FACE ID AND FINGERPRINTS: MODERNIZING FIFTH AMENDMENT PROTECTIONS FOR CELL PHONES

I. INTRODUCTION

> [Y]our smartphone is much more than just a phone. It can tell a more intimate story about you than your best friend. No other piece of hardware in history, not even your brain, contains the quality or quantity of information held on your phone: it "knows" whom you speak to, when you speak to them, what you said, where you have been, your purchases, photos,

> biometric data, even your notes to yourself—and all this dating back years.[1]

For many today, a cell phone is a lifeline. It is the alarm clock that gets you off to school or work on time; the calendar that tells you what appointments to prepare for; the weather forecast that tells you what to wear; the steady stream of aggregated news, memes, and social media that gets you through the day's low points. Consider, however, the sheer amount of information that is stored on your phone and how someone perusing it could easily piece together your personality, habits, and relationships. To police, this information could offer an unnervingly piercing and insightful look into your life.

The Supreme Court has only recently begun addressing users' privacy expectations in regard to their cell phone,[2] but these limited decisions have left a lot of wiggle room for law enforcement to overstep and intrude upon private data. One such hole in the law is the extent to which the Fifth Amendment's self-incrimination privilege[3] applies to protect cell phone users from being forced to expose private data. This issue has been further complicated by the growing use of biometric technologies like fingerprint scanners and facial recognition software as cell phone security measures.[4]

In the absence of direct guidance from the Court, many lower courts have refused to afford even the barest constitutional protection against law enforcement officials' power to compel access to cell phones.[5] A cell phone contains a wealth of its user's private information, and a criminal suspect's cell phone might very well contain data linking the suspect to a crime. Because the Fifth Amendment generally acts as a bar against compelling individuals

---

1. Karina Vold, *Is Your Smartphone an Extension of Your Mind?*, MOTHERBOARD (Mar. 2, 2018, 9:00 AM), https://motherboard.vice.com/en_us/article/qvemgb/is-your-smartphone-an-extension-of-your-mind.

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

3. *See* U.S. CONST. amend. V ("nor shall [any person] be compelled in any criminal case to be a witness against himself. . . .").

4. "Biometrics are a way to measure a person's physical characteristics to verify their identity. These can include physiological traits, such as fingerprints and eyes, or behavioral characteristics, such as the unique way you'd complete a security-authentication puzzle." Kim Porter, *Biometrics and biometric data: What is it and is it secure?*, NORTON, https://us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html (last visited Apr. 14, 2019).

5. *See, e.g.*, State v. Diamond, 905 N.W. 2d 870, 875 (Minn. 2018) (refusing to extend Fifth Amendment protection to a cell phone secured by a fingerprint scanner).

to incriminate themselves, some lower courts' practice of forcing individuals to unlock secured devices is in direct contravention to the self-incrimination privilege.[6] In this Comment, I argue that this errant line of decisions misapplies Fifth Amendment doctrine and must be rejected to prevent virtually unchecked government access to cell phones, devices with which we are intimately connected.[7]

Rapid developments in biometric technology used to secure cell phones, like fingerprint scanning and facial recognition, reflect a need to extend the Fifth Amendment privilege against self-incrimination to people in possession of such devices. This Comment will anticipate how Fifth Amendment law should develop in response to the growing use of these biometric security measures. Part II discusses the Supreme Court's Fifth Amendment precedent and its treatment of the self-incrimination privilege. Part III applies this precedent to an examination of lower courts' inconsistent treatment of biometric and non-biometric access to cell phones. Finally, Part IV proposes a more uniform treatment of cell phone access altogether; namely, that all cell phones should be afforded Fifth Amendment protection, no matter how their contents are secured.

II. THE FIFTH AMENDMENT PRIVILEGE AGAINST SELF-INCRIMINATION AND ITS ATTENDANT PROTECTIONS

The Self-Incrimination Clause of the Fifth Amendment reads: "nor shall [any person] be compelled in any criminal case to be a witness against himself. . . ."[8] Compelling a criminal suspect to act as "a witness against himself"[9] involves law enforcement's use of coercive practices to extract information from the suspect, a practice that is wholly opposed by the Fifth Amendment.[10] The Self-Incrimination Clause's long jurisprudence reflects the Supreme Court's "preference for an accusatorial rather than an inquisitorial system of criminal justice," where a criminal

6. *See* U.S. CONST. amend. V.

7. For time constraint reasons, this Comment does not address the Fourth Amendment in much detail and instead focuses its analysis on the Fifth Amendment.

8. U.S. CONST. amend. V. This clause was selectively incorporated and applied to the states by *Malloy v. Hogan*, 378 U.S. 1, 6 (1964) ("We hold today that the Fifth Amendment's exception from compulsory self-incrimination is also protected by the Fourteenth Amendment against abridgment by the States.").

9. *Id.*

10. Holt v. United States, 218 U.S. 245, 252-53 (1910).

defendant cannot be compelled by the government to give self-incriminating testimony.[11] This accusatory system is based on the idea that the government alone must bear the evidentiary burden of proving a criminal defendant's guilt beyond a reasonable doubt.[12] Thus, to avoid improperly placing this burden on the defendant, the Fifth Amendment privilege against self-incrimination protects against the compelled disclosure of most testimonial communications.[13]

A. TESTIMONIAL AND NON-TESTIMONIAL COMMUNICATIONS

Although the self-incrimination privilege may occasionally shield the guilty from criminal liability, it also safeguards the innocent.[14] The privilege most often applies when the government seeks to compel a criminal defendant to produce evidence that is (1) incriminating and (2) testimonial in nature.[15] As to the first prong, the risk of incrimination from disclosure of the testimony "must be real and appreciable," rather than merely "imaginary and unsubstantial. . . ."[16] Additionally, the scope of the privilege is fairly wide.[17] It protects not only incriminating statements, but also those statements that might lead to the discovery of additional incriminating information.[18]

---

11. Murphy v. Waterfront Comm'n, 378 U.S. 52, 55 (1964); *see also* E. M. Morgan, *The Privilege Against Self-Incrimination*, 34 MINN. L. REV. 1, 4 (1949) (describing the fervent efforts of English ecclesiastical courts to compel self-incriminating testimony through "interrogatory examination[s]").

12. *Murphy*, 378 U.S. at 55.

13. Fisher v. United States, 425 U.S. 391, 409 (1976).

14. *Murphy*, 378 U.S. at 55 (quoting Quinn v. United States, 349 U.S. 155, 162 (1955)).

15. *See Fisher*, 425 U.S. at 408. Although it is most commonly seen in criminal proceedings, the privilege can be invoked "in any proceeding, civil or criminal, administrative or judicial, investigatory or adjudicatory" where "the witness reasonably believes [their testimony] could be used in a criminal prosecution or could lead to other evidence that might be so used." Kastigar v. United States, 406 U.S. 441, 445 (1972).

16. Brown v. Walker, 161 U.S. 591, 599 (1896). Thus, although an admission may technically be testimonial, its disclosure can be compelled if there is no risk of incriminating the defendant. *See* Hiibel v. Sixth Judicial Dist. Court, 542 U.S. 177, 189 (2004) ("The Fifth Amendment prohibits only compelled testimony that is incriminating"). Indeed, such a scenario would not implicate the Fifth Amendment because, without such incriminating information, the defendant would not be "compelled . . . to be a witness against himself. . . ." U.S. CONST. amend. V.

17. *See* United States v. Hubbell, 530 U.S. 27, 37 (2000).

18. *Id.*; *see also* Hoffman v. United States, 341 U.S. 479, 486 (1951) ("The [Self-Incrimination] privilege . . . not only extends to answers that would in themselves support a conviction under a . . . criminal statute but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant for a . . .

