U.C.L.A. Law Review

Biometric Passwords and the Fifth Amendment: How Technology Has Outgrown the Right to Be Free From Self-Incrimination

Adam Herrera

ABSTRACT

Society is transitioning into a new era within the realm of passwords. The growing dependence on smartphones has led consumers to store extremely sensitive information on their password-protected phones. Technology companies have made these smartphones more attractive and secure by allowing users to password protect their phones using their physical features, or "biometric passwords." However, users who adopt such passwords are waiving their right to assert certain constitutional rights. An individual cannot "plead the Fifth" if asked to unlock a smartphone using a physical feature. On the other hand, an individual who possesses the same smartphone, but uses a nonbiometric password, can successfully "plead the Fifth" and refuse to disclose the password. This Comment explores this legal issue and sets forth a proposal on how courts can extend the Fifth Amendment privilege against self-incrimination to biometric passwords. This proposal calls for a new legal test in determining what merits Fifth Amendment protection, taking into consideration the fact that communication today is not the same as communication when the Supreme Court first set out its test for Fifth Amendment protection. This Comment then applies the proposal to the iPhone X, since the phone's facial recognition technology is a model of the growth of biometric passwords.

AUTHOR

UCLA School of Law, J.D., 2019.

Thank you to Professor Ingrid Eagly for her guidance, expertise, and encouragement, and also to Professor Alicia Solow-Niederman for her thoughtful input. I would also like to thank the editors and staff of the *UCLA Law Review* for all of their hard work. Finally, I would like to thank my brother, Randon Herrera, for his tremendous feedback and support, and my parents, for their unconditional love and support.

TABLE OF CONTENTS

INTRODUCTION

In November 2017, Apple released the iPhone X.[1] This was a historic breakthrough for the smartphone industry. Through a technology known as Face ID, an individual can now set his or her face as a biometric password so that an iPhone can be unlocked simply by looking at the screen. Apple created this technology so that users could better protect the private and sensitive information contained within their phones.[2] And soon after the release of the iPhone X, other technology companies began research and development into facial recognition, hoping to capitalize on what appeared to be the new future of smartphone passwords.[3] It is estimated that over one billion smartphones will have facial recognition technology by 2020.[4]

However, consumers should accept such technologies with caution. Despite the increased security that biometric passwords offer, users of biometric passwords are, with respect to unlocking their smartphones, waiving their right to assert the Fifth Amendment privilege against self-incrimination—a privilege they otherwise would have been able to assert with respect to disclosing a nonbiometric password.

Consider the following two hypotheticals, which illustrate how the right to be free from self-incrimination is applied to biometric passwords.

> *Hypothetical A*: The police have a warrant to search John's iPhone X, as they believe it contains information that can incriminate John. The officers execute the warrant and seize the phone. They cannot unlock it because it has a four-digit passcode, and Face ID is not activated. So, a subpoena is issued, and John is brought to court where he is asked to disclose his password. John "pleads the Fifth" and refuses to speak. The court holds that John has the right to do so. Therefore, the officers are unable to access the contents of his phone, despite their belief that there is information within the phone that can be used to charge John with a crime.

1. Press Release, Apple, The Future Is Here: iPhone X (Sept. 12, 2017), http://www.apple.com/newsroom/2017/09/the-future-is-here-iphone-x [http://perma.cc/YJ9S-FZ4B].
2. *See id.*
3. *See, e.g.*, Gordon Kelly, *Samsung 'Confirms' Galaxy S9 Headline Upgrades*, FORBES (Feb. 15, 2018, 7:40 PM), http://www.forbes.com/sites/gordonkelly/2018/02/15/samsung-galaxy-s9-galaxy-s9-plus-camera-specs-release-date-facial-recognition [http://perma.cc/9LJ9-DJNL] ("[T]he Galaxy S9 will add facial recognition . . . .").
4. Rayna Hollander, *Here's When Facial Recognition Will Be Standard on Smartphones*, BUS. INSIDER (Feb. 12, 2018, 9:32 AM), http://www.businessinsider.com/facial-recognition-standard-on-smartphones-2018-2 [http://perma.cc/8JYN-CCVG].

> *Hypothetical B*: The police have a warrant to search Jane's iPhone X, as they believe it contains information that can incriminate Jane. The officers execute the warrant and seize the phone. They cannot unlock it because it has a four-digit passcode, but Face ID is also activated. Just like with John, a subpoena is issued, and Jane is brought to court where she is asked to unlock her phone. Jane similarly "pleads the Fifth" and refuses to speak. But the court holds that Jane has no such right to "plead the Fifth" with respect to Face ID, since she can unlock her phone without speaking. She is then compelled to unlock the phone by looking at her screen to activate Face ID. Therefore, the officers are given full access to the contents of Jane's phone and can use anything found in the phone to charge Jane with a crime.

In the above hypotheticals, both John and Jane have chosen to protect their phones using a password, yet only John can successfully assert the Fifth Amendment right against self-incrimination. The reason for this seemingly inconsistent result is rooted in a legal distinction between testimonial and nontestimonial communications; an individual can assert the Fifth Amendment only if a compelled communication is "testimonial."[5] This in turn requires a communication to contain some factual assertion or to convey incriminating information, explicitly or implicitly.[6]

So, in the posited hypotheticals, it would appear that disclosing a four-digit passcode is a testimonial communication, since disclosing a password conveys factual information.[7] This falls neatly within the protections of the Fifth Amendment. However, using one's face to unlock that very same phone does not convey factual information, because it is a silent action.[8] This leads to the conclusion that Jane, just like any other iPhone X user who uses Face ID, cannot refuse to unlock her phone by asserting the right to be free from self-incrimination. This holds true even when Face ID is used in conjunction with a numeric password.[9]

