the Fifth Amendment's common law roots can be traced back to opposition of the oath *ex officio* in the ecclesiastical courts of thirteenth-century England, which used the oath as a form of coerced self-incrimination. John H. Wigmore, *The Privilege Against Self-Crimination; Its History*, 15 HARV. L. REV. 610, 610, 621 n.3, 623 (1902). Additionally, the Justices can reference early American federal court cases interpreting the Fifth Amendment shortly after the

complicated, however, by the fact that there exists "no exact historical analogue to [biometric] password entry."[196] Solum argues that when applying an originalist framework to a "vague or open-textured" term that lacks "bright-line rules" for application,[197] a "zone of underdeterminacy" created by the term allows for "doctrinal dynamism."[198] This Note argues that "testimonial," as it applies to the Fifth Amendment and compelled biometric decryption, is a vague, open-textured term lacking bright-line application rules, such that it invites doctrinal dynamism to navigate the zone of undeterminancy. For the purposes of this Note, the originalist arguments for the testimonial nature of compelled biometric decryption will be grounded in two key premises: (1) the Fifth Amendment privilege is regarded as "the English common law brought to a new shore,"[199] and (2) the English common law privilege was fueled by the maxim *nemo tenetur prodere seipsum*, which loosely translates to "no one is obliged to accuse himself."[200]

3. Applying the Fifth Amendment's Enshrined Principle to Modern Facts

It's nearly impossible to know how the Framers would apply the Fifth Amendment to a six-by-three-inch device that features multiple built-in cameras, internet access, storage capacity to house intimate details of our lives, and an unlocking mechanism activated by the grooves of our finger. But the practice of courts incorporating evolving social norms into their legal reasoning is "well-settled."[201] The First Amendment's free speech "doctrinal implementing rules" have adapted to new platforms for speech, such as the Internet,[202] and who qualifies as a protected speaker.[203] In Fourth

Constitution's inception. *See, e.g.*, United States v. Goosely, 25 F. Cas. 1363 (C.C.D. Va. 1800) (No. 15,230) (where Goosely was indicted for felony robbery and objected to his testimony on the principle that a witness was not bound to give any evidence which might implicate himself).

196. Kerr, *Decryption Originalism*, *supra* note 1, at 963.

197. Solum, *Originalism Versus Living*, *supra* note 184, at 1248.

198. *Id.* (citing Lawrence Solum, *Originalism and Constitutional Construction*, 82 FORDHAM L. REV. 453, 469–72 (2013) [hereinafter Solum, *Constitutional Construction*]).

199. Kerr, *Decryption Originalism*, *supra* note 1, at 925 (noting this perspective was shared by all sides of the *Burr* trial).

200. Langbein, *supra* note 27, at 1072.

201. Redfern, *supra* note 12, at 613 ("[T]he holdings, dicta, and rationale of landmark cases show that the law can accommodate an advancing society.").

202. Solum, *Originalism Versus Living*, *supra* note 184, at 1248, 1281 (citing Solum, *Constitutional Construction*, *supra* note 198, at 469–72) ("Speech via the Internet may require implementation rules that are different from those that apply to speech in public parks.").

203. Citizens United v. Fed. Election Comm'n, 558 U.S. 310 (2010). In holding that restrictions on corporate independent expenditures, and thus corporate political speech, unconstitutionally violated the First Amendment, the Court wrote, "The Framers may have been unaware of certain types of speakers or forms of communication, but that does not mean [they] are entitled to less First Amendment protection than those types . . . when the Bill of Rights was adopted." *Id.* at 353.

Amendment jurisprudence, practices deemed "reasonable in 1791" may now be "unreasonable," and thereby prohibited by modern caselaw, "not because the meaning of unreasonable search and seizure has changed but because of changes in social judgments of reasonableness."[204] The same holds true for the Eighth Amendment. The society that enacted the Eighth Amendment might not have seen branding, ear cropping, public stocks, stoning, or whipping posts as "cruel and unusual punishment," but modern society surely would today.[205] Consequently, "[s]ince 1958, the Eighth Amendment has been interpreted in accordance with the 'evolving standards of decency that mark the progress of a maturing society.'"[206] For the Fourteenth Amendment, in 1865 the Amendment's equal protection principle "didn't mandate integrated schools; for Americans in 1965, it did."[207] It's not that the meaning of "equality" changed, but rather "the social understanding of what equality required."[208] As history demonstrates, although originalism asserts that a text's "semantic meaning . . . may be fixed," originalism also affirms that the social practices captured by the text can continue to evolve.[209]

CONCLUSION

The Framers did not presume to know the extent of the terms "freedom" or "speaker" (First Amendment), "unreasonable" (Fourth Amendment), "cruel and unusual" (Eighth Amendment), "equal" (Fourteenth Amendment), or even "incriminate" or "testify" (Fifth Amendment) "in all of [their] dimensions" at the time of our founding.[210] Rather, "they entrusted to future generations a charter protecting [a] right," expecting us to continue "learn[ing] its meaning" as society evolves.[211] Testimonial communications look different today than they did 250 years ago. The Fifth Amendment enshrined an enduring principle that no one is bound to accuse themselves,

204. Litman, *supra* note 183 (emphasis omitted) (discussing the Barrett hearing and Justice Barrett's testimony endorsing social evolution as informing her "sense of originalism"). Furthermore, the Supreme Court has been willing to rethink how old constitutional doctrines apply in the modern context of technological change, especially in recognition of the *sui generis* nature of personal devices, where *sui generis* translates to "of its own kind," emphasizing uniqueness. *See Sui Generis*, THE LAW DICTIONARY, https://thelawdictionary.org/sui-generis/ [https://perma.cc/56HA-Z5JC] (last visited Jan. 25, 2023); *see, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018); Riley v. California, 573 U.S. 373, 393–95; Kyllo v. United States, 533 U.S. 27, 34–36 (2001).

205. Litman, *supra* note 183; *see generally* John D. Bessler, *The Concept of "Unusual Punishments" in Anglo-American Law: The Death Penalty as Arbitrary, Discriminatory, and Cruel and Unusual*, 13 NW. J.L. & SOC. POL'Y 307 (2018).

206. Bessler, *supra* note 205, at 314 (quoting Trop v. Dulles, 356 U.S. 86, 101 (1958)).

207. Litman, *supra* note 183.

208. *Id.*

209. *Id.* (citing Justice Barrett's confirmation hearing).

210. *Id.*

211. *Id.* (emphasis omitted) (quoting Obergefell v. Hodges, 576 U.S. 644, 644 (2015)).

"not the set of outcomes that society would have expected in 1789" to satisfy that principle.[212] Accordingly, lower courts and the Supreme Court must reevaluate the testimonial nature of a fingerprint in the context of twenty-first-century technology. Actions speak louder than words, and compelled biometric decryption is a testimonial act worthy of Fifth Amendment protection.

Aubrey Zimmerling[*]

212. *Id.*

* J.D. (2023), Washington University School of Law; B.A. (2013), Claremont McKenna College. A heartfelt thank you to each Volume 99 and Volume 100 *Law Review* Member who contributed to this piece and made its publication possible. Love and gratitude to my family and friends for all their encouragement throughout the Note and law school journey.