As to the second prong, a testimonial communication is one which "explicitly or implicitly" divulges information about the defendant.[19] Theoretically, if the defendant is compelled to reveal his own thoughts,[20] and those mental processes in turn disclose material, incriminating information to law enforcement, those thoughts constitute a testimonial communication.[21] The self-incrimination privilege extends to any form that a testimonial communication might take.[22] An individual's communications can obviously come in the form of spoken statements, but they may also be documented in writings, audio recordings, or through other means.[23]

The Court has recognized a difference between compelling individuals to give a purely testimonial communication that is incriminating and compelling them instead "to engage in conduct that may [itself] be incriminating."[24] Such non-testimonial acts are not protected by the privilege against self-incrimination because they do not require individuals to reveal their own thoughts or knowledge.[25] As such, law enforcement may compel their disclosure.[26] These communications take two possible forms.[27] First, a communication is non-testimonial when a criminal defendant is not forced to disclose "the contents of his or her mind."[28] Second, a communication is non-testimonial if the foregone conclusion doctrine applies.[29]

The first instance of a non-testimonial communication

---

crime."). The first prong is important to the self-incrimination analysis, but this Comment will focus especially on the second prong.

19. Doe v. United States, 487 U.S. 201, 210 (1988).

20. *Id.* at 213; *see also id.* at 211 (quoting Curcio v. United States, 354 U.S. 118, 128 (1957)) ("[T]he attempt to force [the defendant] 'to disclose the contents of his own mind' . . . implicates the Self-Incrimination Clause.").

21. The same is true if those thoughts lead law enforcement to additional incriminating information. *Id.* at 214-15.

22. *See* Schmerber v. California, 384 U.S. 757, 763-64 (1966).

23. *See* United States v. White, 322 U.S. 694, 701 (1944).

24. United States v. Hubbell, 530 U.S. 27, 34-35 (2000).

25. *See* Doe v. United States, 487 U.S. 201, 211 (1988).

26. *See, e.g.*, *Schmerber*, 384 U.S. at 765 (holding that a blood test was not a testimonial act because it was "neither petitioner's testimony nor evidence relating to some communicative act or writing by the [defendant]").

27. *See In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1345-46 (11th Cir. 2012).

28. *Id.* at 1345 (emphasis added).

29. *Id.* at 1345-46.

implicates any "real or physical evidence" from an individual,[30] like blood[31] or handwriting samples.[32] When an individual's body is the source of material evidence, that evidence will not be excluded by the privilege against self-incrimination.[33] Thus, for example, in a case involving a bank robbery where the robber had ordered a bank teller to "put the money in the bag," the defendant's privilege was not violated when he was ordered to repeat the same phrase before witnesses in a line-up.[34] Because the defendant's "body" was the source of the incriminating, material evidence—that is, his voice and features matched those of the robber—the evidence was non-testimonial and it was properly admitted.[35]

This distinction between testimonial and non-testimonial communications is puzzling considering physical evidence (like a blood sample taken from a suspect accused of driving while intoxicated) and testimony (like the suspect's admission that he has been drinking) can be equally self-incriminating. The Supreme Court, however, has rejected an interpretation of the Self-Incrimination Clause that extends protection to a person's actions or physical characteristics.[36] Accordingly, the privilege "offers no protection against compulsion to submit to fingerprinting, photographing, or measurements, to write or speak for identification, to appear in court, to stand, to assume a stance, to walk, or to make a particular gesture."[37]

The second instance of a non-testimonial communication

30. Schmerber v. California, 384 U.S. 757, 764 (1966).

31. *See id.* at 765 (holding that a compulsory blood test did not produce testimonial evidence).

32. *See* Gilbert v. California, 388 U.S. 263, 266-67 (1967) (finding that while the contents of a writing could be protected as a testimonial communication, a handwriting exemplar is not afforded the same protection because it is "an identifying physical characteristic" that is ultimately non-testimonial).

33. Holt v. United States, 218 U.S. 245, 252-53 (1910) ("[T]he prohibition of compelling a man in a criminal court to be witness against himself is a prohibition of the use of physical or moral compulsion to extort communications from him, not an exclusion of his body as evidence when it may be material."); *see also Schmerber*, 384 U.S. at 764.

34. United States v. Wade, 388 U.S. 218, 220-21 (1967).

35. *Id.* at 222-23; *see also Holt*, 218 U.S. at 252-53 (holding that, where a murderer was believed to have worn a particular blouse while executing the crime and where the court later compelled the defendant to put on the blouse, the fact that the defendant fit into the blouse was admissible because the defendant's body was the source of the evidence).

36. *See* Schmerber v. California, 384 U.S. 757, 762 (1966) ("[T]he privilege has never been given the full scope which the values it helps to protect suggest.").

37. *Id.* at 764.

deals with the foregone conclusion doctrine. Under this judicial doctrine:

> an act of production is not testimonial—even if the act conveys a fact regarding the existence or location, possession, or authenticity of the subpoenaed materials—if the Government can show with "reasonable particularity" that, at the time it sought to compel the act of production, it already knew of the materials, thereby making any testimonial aspect a "foregone conclusion."[38]

The doctrine first appeared in *Fisher v. United States*, consolidated cases involving violations of federal income tax laws.[39] Upon learning that they were under investigation, the defendants had tax documents prepared by accountants and then handed off those documents to their respective attorneys.[40] The Internal Revenue Service learned of the existence of the documents and issued subpoenas for them.[41] The defendants refused to comply with the subpoenas, arguing that production of the documents would only serve to violate their Fifth Amendment privilege against self-incrimination.[42] In ordering the documents to be turned over to the Government, the Supreme Court reasoned that, while the documents' contents included incriminating information, their production would not require the defendants to disclose self-incriminating testimonial communications.[43] The only "communication" made by the documents' production was that the documents existed and that the defendants controlled them.[44] Additionally, because the documents' "existence and location" were a "foregone conclusion"—that is, because the Government knew the documents had been drafted and that they were being held by the defendants' attorneys—the Government could compel their production.[45]

---

38. *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1345-46 (11th Cir. 2012).

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

40. *Id.*

41. *Id.*

42. *Id.* at 395.

43. *Id.* at 411.

44. *See* Fisher v. United States, 425 U.S. 391, 411 (1976) ("[T]he [defendant] adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers.").

45. *Id.* Several circuits have imposed an additional requirement that the Government must be able to describe "the location, existence, and authenticity of the purported evidence . . . with reasonable particularity." In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1344 (11th Cir. 2012). The

On its face, the distinction between testimonial and non-testimonial communications seems simple: a defendant cannot be compelled to make a confession, but compelling physical actions, like the production of documents or computer files, is fair game. Nevertheless, in the modern, tech-savvy world where more than three-quarters of Americans own a smartphone,[46] this distinction can become quickly blurred.

B. JUSTICE STEVENS'S *DOE* DISSENT: A BETTER FRAMEWORK

More than thirty years ago, long before cell phones' widespread use, Justice Stevens developed a comprehensive and straightforward framework for differentiating between testimonial and non-testimonial evidence.[47] This framework has been adopted by some lower courts in more recent cases to determine the applicability of the self-incrimination privilege to evidence seized from criminal suspects' cell phones.[48]

Doe involved a grand jury investigation of a defendant accused of fraud.[49] The grand jury subpoenaed records of the defendant's offshore bank accounts from both the defendant and his banks.[50] The defendant produced some records, but, when he was asked whether any additional records existed, he invoked his privilege against self-incrimination.[51] The banks, meanwhile, were unable to comply with the subpoena without signed consent forms from the defendant.[52] The defendant refused to sign the forms and instead argued that the physical act of signing them was a testimonial communication that would only serve to incriminate him in violation of his Fifth Amendment rights.[53] The majority determined that the consent forms were non-testimonial communications because they were carefully written so as to not reveal any direct or derivative incriminating evidence.[54] Instead,

---

Supreme Court has not adopted this "reasonable particularity" standard, but has instead required that the Government prove that it knew at least (1) that the documents existed or (2) the documents' location. *See* United States v. Hubbell, 530 U.S. 27, 45 (2000).