---

5. Doe v. United States, 487 U.S. 201, 207 (1988).
6. *Id.* at 210–13.
7. *See, e.g.*, United States v. Kirschner, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) (holding that forcing a defendant to reveal his password would require the defendant to disclose a fact, and therefore the defendant could properly withhold his password under the Self-Incrimination Clause).
8. *Cf.* Commonwealth v. Baust, No. CR14-1439, 2014 WL 10355635, at *4 (Va. Cir. Ct. Oct. 28, 2014) (holding that compelling an individual to use a fingerprint to unlock an iPhone does not require the individual to "divulge anything through his mental processes"). Although *Baust* involved a fingerprint as opposed to a face, if one were to accept the court's argument, then the same logic would equally apply to the use of Face ID.
9. Of important note, given the way iPhones are currently developed, Face ID will always be used in conjunction with a nonbiometric password. This is because a user must first set up a PIN or alphanumeric password to activate Face ID. *See* APPLE, FACE ID SECURITY 2

This Comment proposes that the type of password an individual deploys should not determine whether that individual can be compelled to unlock a phone. Regardless of whether the password is a combination of numbers, an alphanumeric password, or a physical feature, they all merit protection. This is because fundamentally, all of these passwords serve the same purpose. As society progresses into a new era of biometric technology,[10] such a change in the law is necessary, since judges across the country are increasingly making decisions about biometrics using a body of law that was developed decades before biometric passwords even existed.[11] The current legal framework allows law enforcement agents to increasingly request search warrants so that they can access smartphones that are protected with biometric passwords, even if those smartphones are also protected by numeric passwords.[12] The law must evolve to catch up to technology so that all smartphone users, regardless of the types of passwords they are using, can assert the same protections guaranteed in the Fifth Amendment.

Part I of this Comment explores the growth of biometric authentication leading to the facial recognition features of the iPhone X. Part II then explores how the Self-Incrimination Clause has evolved throughout the twentieth century as the U.S. Supreme Court struggled to find a workable framework. Part III applies the current framework to biometric passwords, using the iPhone X as an example, and concludes that the current framework is outdated and must evolve. I offer a solution in Part IV, wherein I propose an updated framework which would allow courts to take into consideration the biometric technologies that have developed in the past few years and will continue to develop in the upcoming years. This new framework would expand Fifth Amendment protection to technology users, while

(2017), http://www.apple.com/business/docs/FaceID_Security_Guide.pdf [http://perma.cc/JV7T-XC3M]. In the posited hypotheticals, even though Jane could refuse to unlock her iPhone using a numeric password, she would still have to unlock her iPhone using Face ID. This is because under the current framework, just because one password on a phone is "testimonial," it does not automatically mean that other passwords for that same phone are also "testimonial." *See Baust*, 2014 WL 10355635, at *4 (holding that the defendant could be compelled to unlock his iPhone using his biometric password but could not be compelled to unlock the phone using a passcode).

10. *See infra* notes 44–47 and accompanying text.

11. *See* Jack Linshi, *Why the Constitution Can Protect Passwords but Not Fingerprint Scans*, TIME (Nov. 6, 2014), http://time.com/3558936/fingerprint-password-fifth-amendment [http://perma.cc/ZEL9-WDB5].

12. *See, e.g.*, Thomas Brewster, *LAPD Warrant Lets Cops Open Apple iPhone With Owner's Fingerprints*, FORBES (Mar. 31, 2016, 6:00 AM), http://www.forbes.com/sites/thomasbrewster/2016/03/31/warrant-apple-iphone-fingerprints-hack-los-angeles [http://perma.cc/A63E-ZAKG] (discussing a warrant that was issued in Los Angeles which allowed the LAPD to unlock an individual's iPhone using the individual's biometric ID despite the individual also having a nonbiometric passcode).

remaining true to the spirit of the Fifth Amendment, so that individuals cannot be compelled to unlock a device using their physical features.

I. THE GROWTH OF BIOMETRIC AUTHENTICATION

Smartphones have become one of the most important devices that an individual can own. "They are the first thing we touch when we wake in the morning and the last thing we touch when we go to bed at night."[13] A psychotherapist in New York wrote that "[m]ost people now check their smartphones 150 times per day, or every six minutes."[14] Another study revealed that 46 percent of smartphone users said that they could not live without their phone.[15] For many users, smartphones have essentially replaced computers, and their accessibility and mobility allow for a multitude "of functions to be accessed anywhere and anytime."[16]

But as smartphones have become an integral part of daily life, individuals have inevitably become more comfortable with storing sensitive information on their phones. The type of personal information that can now be found on a smartphone includes personal photos, videos, emails, passwords, credit card numbers, and bank account numbers.[17] This raises serious security concerns because smartphone users are vulnerable when they store so much personal information about themselves on a single device. These security concerns are even

13. Tom Chatfield, *The Most Intimate Relationship in Your Life: Your Smartphone*, 99U (Apr. 2, 2015), http://99u.com/articles/41017/the-most-intimate-relationship-in-your-life-your-smartphone [http://perma.cc/TAG9-HGC2].
14. Jane E. Brody, *Hooked on Our Smartphones*, N.Y. TIMES (Jan. 9, 2017), http://www.nytimes.com/2017/01/09/well/live/hooked-on-our-smartphones.html. A mobile application that helps individuals "disconnect from their phones" reports that "[a]lmost half of global smartphone users spend more than five hours a day on their mobile device." *About Us*, MOMENT, https://inthemoment.io/about.
15. Monica Anderson, *6 Facts About Americans and Their Smartphones*, PEW RES. CTR.: FACTTANK (Apr. 1, 2015). The dependence on smartphones has become so strong that there is now a scientific term for the fear of being without a mobile phone: nomophobia. Piercarlo Valdesolo, *Scientists Study Nomophobia—Fear of Being Without a Mobile Phone*, SCI. AM., http://www.scientificamerican.com/article/scientists-study-nomophobia-mdash-fear-of-being-without-a-mobile-phone [http://perma.cc/GQJ6-ULUJ].
16. Maya Samaha & Nazir S. Hawi, *Relationships Among Smartphone Addiction, Stress, Academic Performance, and Satisfaction With Life*, 57 COMPUTERS HUM. BEHAV. 321, 321 (2016); *see also* United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008) ("A cell phone is similar to a personal computer that is carried on one's person . . . .").
17. Herb Weisbaum, *Most Americans Don't Secure Their Smartphones*, CNBC (Apr. 26, 2014, 1:00 PM), http://www.cnbc.com/2014/04/26/most-americans-dont-secure-their-smartphones.html [http://perma.cc/S6N8-SNJ9].