46. Mobile Fact Sheet, PEW RESEARCH CTR. (Feb. 5, 2018), http://www.pew internet.org/fact-sheet/mobile/.

47. *See* Doe v. United States, 487 U.S. 201, 219-20 (1988) (J. Stevens, dissenting).

48. *See*, e.g., Seo v. State, 109 N.E.3d 418, 444 (Ind. Ct. App. 2018).

49. *Doe*, 487 U.S. at 202.

50. *Id.*

51. *Id.* at 202-03.

52. *Id.* at 203.

53. *Id.* at 207.

54. Doe v. United States, 487 U.S. 201, 215 (1988).

the consent forms were simply what they purported to be: an attempt to acquire the defendant's consent for access to his bank records.[55]

Justice Stevens wrote to express his disapproval of the majority's reasoning and conclusion.[56] He found a stricter interpretation of the differences between testimonial and non-testimonial communications was more appropriate.[57] Physical evidence like fingerprints and blood samples are, of course, non-testimonial and are thus not barred by the self-incrimination privilege.[58] Here, however, the Government sought to compel the defendant to "execut[e] . . . a document that purport[ed] to convey the signer's authority."[59] This was a textbook example of testimony because it meant the defendant would be forced "to use his mind to assist the prosecution in convicting him of a crime."[60]

Justice Stevens boiled down the distinction between testimonial and non-testimonial evidence to a simple, but comprehensive, framework. A criminal suspect "may . . . be forced to surrender a key to a strongbox containing incriminating documents."[61] In such a case, the act of handing over the key to a strongbox, or chest, is a physical act that does not require the suspect to disclose his own thoughts. Instead, it requires nothing more than for the suspect to reach into his pocket and proffer the strongbox's key to law enforcement. Under those circumstances, there is theoretically no risk of self-incrimination, or at least no risk that the Court has indicated it is willing to protect. On the other hand, a criminal suspect cannot "be compelled to reveal the combination to his wall safe—by word or deed."[62] In this scenario, there is no key that can be physically handed off; the "key" in question, or the combination, must be extracted from the suspect's mind and conveyed to law enforcement. Whether the suspect verbally communicates the combination to law enforcement ("by word") or writes it down on a piece of paper ("by . . . deed"), the act of conveyance is testimonial.[63]

---

55. Doe v. United States, 487 U.S. 201, 217-18 (1988).
56. *See id.* at 219-20 (J. Stevens, dissenting).
57. *See id.* at 219 (J. Stevens, dissenting).
58. *See id.* (J. Stevens, dissenting).
59. *Id.* (J. Stevens, dissenting).
60. *See* Doe v. United States, 487 U.S. 201, 219 (1988) (J. Stevens, dissenting).
61. *Id.* (J. Stevens, dissenting).
62. *Id.* (J. Stevens, dissenting).
63. *Id.* (J. Stevens, dissenting).

The majority did not reject the dissent's key-combination framework.[64] Instead, it disagreed with Justice Stevens's conclusion that the signing of the consent forms was a testimonial act because that act did not require the defendant to convey his own thoughts.[65] In discounting that conclusion, the majority invoked the key-combination framework and concluded that the disputed act was more akin to being compelled to hand over a physical key, rather than a combination.[66]

The Court revived this framework in *United States v. Hubbell*, this time with Justice Stevens writing for the majority.[67] There, the defendant resisted complying with a grand jury subpoena to produce certain documents and instead invoked his Fifth Amendment privilege.[68] He eventually complied with the subpoena and was subsequently indicted because of the incriminating information found within the documents.[69] The Court granted certiorari in part to determine whether requiring the defendant to produce the documents would implicate a testimonial communication.[70] The Court decided in the affirmative, holding that the documents themselves, as well as the defendant's act of *producing* the documents, had testimonial implications.[71] In explaining the holding, Justice Stevens recalled his framework when he noted that the defendant's act of compiling the subpoenaed documents, instead of "being forced to surrender the key to a strongbox," was more akin to relaying "the combination to a wall safe."[72] He again rejected the Government's contrary view that the documents' production was a physical act immune to Fifth Amendment protection, particularly because of the self-incriminating testimony implicit in such an act.[73]

64. *See* Doe v. United States, 487 U.S. 201, 210 n.9 (1988).

65. *See id.*

66. *See id.*

67. *See* United States v. Hubbell, 530 U.S. 27, 29, 43 (2000).

68. *Id.* at 31.

69. *Id.*

70. *Id.* at 29-30.

71. *Id.* at 29-43. The act of producing the documents was testimonial because it required the defendant to compile "literally hundreds of pages of material," which the Court found was "the functional equivalent of the preparation of an answer to either a detailed written interrogatory or a series of oral questions at a discovery deposition." *Id.* at 41-42.

72. United States v. Hubbell, 530 U.S. 27, 43 (2000).

73. *Id.*

C. THE DRIVING FORCE BEHIND THE SELF-INCRIMINATION PRIVILEGE IS AN INDIVIDUAL'S DIGNITARY INTEREST

The key-combination framework and the Supreme Court's interpretation of the Self-Incrimination Privilege as extending to testimonial evidence both appear to be largely based on a desire to protect an individual's expectation of privacy and dignity.[74] This expectation, referred to as an individual's dignitary interest, is often invoked in conjunction with both the Fourth Amendment,[75] which acts as a bar to "unreasonable searches and seizures" by law enforcement,[76] and the Fifth Amendment,[77] which demands that courts and law enforcement alike respect an individual's "private inner sanctum of individual feeling and thought."[78] Government entities violate this interest when they fail to afford "people the respect and deference to which they are entitled by virtue of their . . . intrinsic humanity."[79]

In the context of criminal prosecutions, this dignitary interest is intended to protect the weak from abuse by the powerful.[80] The

74. Justice Stevens's *Doe* dissent invoked these interests. Doe v. United States, 487 U.S. 201, 219 (1988) (J. Stevens, dissenting). The Supreme Court has similarly honored them. *See, e.g.*, Schmerber v. California, 384 U.S. 757, 762 (1966). *But see* John D. Castiglione, *Human Dignity Under the Fourth Amendment*, 2008 WIS. L. REV. 655, 665 (2008) (indicating that the Court is willing to forego these interests in advancement of more pressing law enforcement needs).

75. *See, e.g.*, *Schmerber*, 384 U.S. at 767 ("The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State."); *see also* Kiel Brennan-Marquez & Andrew Tutt, *Offensive Searches: Toward a Two-Tier Theory of Fourth Amendment Protection*, 52 HARV. C.R.-C.L. L. REV. 103, 120 (2017) ("[T]he Court has long recognized, though seldom named, a dignitary core of Fourth Amendment protection.").

76. U.S. CONST. amend. IV.

77. *See, e.g.*, Miranda v. Arizona, 384 U.S. 436, 460 (1966). Both Amendments are so intertwined that the Supreme Court often addresses them conjointly. *See* Schmerber v. California, 384 U.S. 757, 767 (1966) ("The values protected by the Fourth Amendment thus substantially overlap those . . . the Fifth Amendment helps to protect."). *But see* Nita A. Farahany, *Incriminating Thoughts*, 64 STAN. L. REV. 351, 406 (2012) ("Mental privacy is not sacrosanct under either the Fourth or Fifth Amendment, which provide procedural safeguards but not substantive ones to adequately protect mental privacy.").

78. Couch v. United States, 409 U.S. 322, 327 (1973).

79. Jeffrey Rosen, *The Purposes of Privacy: A Response*, 89 GEO. L.J. 2117, 2125 (2001).

80. Margaret Raymond, *Looking for Trouble: Framing and the Dignitary Interest in the Law of Self-Defense*, 71 OHIO ST. L.J. 287, 326 (2010); *see also* Kiel Brennan-Marquez & Andrew Tutt, *Offensive Searches: Toward a Two-Tier Theory of Fourth Amendment Protection*, 52 HARV. C.R.-C.L. L. REV. 103, 120 (2017) ("Dignitary protections safeguard important interests in autonomy, equality, and human flourishing.").

Court notably enshrined this protection in *Miranda v. Arizona*.[81] There, it grounded the interest in maintaining a careful balance between a government's position of authority over its citizens and "the respect [it] . . . must accord to the dignity and integrity of its citizens."[82] In the Court's view, the protection afforded by the Fifth Amendment—namely, the right to decline to give self-incriminating testimony and the suppression of such testimony—guards this interest.[83] Justice Stevens similarly invoked this interest in his key-combination framework, where he equated a Fifth Amendment violation with an invasion of "the dignity of the human mind. . . ."[84] In his view, anything less than complete protection of the privilege against self-incrimination will result in the "abuse" of an individual's dignitary interest.[85]

This interest in an individual's privacy and freedom from being compelled to disclose closely-held information is in conflict with modern times, where almost seventy percent of American adults willingly publish personal information on various social media platforms.[86] Cell phones enable people to broadcast their every-day lives, from something as mundane as what they had for lunch to more sensitive topics like their political leanings.[87] With modern technological advancements and the increased ability of people to transmit their lives throughout the Internet, however, comes an increased risk of violating the sanctity of one's private life.[88] The recent decade alone has seen an increased push for stricter laws designed to guard this privacy against intrusive invasion by both the government and private entities.[89] It is

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

82. *Id.* at 460.

83. *Id.* (quoting Malloy v. Hogan, 378 U.S. 1, 8 (1964)) ("[T]he privilege is fulfilled only when the person is guaranteed the right 'to remain silent unless he chooses to speak in the unfettered exercise of his own will.'").

84. Doe v. United States, 487 U.S. 201, 219 n.1 (1988) (J. Stevens, dissenting).

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

86. Social Media Fact Sheet, PEW RESEARCH CTR. (Feb. 5, 2018), https://www.pewinternet.org/fact-sheet/social-media/.

87. *See* Lee Rainie, *Americans' complicated feelings about social media in an era of privacy concerns*, PEW RESEARCH CTR. (Mar. 27, 2018), https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/.

88. *See, e.g.*, Tiffany Hsu, *For Many Facebook Users, a 'Last Straw' That Led Them to Quit*, N.Y. TIMES (Mar. 21, 2018), https://www.nytimes.com/2018/03/21/technology/users-abandon-facebook.html.

89. *See* Fred H. Cate, *Here's a blueprint for new laws that could protect your data*, SALON (Apr. 21, 2019, 12:59 PM), https://www.salon.com/2019/04/21/heres-a-blueprint-for-new-laws-that-could-protect-your-data_partner/.

evident that maintaining protections surrounding this dignitary interest is more important today than it ever was.[90]

III. LOWER COURTS' (MIS)TREATMENT OF CELL PHONE SECURITY METHODS

According to a 2018 Pew survey, 77 percent of Americans own a smartphone.[91] People today use their phones for more than just making calls.[92] Smartphones are mobile shopping malls, dating services, and handheld entertainment devices.[93] This widespread use of these devices necessarily means that more people than ever before are walking the streets with locked cell phones, and each one presents a case ripe for Fifth Amendment review. The Supreme Court itself has recognized that modern-day cell phones contain "a cache of sensitive personal information,"[94] but the question remains as to whether the Court would be willing to extend Fifth Amendment protection to security measures used to protect these devices.

Cell phone manufacturers, meanwhile, have developed a variety of ways to lock cell phones and prevent unauthorized access, including alpha-numerical passcodes, fingerprint scanners, and facial recognition software.[95] Such security methods are necessary to protect devices that have essentially become lockboxes full of an individual's innermost thoughts, capable of incriminating the individual if revealed.[96] The following sections describe lower courts' inconsistent treatment of these security methods in the context of the Fifth Amendment privilege against self-incrimination.

---

90. *See* People v. Kramer, 706 N.E.2d 731, 734 (N.Y. 1998) ("[Technology] cannot be allowed to outpace the array of checks and balances and protections affecting these privacy intrusions, important to individuals and society at large.").

91. This is up from 35 percent in 2011. Mobile Fact Sheet, PEW RESEARCH CTR. (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/mobile/.

92. *See* Andrew Perrin, *10 facts about smartphones as the iPhone turns 10*, PEW RESEARCH CTR. (June 28, 2017), http://www.pewresearch.org/fact-tank/2017/06/28/10-facts-about-smartphones/.

93. *See id.*

94. Riley v. California, 573 U.S. 373, 395 (2014).

95. *See* Dan Seifert, *Fingerprint, face scan, or password: what's the best way to unlock your Galaxy S8?*, VERGE (Apr. 21, 2017, 8:00 AM), https://www.theverge.com/2017/4/21/15360584/samsung-galaxy-s8-unlock-face-iris-fingerprint-scanner-most-secure.

96. *See* Riley v. California, 573 U.S. 373, 375 (2014) ("[A] cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record.").

A. NON-BIOMETRIC ACCESS: ALPHA-NUMERICAL PASSCODES

Alpha-numerical passcodes are not biometrics because they do not involve an individual's "physiological [or] behavioral characteristics."[97] Although the issue of forced disclosure of a cell phone's passcode has not yet reached the Supreme Court,[98] several lower courts have held that passcodes constitute a testimonial communication.[99] Some have based their arguments at least in part on Justice Stevens's key-combination framework.[100]

The Court of Appeals of Indiana was one such court.[101] There, the defendant alleged she had been raped by a man.[102] A detective investigated her claims and, with the defendant's consent, conducted a forensic downloaded of her iPhone's contents.[103] Based on those contents, as well as information received from the alleged rapist himself, the detective concluded that the defendant had actually been stalking the man and was contacting him via her cell phone up to thirty times a day.[104] The defendant was charged with felony stalking and several other crimes.[105] The trial court issued a warrant that ordered her "to unlock (via biometric fingerprint passcode, password or otherwise) [her cell phone]," but she refused to comply and was held in contempt.[106]

On appeal, the court of appeals had to determine whether the phone's passcode constituted a testimonial communication.[107] The

---

97. Robin Feldman, *Considerations on the Emerging Implementation of Biometric Technology*, 25 HASTINGS COMM. & ENT. L.J. 653, 654 (2003). Passcodes instead involve a particular combination of letters, numbers, or both, the order and choice of which are typically decided by the user.

98. Most recently, the Court has examined the warrant requirements under the Fourth Amendment for searching a cell phone. *See* Riley v. California, 573 U.S. 373, 373 (2014)

99. *See, e.g.*, United States v. Kirschner, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) (finding that the compelled disclosure of the defendant's computer password, which "require[d] Defendant to communicate 'knowledge,'" was a testimonial communication); *see also* Commonwealth v. Baust, 89 Va. Cir. 267 (Va. Cir. Ct. 2014) (holding that compelling the defendant to disclose his cell phone passcode involved a testimonial communication).

100. *See, e.g.*, Seo v. State, 109 N.E.3d 418, 431 (Ind. Ct. App. 2018).

101. *Id.*

102. *Id.* at 420-21.

103. *Id.* at 421.

104. *Id.*

105. These other crimes included misdemeanor intimidation, misdemeanor theft, and misdemeanor harassment. Seo v. State, 109 N.E.3d 418, 421 (Ind. Ct. App. 2018).