more troubling in light of the fact that millions of individuals have either been victims of smartphone theft or have simply lost their phone.[18]

A. The Limits of a Password

Technology companies have tried alleviating the vulnerabilities of smartphones by allowing users to protect their smartphones with a password.[19] And smartphone users generally take advantage of the password-setting capabilities of their phones: The Pew Research Center found that 72 percent of smartphone owners have some sort of screen lock on their phones.[20] Yet the reliability of passwords should not be exaggerated. For example, many iPhone lock screen passwords are a four-digit PIN.[21] But regardless of how random, complex, or unique a four-digit PIN is, any four-digit combination of numbers can be hacked through brute force[22] in just seven minutes.[23] Of course, iPhone users

18. For example, in 2014, roughly 5.2 million smartphones were lost or stolen in the United States. *Smartphone Thefts Drop as Kill Switch Usage Grows*, CONSUMER REPS. (June 11, 2015, 12:15 PM), http://www.consumerreports.org/cro/news/2015/06/smartphone-thefts-on-the-decline/index.htm [http://perma.cc/XB7T-JX67]

19. Matthew J. Weber, *Warning—Weak Password: The Courts' Indecipherable Approach to Encryption and the Fifth Amendment*, 2 U. ILL. J.L. TECH. & POL'Y 455, 456 (2016).

20. AARON SMITH & KENNETH OLMSTEAD, *Password Management and Mobile Security*, *in* AMERICANS AND CYBERSECURITY, PEW RES. CTR. (2017), http://www.pewinternet.org/2017/01/26/2-password-management-and-mobile-security [https://perma.cc/9FX6-X6EM]. "An especially large share of smartphone owners" who are age 65 and older do not lock their screens. *Id.* It is understandable why those who are older may not use a password, since the older generation of smartphone owners did not grow up with smartphones as young adults and may not be as dependent on smartphones. And if they are less dependent, then they are less likely to store sensitive information on their smartphones, which lowers the necessity to password protect their smartphones.

21. *Smart Phone Thefts Rose to 3.1 Million in 2013*, CONSUMER REPS. (May 28, 2014, 4:00 PM), http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm [http://perma.cc/C7CT-YRU9] (observing that in 2013, the most commonly used password on a smartphone was a four-digit pin, which was used by 36 percent of smartphone users).

22. Brute-force hacking is an attempt by hackers to figure out a user's password by "systematically trying every possible combination of letters, numbers, and symbols" until the password is cracked. G. Sowmya & A. Naveen Kumar, *Brute Force Attack—Blocking* Technique, 2 INT'L J. ENGINEERING & COMPUTER SCI. 2541, 2541 (2013), http://www.ijecs.in/index.php/ijecs/article/view/1810. Rather than manually trying to figure out all of the potential passwords, hackers can use widely available tools that utilize rules and wordlists to "intelligently and automatically guess user passwords." *Id.*

23. *See* Robert Hackett, *How Long It Takes to Break a Passcode*, FORTUNE (Mar. 18, 2016), http://fortune.com/2016/03/18/apple-fbi-iphone-passcode-hack [http://perma.cc/AK27-HFVX] (showing, through an interactive feature, that an average time for a computer to hack a four-digit passcode is 6 minutes, 34 seconds). The 6 minutes and 34 seconds it takes to hack applies whether a password is as simple as 1111 or as random as 9401. *Id.*

have the option of adding additional security to their phone by making their passwords six digits as opposed to four.[24] But such a password can still be hacked through brute force in just eleven hours.[25]

With this reality in mind, smartphone users are aware that their passwords are vulnerable to hacking. In a Gallup poll, 62 percent of Americans said that they worry about having their computer or mobile device hacked.[26] These fears are not unfounded, since millions of smartphones are lost or stolen every year.[27] While traditional smartphone passwords are definitely a step in the right direction for protecting sensitive information, these passwords still do not provide modern-day smartphone users with the protection they need.

B. A Step Toward Biometric Authentication

One response to the weakness of traditional smartphone passwords has been biometric authentication. A biometric is a "unique, measurable, biological characteristic or trait for . . . verifying the identity of a human being."[28] Biometric authentication uses an individual's biometrics in lieu of, or in addition to, a traditional password to protect that individual's device.[29] A smartphone equipped with such a technology will unlock after its true owner identifies him– or herself using some sort of physical feature that the owner originally registered with the phone.[30]