106. *Id.* at 422.

107. *Id.* at 429.

defendant argued that the Fifth Amendment privilege applied because the passcode was contained within the contents of "her own mind. . . ."[108] Conversely, the State argued that there was a difference between compelling the defendant to speak aloud or write down her password and instead making the defendant enter the passcode into the phone herself.[109] The State asserted it could compel the defendant to unlock the phone by manually entering her passcode, as this would *not* require the defendant to reveal the passcode itself, and would instead merely constitute a non-testimonial communication.[110]

The court ultimately held that compulsory disclosure of passcodes in *any* form constitutes self-incriminating testimony and grounded this holding in Justice Stevens's framework.[111] Rather than specifically differentiating between either of the State's methods as "testimonial" or "non-testimonial," the court instead rejected the argument entirely because either method would produce the same result: an unlocked iPhone that the State could then freely peruse.[112] Indeed, either method would also result in the defendant being compelled to disclose "the contents of her mind," implicating a testimonial communication and Fifth Amendment protections, because the act of disclosure would be more analogous to divulging the combination to a safe.[113] To the court, fulfilling the State's request to compel the defendant to unlock her secured cell phone would result in a gross invasion of privacy because it would essentially recreate the contents of the defendant's own mind.[114]

In another case involving the forced disclosure of a passcode, an intoxicated minor killed one of his passengers in a car accident.[115] Police understood that the minor's phone might contain incriminating information, so they obtained an expansive warrant to scour the phone's contents.[116] When police were unable to access the passcode-protected phone, they then sought to compel

108. Seo v. State, 109 N.E.3d 418, 429 (Ind. Ct. App. 2018) (emphasis removed).

109. *Id.*

110. *See id.*

111. *Id.* at 430.

112. *Id.* at 431. Additionally, the foregone conclusion doctrine did not apply because the State did "not demonstrate[] that it [could], with reasonable particularity, identify any files or describe where they [were]" on the phone. *Id.* at 436.

113. Seo v. State, 109 N.E.3d 418, 431 (Ind. Ct. App. 2018).

114. *Id.*

115. G.A.Q.L. v. State, 257 So. 3d 1058, 1059-60 (Fla. Dist. Ct. App. 2018).

116. *Id.* at 1060.

the minor to disclose his passcode, an order the trial court granted.[117] The court of appeal reversed, citing Justice Stevens's key-combination framework.[118] In explaining the reasoning for its holding, the court of appeal, like the *Seo* court,[119] recognized that the forced disclosure of a passcode requires "prob[ing]" into an individual's mind.[120] The court of appeal refused to sanction such an intrusive act.[121]

B. BIOMETRIC ACCESS: FINGERPRINT AND FACIAL SCANNERS

Unlike alpha-numerical passcodes, which are stored in an individual's brain to be retrieved later, "[b]iometrics . . . are inherently public" because the source of the biometric identifier—a face, an iris, a fingerprint—comes from outside a person's body.[122] Biometrics have been defined broadly as "the automated recognition of individuals based on their anatomical and behavioral characteristics. . . ."[123] Although this wordy definition makes biometrics appear to be a thing of the future, the technology has actually been around for a while, albeit in less advanced forms.[124] Today, biometrics are commonly used by government organizations like the Federal Bureau of Investigation for criminal identification purposes[125] and the Department of Homeland Security for border security.[126] Private companies have also adopted biometrics to revolutionize how consumers interact with

117. G.A.Q.L. v. State, 257 So. 3d 1058, 1060 (Fla. Dist. Ct. App. 2018). Police also sought the minor's iTunes account password "because the phone could not be searched before receiving a software update from Apple's iTunes service. *Id.*

118. *Id.* at 1061.

119. Seo v. State, 109 N.E.3d 418, 431 (Ind. Ct. App. 2018).

120. *G.A.Q.L.*, 257 So. 3d at 1061.

121. *Id.* at 1065 (quashing the trial court's order to compel the minor to disclose the cell phone's passcode).

122. April Glaser, *Biometrics Are Coming, Along With Serious Security Concerns*, WIRED (Mar. 9, 2016), https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/.

123. *What is Biometrics?*, BIOMETRICS RES. GROUP, http://biometrics.cse.msu.edu/info/index.html (last visited Feb. 16, 2019).

124. April Glaser, *Biometrics Are Coming, Along With Serious Security Concerns*, WIRED (Mar. 9, 2016), https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/ ("Police have been fingerprinting for over 100 years and have used digital biometric databases since the 1980s."). The FBI has also maintained a fingerprint database since 1924. *Fingerprints and Other Biometrics*, FBI, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ (last visited Mar. 12, 2019).

125. *Fingerprints and Other Biometrics*, FBI, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ (last visited Mar. 12, 2019).

126. *Biometrics*, HOMELAND SECURITY, https://www.dhs.gov/biometrics (last visited Mar. 12, 2019).

their products.[127] On a more personal and handheld level, biometrics are more commonly recognized as fingerprint scanners and facial recognition cameras on modern cell phones.[128]

Widespread adoption of biometric technologies has caused some technology and security experts to express misgivings about the privacy risks inherent in such a shift. When Apple first adopted its fingerprint identification technology for its line of iPhones in 2013, for example, experts warned about the hazard of securing phones with a fingerprint, cautioning that it could have "unintended consequences" for criminal suspects.[129] Critics fear that adoption of biometric security measures that take stock of users' physical characteristics to unlock a device, rather than passcodes, may entirely bypass the privilege against self-incrimination.[130]

Law enforcement officials have also adopted some ethically questionable methods to access these devices.[131] In response to these methods, lower courts have unwittingly been tasked with deciphering obsolete Supreme Court precedent to decide whether

---

127. Facebook, for example has developed technology that digitally catalogs pictures of its users and uses the extracted "biometric data" from the harvested photos to suggest who should be "tagged" in newly-uploaded photos. Yana Welinder, *A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks*, 26 HARV. J.L. & TECH. 165, 172 (2012). Windows has also adopted a "user friendly" biometric technology that allows its users to bypass the passcode process entirely and log onto their computers through the company's own facial recognition software. Matt Kapko & Matthew Finnegan, *What is Windows Hello? Microsoft's biometrics security system explained*, COMPUTERWORLD (Nov. 26, 2018, 8:04 AM), https://www.computerworld.com/article/3244347/what-is-windows-hello-microsofts-biometrics-security-system-explained.html.

128. *See, e.g.*, *About Touch ID advanced security technology*, APPLE, https://support.apple.com/en-us/HT204587 (last visited Feb. 22, 2019); *see also About Face ID advanced technology*, APPLE, https://support.apple.com/en-us/HT208108 (last visited Feb. 16, 2019).

129. Marcia Hofmann, *Apple's Fingerprint ID May Mean You Can't 'Take the Fifth,'* WIRED (Sept. 12, 2013, 9:29 AM), https://www.wired.com/2013/09/the-unexpected-result-of-fingerprint-authentication-that-you-cant-take-the-fifth/.