24. *See Use a Passcode With Your iPhone, iPad, or iPod Touch*, APPLE, http://support.apple.com/en-us/HT204060 [https://perma.cc/952U-BFKF].
25. *See* Hackett, *supra* note 23.
26. Rebecca Riffkin, *Hacking Tops List of Crimes Americans Worry About Most*, GALLUP (Oct. 27, 2014), http://news.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry.aspx?utm_source=alert&utm_medium=email&utm_content=heading&utm_campaign=syndication. Notably, according to the poll, Americans worry about only one other crime more than having their smartphone hacked, which is having their credit card information stolen. *Id.* Ironically, credit card information can be stored on a smartphone. Every other crime in the survey—burglary, assault, hate crimes, and so forth—are crimes that Americans worry less about than having one's smartphone hacked. *Id.*
27. *Smartphone Thefts Drop as Kill Switch Usage Grows*, *supra* note 18.
28. Colin Soutar et al., *Biometric Encryption*, *in* RANDALL K. NICHOLS, ICSA GUIDE TO CRYPTOGRAPHY 649 (1999), http://www.cse.lehigh.edu/prr/Biometrics/Archive/Papers/BiometricEncryption.pdf [http://perma.cc/U77X-2JE9].
29. *See id.* at 4.
30. *See, e.g.*, *About Face ID Advanced Technology*, APPLE, http://support.apple.com/en-us/HT208108 [http://perma.cc/CG93-NSGM] (last updated Nov. 6 2018) (explaining how an iPhone X user can register his or her face on an iPhone X so that the user can subsequently unlock the iPhone using his or her face).

Apple took a major step with respect to biometric authentication when it released the iPhone 5s in 2013.[31] The new smartphone was equipped with Touch ID, which allows users to register their fingerprints and unlock their iPhones by merely placing a finger on the home button.[32] Individuals no longer had to depend solely on traditional passwords, which could easily be hacked by third parties.[33] Instead, they could set up more secure passwords in conjunction with their fingerprints. This was an improvement from a security perspective because fingerprints are unique, so only the person who has the fingerprint registered to the phone can access it.[34]

The push for biometric authentication did not stop with the iPhone 5s. Technology companies began looking at other ways to incorporate an individual's unique biometrics as a means of identification.[35] For example, a company developed an app which allowed a user to press his or her ear against a smartphone screen to unlock the phone.[36] Other companies developed software products that applied keystroke dynamics, which could identify and authenticate users of a computer from their distinctive typing patterns.[37] Researchers even

31. *See* Press Release, Apple, Apple Announces iPhone 5s—The Most Forward-Thinking Smartphone in the World (Sept. 10, 2013), http://www.apple.com/newsroom/2013/09/10Apple-Announces-iPhone-5s-The-Most-Forward-Thinking-Smartphone-in-the-World [http://perma.cc/XTT5-LRXX].

32. *Id.*

33. *See* Hackett, *supra* note 23. The reason that an individual would no longer have to depend on a traditional password is because a biometric password makes it more reasonable to set a longer, more complex alphanumeric password, which is a unique combination of numbers, letters, and symbols. This is because the smartphone owner can simply touch the home button to unlock the phone instead of manually typing out a long and complex password every time the owner wants to access the phone. This allows the smartphone user to utilize a more secure password without having to give up convenience. *See* APPLE, *supra* note 9, at 2 ("Face ID makes using a longer, more complex passcode far more practical because you don't need to enter it as frequently."). Such passwords are more secure because they are more difficult to hack. For example, it would take two years and nine months to brute-force hack a password of "aabb11." Hackett, *supra* note 23.

34. *See* Khidr Suleman, *How Secure Is Apple's Touch ID?*, IT PRO (Oct. 8, 2013), http://www.itpro.co.uk/mobile/20728/how-secure-apples-touch-id. However, this does not preclude the possibility that a fingerprint can be replicated, allowing a hacker to access a phone with fingerprint recognition. *Id.*

35. *See* Heather Kelly, *5 Biometric Alternatives to the Password*, CNN (Apr. 4, 2014, 5:07 PM), http://www.cnn.com/2014/04/04/tech/innovation/5-biometrics-future [http://perma.cc/8X27-VWWQ].

36. *More Info*, DESCARTES BIOMETRICS, http://www.descartesbiometrics.com/ergo-info [http://perma.cc/J39V-CSG3] ("[A]n individual user simply lifts their device to their ear and presses their ear to the touch screen to authenticate and unlock their device.").

37. *See* Kelly, *supra* note 35; *see also* M. Karnan et al., *Biometric Personal Authentication Using Keystroke Dynamics: A Review*, 11 APPLIED SOFT COMPUTING 1565, 1566 (2011) (explaining how keystroke dynamics can identify users based on certain features of an

looked into the possibility of gait recognition, in which a device could analyze a person's distinctive walking patterns to determine if that person is the rightful owner.[38]

And of course, researchers began looking into facial recognition, which would use an individual's face to unlock a device.[39] From this came Face ID.

C. An Even Bigger Step Toward Biometric Authentication: Facial Recognition

Only four years after the release of the iPhone 5s, Apple released the iPhone X, which came with facial recognition technology known as Face ID.[40] This technology allows a user to set his or her face as a password to unlock the iPhone X.[41] It maps the geometry of a user's face, and it is programmed to unlock the phone only when it recognizes a registered user's unique facial characteristics.[42] Additionally, Face ID has a secure technology which is designed to protect users from hackers who try to recreate a user's face through the use of a mask, photo, or other techniques.[43]

The significance of Face ID goes well beyond the immediate security benefits provided by the iPhone X. Similar technologies are already being incorporated in devices besides smartphones.[44] Moreover, Apple is not alone in trying to revolutionize the smartphone industry; other smartphone manufacturers have either begun experimenting with facial recognition or will begin doing so in the near future.[45] And the expansion of facial recognition technology on smartphones

individual's typing, including "duration of a keystroke or key hold time, . . . typing error, force of keystrokes etc.").

38. Kelly, *supra* note 35.
39. *See, e.g.*, Marc Saltzman, *FastAccess Anywhere: Face Recognition Replaces Password*, USA TODAY (June 4, 2013, 3:53 PM), http://www.usatoday.com/story/tech/2013/06/04/fastaccess-anywhere-facial-recognition-app-insider/2389349 [http://perma.cc/F75Q-RXKS].
40. Press Release, Apple, *supra* note 1.
41. *Id.* ("Face ID only unlocks [an] iPhone X when customers look at it."). Additionally, Face ID can be used to enable certain features and gain access to secure apps on an iPhone X. *Id.*
42. APPLE, *supra* note 9, at 2.
43. *Id.* at 3.
44. For example, Apple incorporated Face ID into its iPads in 2018. *See Use Face ID on Your iPhone or iPad Pro*, APPLE, https://support.apple.com/en-us/HT208109 [https://perma.cc/MWL6-8MVQ] (last updated Nov. 6, 2018). Other companies, such as Microsoft, have incorporated facial recognition into computers, allowing users to log into their computer just by staring at the computer screen. *See, e.g.*, *Windows Hello: Discover Facial Recognition on Windows 10*, MICROSOFT, http://www.microsoft.com/en-us/windows/windows-hello [http://perma.cc/X9RB-VVV3].
45. For example, one of Apple's competitors, Samsung, followed Apple's footsteps by incorporating facial recognition technology into the Galaxy S8. *See Galaxy S8*, SAMSUNG, http://www.samsung.com/uk/smartphones/galaxy-s8/security [http://perma.cc/2GKV-

and other password-protected devices is only going to continue growing: Consumers globally are increasingly looking for more security when they log on to devices that contain sensitive information.[46] Specifically, consumers increasingly view biometric authentication as more secure than traditional passwords and PINs.[47]

Despite the growing excitement and potential for facial recognition technologies such as Face ID, there is a concern when this technology meets the law: Even though biometric passwords can better protect smartphone users from hackers, these passwords cannot protect smartphone users from law enforcement seeking access to their phones. Specifically, the trajectory of case law suggests that an individual can be compelled to unlock his or her smartphone using a biometric password, yet a similarly situated individual can assert the right to be free from self-incrimination when asked to disclose a numeric passcode or alphanumeric password. To understand how the law arrived at this result, it is imperative to understand how the law surrounding the Self-Incrimination Clause has developed.

II. THE STATE OF THE LAW

The Fifth Amendment's Self-Incrimination Clause states that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself."[48] Generally, an individual can invoke the privilege against self-incrimination when three requirements are satisfied: (1) compulsion, (2) incrimination, and (3) a testimonial communication or act.[49] Compulsion exists when an individual is coerced into testifying out of fear that refusing to testify will lead to an adverse inference of

QFTE]. The Galaxy S8 also has iris scanner technology, which allows users to open up their smartphone by aligning their eyes with two circles on-screen. *Id.* Additionally, other smartphone vendors, including "Xiaomi, Huawei, OPPO, and Vivo will likely follow in Apple's steps and increasingly adopt 3D facial technology." Hollander, *supra* note 4.

46. A global study released by IBM in early 2018 examined "consumer perspectives around digital identity and authentication." Press Release, IBM, IBM Future of Identity Study: Millennials Poised to Disrupt Authentication Landscape (Jan. 29, 2018), http://www-03.ibm.com/press/us/en/pressrelease/53646.wss?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy [http://perma.cc/75TA-ZN7P]. Particularly, younger adults are more likely to use biometrics to improve their personal security. Of the people who were identified as "millennials," 75 percent said they are comfortable using biometrics today. *Id.*

47. *Id.*

48. U.S. CONST. amend. V; *see also* Schmerber v. California, 384 U.S. 757, 760–61 (1966) ("[T]he Fifth Amendment guarantees . . . the right of a person to remain silent unless he chooses to speak in the unfettered exercise of his own will, and to suffer no penalty . . . for such silence." (quoting Malloy v. Hogan, 378 U.S. 1, 8 (1964))).

49. *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1341 (11th Cir. 2012).

guilt.[50] Incrimination occurs when an individual is asked to produce something or give an answer which could then support a conviction of that individual, or even lead to a chain of evidence that could be used to prosecute that individual for a crime.[51]

The third requirement, a testimonial communication or act, has been more difficult for the judiciary to define.[52] Particularly, courts have struggled in articulating the rule for when a communication or act becomes "testimonial." This was true throughout the twentieth century, during which the Supreme Court issued multiple landmark cases regarding the right to be free from self-incrimination. A reading of these cases shows a struggle to develop a framework that allows for consistent results, especially in light of cases that the Supreme Court had already decided.

A. The Dichotomy Between Physical and Communicative Information

One of the earlier attempts by the Supreme Court to define the parameters of the Self-Incrimination Clause occurred in *Holt v. United States*.[53] The Court considered whether a defendant in a murder trial could be compelled to don a certain blouse to see if it fit the defendant, because a witness had seen the murderer wearing it.[54] In rejecting the defendant's argument that trying on the blouse would be a form of self-incrimination, Justice Holmes reasoned that "the prohibition of compelling a man in a criminal court to be [a] witness against himself is a prohibition of the use of . . . compulsion to extort communications from him, not an exclusion of his body as evidence."[55] Holmes seemed to suggest that information must be "communicative" in order to have an incriminating feature, whereas evidence that is purely "physical," such as wearing a blouse, cannot be incriminating.