130. *See id.*

131. In some instances, police have been known to use the fingerprints of deceased individuals, whether criminals or victims, to access their phones before the devices auto-lock and require a password. Thomas Brewster, *Yes, Cops Are Now Opening iPhones With Dead People's Fingerprints*, FORBES (Mar. 22, 2018, 10:50 AM), https://www.forbes.com/sites/thomasbrewster/2018/03/22/yes-cops-are-now-opening-iphones-with-dead-peoples-fingerprints/. Police have also contracted with private forensic technology companies to bypass the biometric security measures entirely. *See* Thomas Reed, *GrayKey iPhone unlocker poses serious security concerns*, MALWAREBYTES LABS (Mar. 15, 2018), https://blog.malwarebytes.com/security-world/2018/03/graykey-iphone-unlocker-poses-serious-security-concerns/.

compelled access to biometrics constitutes self-incriminating testimony under the Fifth Amendment. Some courts have risen to the challenge, holding in the affirmative.[132] Others have floundered.[133]

Courts that have refused to invalidate overreaching warrants seeking the contents of secured cell phones have done so because of their misplaced focus on *how* information is extracted from the subject cell phones.[134] In one such case, law enforcement sought permission to compel four individuals at a residence to press their fingers to the fingerprint scanners on their cell phones in order to unlock the devices.[135] The court reasoned that this physical act of adhering one's fingerprint to a scanner was an inherently non-testimonial act as it did not require the warrant's targets to communicate any information to law enforcement.[136] Under Supreme Court precedent as this lower court saw it, compelling criminal suspects to unlock a cell phone via biometric means did not require them to act as "witness[es]" against themselves.[137] Therefore, the Fifth Amendment protection against self-incrimination was not implicated.[138] Instead, any incriminating information revealed by the unlocked cell phone's contents was the result of the suspects "surrender[ing] a key to a safe. . . ."[139]

---

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

133. *See, e.g.*, *In re* Search Warrant Application for [redacted text], 279 F. Supp. 3d 800, 805 (N.D. Ill. 2017).

134. *See, e.g.*, *id.* (examining the act of adhering one's fingerprint to a fingerprint scanner to access a cell phone's contents).

135. *In re Search Warrant Application*, 279 F. Supp. 3d at 802.

136. *Id.* at 805. The court also noted that, pursuant to the warrant's language, the officers themselves would choose which of the suspect's fingers they would place on the scanner in an attempt to unlock the phones. This would assumedly further protect the suspects from divulging any information to law enforcement, as the suspects would not have to reveal *which* of their fingers would provide the correct fingerprint needed to access the phone. *Id.* It is worth noting that Apple iPhones—the subjects of this case's warrant—require a successful fingerprint match within five attempts; if not, the phone will auto-lock and require entry of a passcode. *About Touch ID advanced security technology*, APPLE, https://support.apple.com/en-us/HT204587 (last visited Feb. 22, 2019). Additionally, Apple's fingerprint technology can store up to five unique fingerprints. *Use Touch ID on iPhone and iPad*, APPLE SUPPORT (Oct. 1, 2018), https://support.apple.com/en-us/HT201371. If law enforcement officials have five attempts to pick out a fingerprint for each phone and the phones are capable of holding five fingerprints, then chances are the phones will easily unlock after checking each of the suspects' thumbs and pointer fingers.

137. *In re Search Warrant Application*, 279 F. Supp. 3d at 806 (quoting U.S. CONST. amend. V).

138. *Id.* at 807.

139. *Id.* at 806.

In a similar case, law enforcement sought to compel a suspect to unlock his cell phone through any of his "biometric features," including fingerprint or facial recognition.[140] Here, the court again failed to account for the information that would be revealed as a result of the phone unlocking and how such information implicates the Fifth Amendment.[141] Instead, it focused on the physical act of unlocking the cell phone and whether compelling the suspect to use his physical features, such as his face or fingerprint, would be testimonial.[142] The court reasoned that compelling the suspect to present his physical, biometric characteristics to the phone's scanner to then unlock its contents was non-testimonial, as such an act is more analogous to handing over the key to a safe.[143] According to the court, that act did not require the suspect to divulge any of the suspect's inner thoughts, nor did it communicate anything to law enforcement.[144] Therefore, the court refused to afford the suspect Fifth Amendment protection.[145]

The above courts' approach to this issue, which addresses the potential testimonial nature of biometrics by framing them in terms of the physical actions needed to access secured phones, is heedless at best because it fails to account for the wide breadth of potentially incriminating information a modern cell phone is capable of holding. Rather than emphasizing the method needed to access a given phone, courts examining biometrics should instead focus on the phone's contents themselves—the actual information the government is seeking to access. Courts employing this more thoughtful approach have identified the dignitary interest implicit in the modern-day trend towards increased digital privacy.[146]

Lower courts that have denied warrants to compel biometric access to cell phones have recognized the role that all courts must play in respecting and upholding an individual's constitutional

140. *In re* Search of [Redacted] Washington, D.C., 317 F. Supp. 3d 523, 526-27 (D.D.C. 2018).

141. *See id.* at 534.

142. *Id.*

143. *Id.* at 535.

144. *Id.* at 536.

145. *In re* Search of [Redacted] Washington, D.C., 317 F. Supp. 3d 523, 537 (D.D.C. 2018).

146. *See In re* Search of a Residence in Oakland, CA, 354 F. Supp. 3d 1010, 1014-15 (N.D. Cal. 2019) ("Citizens do not contemplate waiving their civil rights when using new technology. . . .").

rights.[147] One such right includes maintaining the same "degree of privacy" against unwanted government intrusion[148] that was expected when both the Fourth and Fifth Amendments were ratified.[149] While cell phones were admittedly an inconceivable thing of the distant future when both amendments were first adopted, it is not too much of a stretch to extend their privacy protections to modern technology. As such, these courts maintain that they must guard against undue intrusion into cell phones, as these devices are capable of "contain[ing] some of the most intimate details of an individual's life. . . ."[150]

In denying a warrant, one court identified two specific reasons to find that compelling biometric access implicates a testimonial communication.[151] First, both biometrics and alpha-numerical passcodes functionally "serve the same purpose": they secure an individual's cell phone from unwanted access.[152] Many courts have found that the disclosure of passcodes is testimony, and so it follows that utilizing biometric security features should also constitute a testimonial communication.[153] Courts that have held the opposite have done so on the grounds that biometrics involve physical acts that do not convey any inculpatory information to law enforcement.[154] Accordingly, where an individual's fingerprint is used to secure a phone, that physical act of unlocking the phone, of placing a finger on a scanner, is non-testimonial.[155] But, where the individual instead uses a passcode to secure a phone, that passcode is off-limits because its disclosure involves the individual's own knowledge.[156] This logic is frustrating and convoluted. Where one method serves to lock a phone and protect its contents and another

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

148. *Id.* (internal quotations omitted).

149. *In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073 (N.D. Ill. 2017) (suggesting that privacy concerns implicate both the Fourth and Fifth Amendment).

150. *Id.* at 1073-74.

151. *See In re Search of a Residence in Oakland*, CA, 354 F. Supp. 3d at 1015-16.

152. *Id.* at 1015.

153. *Id.* at 1016.

154. *See, e.g.*, *In re* Search Warrant Application for [redacted text], 279 F. Supp. 3d 800, 805 (N.D. Ill. 2017) ("[T]he fingerprint seizure is just that—the agents seize a finger and apply it to the sensor, and that act does not make use of the content of the person's mind.").

155. *See* Commonwealth v. Baust, 89 Va. Cir. 267, 268-69 (Va. Cir. Ct. 2014).

156. *See id.*

method does the same, they should both be treated the same for Fifth Amendment purposes.

Second, the physical act of unlocking a cell phone, even through biometric means, is an inherently testimonial act because it concedes ownership and control over the phone.[157] This point is particularly significant in cases where the subject is accused of using a cell phone to facilitate a crime and the disclosure of the phone's contents may contain digital records of the alleged crime.[158] If the subject of a warrant is compelled to place a fingerprint on or present their face before a scanner, and that scanner then recognizes either biometric feature and unlocks the phone, then that act has at least "implicitly relate[d] a factual assertion or disclose[d] information"—namely, that the suspect is the custodian of the incriminating information on the device .[159] The "physical" act of unlocking a cell phone, then, is testimonial for Fifth Amendment purposes.[160]

IV. PROPOSAL: DEMOLISH THE DISTINCTION BETWEEN BIOMETRIC AND NON-BIOMETRIC ACCESS TO CELL PHONES

This Comment proposes that courts completely forego imposing a fictional divide on biometric and non-biometric access to cell phones, as such a distinction is misguided. Addressing the testimonial nature of biometrics (or lack thereof) by examining *how* a phone is accessed appears to be a poor excuse to encourage widespread constitutional violations by law enforcement. For Fifth Amendment purposes, the relevant inquiry should not be on how a phone is accessed, but the wide breadth of information that will be revealed and the resulting effects that such access will have on a criminal suspect's privilege against self-incrimination. If courts

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

158. The subject in one particular case was accused of extorting a victim through Facebook Messenger, an online messaging service that has a dedicated cell phone app. *See id.* at 1013. Another case involved child pornography. *See In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1067 (N.D. Ill. 2017).