50. *See* Griffin v. California, 380 U.S. 609 (1965) (reversing an individual's first-degree murder conviction because the lower court improperly used the defendant's failure to testify as probative of the defendant's guilt). Compulsion need not rise to the level of imprisonment. For example, sufficient compulsion can be the threat of termination of a public job or disbarment of a lawyer. S. DOC. NO. 108-17, at 1397–98 (2002).
51. Hoffman v. United States, 341 U.S. 479, 486 (1951).
52. This is not to suggest that the other parts of the Self-Incrimination Clause are easily interpretable. For a breakdown of each part of the clause, see Akhil Reed Amar & Renée B. Lettow, *Fifth Amendment First Principles: The Self-Incrimination Clause*, 93 MICH. L. REV. 857 (1995) (exploring the meaning of "person," "compelled," "in any criminal case," and "witness" within the Self-Incrimination Clause).
53. 218 U.S. 245 (1910).
54. *Id.* at 252–53.
55. *Id.*; *see also* Brooks v. United States, 494 A.2d 922, 925 (D.C. Cir. 1984) (holding that requiring the defendant to wear a coat, which was found at the crime scene, in the presence of the jury did not violate the defendant's right to be free from self-incrimination).

Then came *Schmerber v. California*,[56] a DUI case, in which the government sought to use a report containing the defendant's blood alcohol level at the time of arrest against the defendant.[57] The defendant argued that withdrawal of his blood, despite his refusal, and admission of the coinciding report, without his consent, forced the defendant to incriminate himself.[58] In rejecting this argument, Justice Brennan drew upon a similar line of reasoning as in *Holt*. Particularly, Brennan reasoned "that the privilege is a bar against compelling 'communications' or 'testimony,' but that compulsion which makes a suspect or accused the source of 'real or physical evidence' does not violate it."[59] Similar to *Holt*, the distinction that Brennan made focused on whether the evidence is "communicative" or "physical" in nature, with only communicative evidence receiving protection.

But Brennan did not stop there—he took the analysis a step further. He realized that there were flaws in having such a rigid distinction between "communicative" and "physical" evidence, and that there could be instances in which the framework would fail.[60] As an illustration, he gave the example of a lie detector: Such a test measures "changes in body function,"[61] which can technically be considered physical evidence under the *Holt* framework. But at the same time, a lie detector may elicit responses which are "testimonial," according to Brennan.[62] To correct for this seemingly erroneous result, Brennan's new framework extended the self-incrimination privilege to evidence that was "testimonial," even if that evidence was considered physical in nature.[63] But Brennan fell short of defining what it means for something to be "testimonial" because he was able to resolve the case narrowly: There was "[n]ot even a shadow" of communication made by the defendant in the extraction of his blood or in the blood alcohol report.[64] Still, Brennan's use of "testimonial" foreshadowed the new standard to come, and it would force future courts to struggle to define what constitutes a "testimonial" communication.

56. 384 U.S. 757 (1966).
57. *Id.* at 758–59.
58. *Id.* at 759.
59. *Id.* at 764.
60. *Id.*
61. *Id.*
62. *Id.* As Brennan argues, "[t]o 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." *Id.* For a further discussion of how polygraph testing implicates the Self-Incrimination Clause, see Ashley J. Fausset, Comment, *Answer Me or Go to Jail: Why Court Ordered Polygraph Testing to Treat Probationers Violates the Fifth Amendment*, 21 AM. U. J. GENDER SOC. POL'Y & L. 455 (2012).
63. *See Schmerber,* 384 U.S. at 761.
64. *Id.* at 765.

Not long after *Schmerber*, the Supreme Court in *United States v. Wade*[65] had its first opportunity to give meaning to "testimonial." The defendant in *Wade* was a suspect in a bank robbery case, but the FBI was unsure of who exactly committed the crime.[66] So, the FBI brought in two of the bank employees who witnessed the robbery to observe a lineup which included the defendant.[67] Each person in the lineup was forced to say, "put the money in the bag," just as the actual robber had said.[68] The bank employees identified the defendant as the bank robber, and their identification of the defendant was subsequently elicited at trial.[69] On appeal of the defendant's conviction, the Supreme Court considered whether forcing the defendant to say certain words violated his right to be free from self-incrimination.[70]

Unlike *Holt* and *Schmerber*, the Court was confronted with a situation in which the evidence at issue had a communicative component: The defendant had *verbally* communicated to the bank employees by uttering certain words. This was clearly not physical in nature, and by definition, the defendant's speaking had communicative features. If the Court had strictly applied the *Holt* physical versus communicative framework, then the defendant's speaking probably would have been protected, since it fell neatly into the communicative realm, as opposed to the physical. However, Justice Brennan, again writing for the Court, was able to fall back on his dicta from *Schmerber* and resolve the case on the grounds of whether the uttered statements were "testimonial."[71] In holding that the statements were not testimonial, Brennan reasoned that the defendant was compelled to use his voice only as an "*identifying* physical characteristic," as opposed to being compelled to verbally state his guilt.[72] The use of the defendant's voice for identification purposes was not sufficiently testimonial for the *Wade* court.[73]

That same year, the Court also heard arguments for *Gilbert v. California*,[74] a case in which an individual robbed a bank using a handwritten note that said "your

65. 388 U.S. 218 (1967).
66. *Id.* at 220.
67. *Id.*
68. *Id.*
69. *Id.*
70. *See id.* at 221.
71. *Id.* at 222.
72. *Id.* at 222–23 (emphasis added); *see also* United States v. Dionisio, 410 U.S. 1, 3–7 (1973) (holding that compelling a defendant to read a script so that it could be compared to a recorded conversation for identification purposes did not implicate the defendant's right to be free from self-incrimination).
73. *See Wade*, 388 U.S. at 222–23.
74. 388 U.S. 263 (1967).

money or your life."[75] Because the identity of the criminal was unknown, the defendant was asked to produce a handwriting exemplar to be compared to the original note used in the bank robbery.[76] The Court conceded that handwriting, just as voice in *Wade*, is a means of communication.[77] But it stressed that not every piece of communication is protected.[78] Just as in *Wade*, the handwriting exemplar was used as a means of identification, as opposed to a means of compelling the defendant to write his guilt.[79]