159. *In re Application for a Search Warrant*, 236 F. Supp. 3d at 1073 (quoting *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1342 (11th Cir. 2012)). This particular argument assumes that the prosecution would not withhold the fact that the defendant used his biometric features to unlock the phone.

160. *In re Search of a Residence in Oakland*, CA, 354 F. Supp. 3d at 1016; *see also* Doe v. United States, 487 U.S. 201, 215 (1988) (holding that a testimonial communication is one whose "form" or "execution . . . communicates any factual assertions, implicit or explicit, or conveys any information to the Government").

adopt this approach, they will quickly recognize that biometrics, although created by an individual's physical characteristics, are wholly testimonial because they both reveal potentially incriminating information and certify that such information is under the custody and control of the individual.

A. COURTS' FRAMEWORK FOR CONCLUDING THAT BIOMETRICS ARE TESTIMONIAL

Specifically, there are two avenues by which courts must find that biometrics are testimonial. First, courts should treat an individual's biometric features as if they were a cell phone's alpha-numerical passcode. Recall that many courts are now holding that compelled disclosure of a passcode involves a testimonial communication because, in disclosing the passcode, individuals must impart their own knowledge.[161] While passcodes themselves are distinctly different from the physical characteristics used to pass a biometric test—the former is typed into the phone, while the latter is a physical characteristic of the user's body that is scanned by the phone—the two should not be treated differently, as they are fundamentally the same thing.[162] Indeed, both passcodes and biometrics serve the same purpose: securing sensitive, private information on an individual's cell phone.[163]

Second, courts should treat an individual's biometric features as an incriminating and testimonial product of a physical test. Although non-testimonial communications typically include any "real or physical evidence" from an accused, dicta in *Schmerber v. California* is insightful.[164] The *Schmerber* Court noted the difficulty in drawing a bright line between testimonial and non-testimonial evidence.[165] One such instance "in which . . . a distinction is not readily drawn" involves a seemingly physical test that produces incriminating, testimonial results.[166]

In illustrating this scenario, the Court provided the example of a lie detector test.[167] Lie detector tests, also known as polygraph

161. *See supra* Section III(A).

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

163. Thomas Brewster, *Feds Force Suspect To Unlock An Apple iPhone X With Their Face*, FORBES (Sept. 20, 2018, 10:01 AM), https://www.forbes.com/sites/thomasbrewster/2018/09/30/feds-force-suspect-to-unlock-apple-iphone-x-with-their-face/.

164. Schmerber v. California, 384 U.S. 757, 764 (1966).

165. *Id.*

166. *Id.*

167. *See id.*

tests, attempt to determine whether an individual is telling the truth in response to specific questions by observing any "psychophysiological changes" in the individual.[168] The polygraph device is attached to an individual and monitors the individual's heart rate, blood pressure, and other bodily characteristics,[169] all of which easily constitute "physical evidence."[170] Based on an amalgamation of that physical evidence and the individual's responses to various questions, the examiner then attempts to infer whether the individual is lying or telling the truth.[171] Because a polygraph "measur[es] changes in body function during [an] interrogation," it is essentially a "test[] . . . directed to obtain 'physical evidence'" that nevertheless produces testimonial results.[172] The *Schmerber* Court indicated that this practice—using a physical test to produce a testimonial response—implicates the privilege against self-incrimination.[173]

In terms of biometrics, this framework works as well. When individuals affix their finger to a fingerprint scanner, that is a physical act, or a physical *test*, that unlocks the phone and produces its contents.[174] Those contents assumedly contain the individual's own knowledge or thoughts in at least some form, so they are testimonial. Additionally, as discussed earlier,[175] the fact that the individual can successfully access the phone's biometrics at least "implicitly" conveys another testimonial communication: that the individual owns or is in some way connected to the phone and its contents.[176] Thus, the physical test of unlocking the phone produces testimony that is twofold: (1) the phone's contents and (2) the identity of the phone's owner.[177]

---

168. *The Truth About Lie Detectors (aka Polygraph Tests)*, AM. PSYCHOL. ASS'N (Aug. 5, 2004), https://www.apa.org/research/action/polygraph. Although the reliability of polygraphs has been called into question, the *Schmerber* Court did not take this into consideration in giving its illustration. *See* Schmerber v. California, 384 U.S. 757, 764 (1966).

169. AM. PSYCHOL. ASS'N, *supra* note 168.

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

171. AM. PSYCHOL. ASS'N, *supra* note 168.

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

173. *Id.* ("To compel a person to submit to testing in which an effort will be made to determine his guilt or innocence on the basis of physiological responses, whether willed or not, is to evoke the spirit and history of the Fifth Amendment.").

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

175. *See supra* Section III(B).

176. *In re Application for a Search Warrant*, 236 F. Supp. 3d at 1073 (citation omitted).

177. *See id.*

B. PROTECTING RIGHTS AND PREVENTING POLICE MISCONDUCT: WHY THIS ALL MATTERS

Ultimately, the arguments for and against extending Fifth Amendment protection to biometrics are based on balancing competing interests between an individual's expectation of their own privacy and law enforcement's efforts to combat crime.[178] Those who are against extending the privilege advocate for allowing law enforcement the widest latitude possible to conduct criminal investigations.[179] It is true that denying law enforcement access to the veritable treasure trove of information contained on cell phones ultimately serves to hamper criminal investigations.[180] It is also true that many cases necessitating compelled disclosure of information on electronic devices tend to involve particularly wicked crimes like child pornography,[181] extortion,[182] and terrorism.[183] If defendants who are guilty of such crimes go free because the government cannot access incriminating, sensitive files to prove defendants' guilt beyond a reasonable doubt, then other victims may be put in danger.

The Self-Incrimination Clause, however, was intended to safeguard "our accusatory system of criminal justice," wherein the government is charged with the responsibility of accusing a suspect of a crime and then proving up that suspect's guilt.[184] Enabling the government to compel a defendant to hand over a locked cell phone

178. *See* Spano v. New York, 360 U.S. 315, 315 (1959) ("[W]e are forced to resolve a conflict between two fundamental interests of society; its interest in prompt and efficient law enforcement, and its interest in preventing the rights of its individual members from being abridged by unconstitutional methods of law enforcement.").

179. The FBI has gone as far as to call for a digital "backdoor" into cell phones to enable easier access to phones' contents. Aaron Pressman, *The Secret History of the FBI's Battle Against Apple Reveals the Bureau's Mistakes*, FORTUNE (Mar. 27, 2018), http://fortune.com/2018/03/27/fbi-apple-iphone-encryption-san-bernardino/.

180. *See* Riley v. California, 573 U.S. 373, 394 (2014) ("Even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on.").

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

182. *See, e.g.*, *In re* Search of a Residence in Oakland, CA, 354 F. Supp. 3d 1010, 1014-15 (N.D. Cal. 2019).

183. *See, e.g.*, Joel Rubin et al., *FBI unlocks San Bernardino shooter's iPhone and ends legal battle with Apple, for now*, L.A. TIMES (Mar. 28, 2016, 10:39 PM), https://www.latimes.com/local/lanow/la-me-ln-fbi-drops-fight-to-force-apple-to-unlock-san-bernardino-terrorist-iphone-20160328-story.html.