B. *United States v. Doe*: Giving Meaning to Testimonial

Up until *Gilbert v. California*, the Supreme Court had yet to define what exactly it meant for a communication or act to be "testimonial." This was because the cases where the Court confronted the issue were readily solved on narrow grounds. *Holt* (wearing a blouse) and *Schmerber* (withdrawn blood) involved physical acts in which there was no communication conveyed from the acts. *Wade* (speaking in a lineup) and *Gilbert* (handwritten note) were communications, but the communications were used only for identification purposes. The Court finally gave guidance as to what was meant by "testimonial" in *Doe v. United States*.[80]

In *Doe*, the government sought to compel the defendant to sign broad release forms consenting to disclosure of any bank records regarding twelve foreign bank accounts that the defendant may have controlled.[81] The trial court denied the motion on the grounds that signing the consent forms would necessarily amount to the defendant admitting to the existence of the bank accounts.[82] Additionally, if

75. *Id.* at 266, 291.
76. *Id.* at 266.
77. *Id.*
78. *Id.* ("It by no means follows, however, that every compulsion of an accused to use his voice or write compels a communication within the cover of the privilege.").
79. *See id.* at 266–67; *see also In re* Special Federal Grand Jury Empanelled Oct. 31, 1985, 809 F.2d 1023, 1024–28 (3d Cir. 1987) (holding that compelling an individual to provide handwriting exemplars to the FBI, so that the exemplars could be compared with handwritten documents whose authorship were unknown, did not violate the defendant's right to be free from self-incrimination). Notably, in *In re Special Federal Grand Jury*, the defendant was asked to write using a "backward slant," since that was how the documents whose authorship were unknown were written. *Id.* at 1024–25. The defendant argued that such a handwriting exemplar went beyond mere physical evidence because it would compel his "intellectual processes." *Id.* at 1025. According to the defendant's argument, the government was seeking how the defendant "slants his writing when trying to disguise his normal style." *Id.* The Court rejected this argument and still found that the compelled handwriting was only physical evidence. *Id.* at 1027.
80. 487 U.S. 201 (1988).
81. *Id.* at 203.
82. *Id.* at 203–04.

the banks delivered the records pursuant to the consent forms, it would have been equivalent to the defendant admitting that he had "signatory authority over such accounts."[83] Both of these admissions were tantamount to the defendant admitting his guilt in violation of the Self-Incrimination Clause, since he was being investigated for fraud and unreported income.[84]

On appeal, the Supreme Court focused on whether execution of the forms constituted a testimonial communication.[85] In doing so, the Court articulated a standard: For an individual's communication or act to be testimonial, the individual must explicitly or implicitly relate a factual assertion.[86] Specifically, information can be "testimonial" if it requires the individual to sort through the contents of his or her mind in order to relate the information.[87]

The Court found that execution of the consent forms was not testimonial, since "neither the form, nor its execution, communicate[d] any factual assertions, implicit or explicit, or convey[ed] any information to the Government."[88] Taken literally, the defendant's signing of the forms did not convey any information.[89] The forms did not acknowledge that the defendant actually owned or had control of any particular bank account; they did not acknowledge the existence of certain defendant.[90] Rather, the forms were drafted carefully so as to speak in the hypothetical—they merely authorized the defendant's consent to have the foreign banks disclose records owned by the defendant, if those records even existed.[91] Thus, the government's careful drafting allowed them to overcome any Fifth Amendment argument that the defendant was incriminating himself by disclosing factual information.

By using a rule that focused on whether any factual assertions were conveyed, the Supreme Court was able to consolidate its previous holdings into a framework with consistent results. For example, in *Wade* and *Gilbert*, the defendants did not convey any factual information through their communications. By saying "put the money in the bag," or writing "your money or your life," the defendants were not admitting the truth of those statements, and therefore could not have been

83. *Id.* at 204.
84. *See id.*
85. *Id.* at 207.
86. *Id.* at 209–10. Although the Court set forth a standard of what is considered "testimonial," it made clear that whether a communication is "testimonial" will often depend on the facts and circumstances of a case. *Id.* at 214–15.
87. *See id.* at 211.
88. *Id.* at 215.
89. *Id.* at 215–16.
90. *Id.* at 215.
91. *Id.*

conveying any facts.[92] Rather, the statements were compelled so that witnesses to the crime could identify physical characteristics of defendants, such as their voice or handwriting, regardless of the truth of the compelled statements.

The Supreme Court further clarified the *Doe* framework in *United States v. Hubbell*,[93] in which the defendant was asked to produce multiple categories of documents.[94] In deciding whether the defendant had a right to plead the Fifth, the Court stressed that the inquiry was not whether the *content* of the documents was testimonial, but whether the *act* of producing the documents was testimonial.[95] And in this case, response to the government's subpoena would have amounted to a testimonial act, since the defendant would have used "the contents of his own mind" to identify the hundreds of documents fitting the broad categories requested by the government.[96] Additionally, the act of production would implicitly communicate facts, since the defendant would have been admitting "that the papers existed, were in his possession or control, and were authentic."[97] The Court analogized this to asking for a combination to a wall safe, as opposed to being forced to surrender the key to a strongbox—the former being "testimonial," the latter being nontestimonial.[98]

C. The Foregone Conclusion Doctrine: An Exception to the Testimonial Test

Given the *Doe* framework, disclosing a biometric password must convey factual information for an individual to successfully assert the privilege against