184. Miranda v. Arizona, 384 U.S. 436, 460 (1966).

full of gigabytes' worth of potentially incriminating information would essentially negate this traditional framework, thereby breaking down the adversarial justice system.

Honoring the protection afforded by the self-incrimination privilege further requires protecting criminal suspects from law enforcement's attempt to game the system. Recall that under current lower court precedent, disclosing a passcode is a testimonial communication that invokes Fifth Amendment protections.[185] Some phones, such as the Apple iPhone, have an auto-lock feature that will activate after five failed attempts to scan a biometric feature, after which the phone requires entry of a user's passcode.[186] Because of the implications of activating such a security feature—namely, that the phone will require a passcode, thereby invoking Fifth Amendment protection—technology forensic experts are now warning law enforcement officers to avoid looking at phones equipped with these features to avoid "accidentally trigger[ing] this mechanism."[187] Thus, because of lower courts' errant distinctions between biometric and non-biometric access, officers are now aware that they must keep a cell phone's biometric access open and available to use. In this way, they are able to bypass the potentially tricky matter of the testimonial nature of the phone's passcode.[188]

Another argument against extending the privilege to biometrics asserts that, "[b]efore cell phones, much of [the] information [on them] would be found in a person's home," which is accessible via a search warrant[189] or under exigent circumstances.[190] As such, if police can attain a warrant to search

185. *See supra* Section III(A).

186. *See, e.g.*, *About Touch ID advanced security technology*, APPLE, https://support.apple.com/en-us/HT204587 (last visited Feb. 22, 2019); *see also About Face ID advanced technology*, APPLE, https://support.apple.com/en-us/HT208108 (last visited Feb. 16, 2019).

187. Joseph Cox, *Cops Told 'Don't Look' at New iPhones to Avoid Face ID Lock-Out*, MOTHERBOARD (Oct. 12, 2018, 10:05 AM), https://motherboard.vice.com/en_us/article/5984jq/cops-dont-look-iphonex-face-id-unlock-elcomsoft.

188. Thomas Brewster, *Feds Force Suspect To Unlock An Apple iPhone X With Their Face*, FORBES (Sept. 20, 2018, 10:01 AM), https://www.forbes.com/sites/thomasbrewster/2018/09/30/feds-force-suspect-to-unlock-apple-iphone-x-with-their-face/.

189. Matt Hamilton & Richard Winton, *The government wants your fingerprint to unlock your phone. Should that be allowed?*, L.A. TIMES (Apr. 30, 2016, 3:00 AM), https://www.latimes.com/local/california/la-me-iphones-fingerprints-20160430-story.html.

190. *See* Mincey v. Arizona, 437 U.S. 385, 393-94 (1978) ("[W]arrants are generally required to search a person's home or his person unless 'the exigencies of the situation' make the needs of law enforcement so compelling that the warrantless search is

a suspect's home for contraband, then they should also be able to attain a warrant to compel a suspect to unlock their biometrically-secured cell phone.[191] This argument, however, fails to account for the wide breadth of information modern cell phones are capable of storing. The newest Apple iPhone, for example, can store up to 512 gigabytes of data.[192] A single gigabyte can store the equivalent of approximately 700 floppy disks' worth of information.[193] A cell phone with a 512-gigabyte storage capacity, then, can store the same amount of information as 358,400 floppy disks.[194]

Imagine storing all of your most sensitive information in a cache of more than 300,000 floppy disks, including your text messages, phone call log, Internet search history, calendar, pictures, emails, banking and credit card information, medical records, and more. You then leave those floppy disks behind the locked door of your home. You have a certain expectation of privacy with regards to maintaining the sanctity of your home against police intrusion,[195] but, as a savvy legal mind, you understand that police are able to enter your home with a valid warrant based on probable cause.[196] If police were to raid your home pursuant to a warrant in search of contraband or incriminating information, they would have the formidable task of searching through the 300,000 floppy disks.

Consider how much more easily digestible that sheer amount of information is in the form of a handheld device like your cell phone. Police could spend hours, days, or even weeks combing through the floppy disks in search of incriminating evidence. In

---

objectively reasonable under the Fourth Amendment.") (citation omitted).

191. *See* Hamilton & Winton, *supra* note 189.

192. *iPhone 11 Pro*, APPLE, https://www.apple.com/iphone-11-pro/specs/ (last visited Jan. 7, 2020).

193. Tim Fisher, *Terabytes, Gigabytes, & Petabytes: How Big Are They?*, LIFEWIRE, https://www.lifewire.com/terabytes-gigabytes-amp-petabytes-how-big-are-they-4125169 (last updated Jan. 7, 2019).

194. *See id.*

195. U.S. CONST. amend. IV; *see also* Kyllo v. United States, 533 U.S. 27, 31 (2001) ("'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.") (citation omitted).

196. U.S. CONST. amend. IV; *see also* Groh v. Ramirez, 540 U.S. 551, 559 (2004) (stating that it is a "'basic principle of Fourth Amendment law' that searches and seizures inside a home without a warrant are presumptively unreasonable") (citation omitted).

contrast, if police are able to compel you to unlock your biometrically-secured cell phone, then they can access and absorb the same amount of information in the span of a short afternoon. Thus, the two containers of information (the floppy disks sitting in your home and the cell phone held in your hand) should be treated differently because the latter allows for an easier, quicker, and thus more intrusive and probing search into your private information. Otherwise, by allowing unfettered access to a secured cell phone, you essentially do law enforcement's job for them when you are compelled to unlock and hand over that device.

V. CONCLUSION

Floppy disks aside, modern cell phones present a moral and constitutional conundrum. Today, cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[197] Widespread use of phones equipped with biometrics, in addition to the sheer amount of information stored on those devices, makes this issue ripe for review. The Supreme Court cannot sit idly by as lower courts struggle to reach a just conclusion on this issue.[198] Ultimately, declining to extend Fifth Amendment protection to biometrics could rupture public confidence in the privilege against compulsory self-incrimination.[199] The public has come to rely on its ability to keep private things private,[200] to "plead the Fifth," and seek the Self-Incrimination Clause's protection.[201] If people store sensitive information on

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

198. Some fear that constitutional protections and judicial action are insufficient to solve this problem and instead advocate for the adoption of additional safeguards by the legislature. Farahany, *supra* note 77, at 406.

199. *See In re* Search of a Residence in Oakland, CA, 354 F. Supp. 3d 1010, 1014-15 (N.D. Cal. 2019) ("Citizens do not contemplate waiving their civil rights when using new technology. . . .").

200. Farahany, *supra* note 77, at 406 ("A sphere of private rumination is essential to our fundamental concepts of freedom of thought, freedom of expression, freedom of will and individual autonomy.").

201. As one expert noted, "'You have the right to remain silent' is a bedrock of our constitutional and pop culture. And adding an asterisk to that—except you have to tell us your password—seems fundamentally counter to what the Fifth Amendment stands for." Cyrus Farivar, *Court: Teen's driving killed someone, but he can't be forced to give up passcode*, ARS TECHNICA (Oct. 28, 2018, 9:00 AM), https://arstechnica.com/tech-policy/2018/10/court-teens-driving-killed-someone-but-he-cant-be-forced-to-give-up-passcode/.

their secured cell phones in reliance on that privilege, that sensitive information should be protected.[202]

Brittany A. Carnes

202. And, on the bright side, at least Americans do not have to worry about police staging fake muggings just to get unlocked phones from criminal suspects. Dominic Casciani & Gaetan Portal, *Phone encryption: Police 'mug' suspect to get data*, BBC NEWS (Dec. 2, 2016), https://www.bbc.com/news/uk-38183819.