92. *See* Gilbert v. California, 388 U.S. 263, 266–67 (1967).
93. 530 U.S. 27 (2000).
94. *Id.* at 31.
95. *Id.* at 40. In applying this reasoning to the context of iPhones and smartphones, the proper inquiry would be whether the act of unlocking an iPhone (whether through a password, fingerprint, or face) is testimonial. What is not proper is to inquire whether the potentially incriminating contents within the iPhone are testimonial.
96. *Id.* at 43 (quoting Curcio v. United States, 354 U.S. 118, 128 (1957)); *see also id.* at 41–42 ("The assembly of literally hundreds of pages of material in response to a request for 'any and all documents reflecting, referring, or relating to any direct or indirect sources of money . . .' is 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.").
97. *Id.* at 36 (quoting Doe v. United States, 487 U.S. 201, 209 (1988)). The more specific request in *Hubbell* is distinct from the request in *Doe*, in which the government's request spoke in the hypothetical, meaning that the defendant's response technically would not have been admitting to ownership of any bank accounts. *See Doe,* 487 U.S. at 215. Had the government also made a vague, hypothetical request in *Hubbell*, it likely would have been able to obtain the requested information without violating the defendant's right to be free from self-incrimination.
98. *Hubbell*, 530 U.S. at 43.

self-incrimination. However, even if this is satisfied, there are still exceptions that may allow for compulsion of the sought-after information. While this Comment only explores the threshold question of whether a compelled act is "testimonial," one exception deserves brief mention, as it opens the door for even more legal issues when it comes to compelled disclosure of biometric passwords.

The foregone conclusion doctrine allows the government to compel an individual to disclose testimonial information if that information is already known to the government.[99] In such circumstances, the sought-after information loses its "testimonial" value since an individual's conceding of that information would add nothing new to the government's case.[100] For example, if the government serves a subpoena on a defendant seeking certain documents, and the government already knows that the defendant owns those documents, then the defendant cannot argue that response to the subpoena is tantamount to admitting ownership of those documents in violation of his right to be free from self-incrimination.[101] This is because the defendant's ownership of the documents is a "foregone conclusion"—the government already knows that he owns those documents.[102] If, on the other hand, the government serves the same subpoena but does not know that the defendant possesses those documents (meaning, the government is going on a "fishing expedition" for certain information),[103] then the foregone conclusion doctrine is inapplicable.[104] Thus, whether the foregone conclusion doctrine applies depends on what the government already knows beforehand.[105]

99. *See* Fisher v. United States, 425 U.S. 391, 411 (1976).
100. *See id.*
101. *See id.*
102. *Id.* Another way to look at the issue is whether or not the government is relying on the "truth-telling" of the individual. *Id.* (quoting 8 WIGMORE, EVIDENCE § 2264, at 380 (3d ed. 1940). If the government is relying on the truth-telling (which means that the government does not know the sought-after information), then the information is not a foregone conclusion. *Id.* If, on the other hand, the government is not relying on the truth-telling (which means the government already knows what it is going after), then the information is a foregone conclusion. *Id.*
103. *Hubbell*, 530 U.S at 32.
104. *See id.* at 44–45 (holding that a defendant's response to documents was not a foregone conclusion because the government did not show that it had prior knowledge of the existence or whereabouts of the 13,120 pages of documents that it requested); *see also id.* at 32 (discussing district court's characterization of government subpoena as a "fishing expedition"). In *Hubbell*, the government was unable to prove the existence of the documents with "reasonable particularity." United States v. Hubbell, 167 F.3d 552, 579 (D.C. Cir. 1999), *aff'd*, 530 U.S. 27 (2000).
105. Although this Comment does not explore the foregone conclusion doctrine, there is a great deal of legal scholarship that discusses its applicability to passwords, both biometric and traditional. For example, one scholar argues that the foregone conclusion doctrine only applies to the production of physical evidence—and not passwords—since the only cases that the U.S. Supreme Court has issued with regards to the foregone conclusion

III. APPLYING THE LEGAL FRAMEWORK TO SMARTPHONES

Given the wealth of personal information stored in mobile devices, law enforcement officials have an incentive to access the smartphones of suspects to a crime. The potentially incriminating information stored on smartphones can assist law enforcement with investigations and aid prosecutors in building their cases against defendants.[106] Such incriminating information can come in the form of photos, videos, text messages, voicemails, call history, contact lists, emails, and browser history.[107]

Yet there is an obstacle for police officers and prosecutors who seek access to an individual's smartphone. Without knowing the password to a certain smartphone, a police officer or prosecutor, just as any other individual, cannot immediately access that phone. The seemingly obvious solution is for law enforcement agents to obtain a warrant, which would allow them to seize an individual's phone and to have the legal right to search the phone's contents.[108]

However, even when law enforcement officials have the legal right to search a phone, the right to be free from self-incrimination does not completely dissipate, depending on the type of password on the phone. This can be understood using the combination/key analogy that was articulated in *Doe*: A password, like a

doctrine have been cases in which a defendant was asked to produce physical evidence, such as a document. *See* Andrew T. Winkler, *Password Protection and Self-Incrimination: Applying the Fifth Amendment Privilege in the Technological Era*, 39 RUTGERS COMPUTER & TECH. L.J. 194, 211–12 (2013). Other scholars have argued that if the government can show that an individual possesses a particular file that the government is seeking, then the sought-after information is a foregone conclusion, and the individual should not be able to circumvent the government's efforts by using a password. *See* Vivek Mohan & John Villasenor, *Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era*, 15 U. PA. J. CONST. L. HEIGHTENED SCRUTINY 11, 23 (2012). For an application of the foregone conclusion doctrine to passwords, see *In re Grand Jury Subpoena Duces Tecum Dated March 25 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012) (holding that compelling an individual to decrypt his hard drive through use of a password was not a foregone conclusion because the government did not know about the existence of any files on the hard drive).

106. *See* Efren Lemus, Comment, *When Fingerprints Are Key: Reinstating Privacy to the Privilege Against Self-Incrimination in Light of Fingerprint Encryption in Smartphones*, 70 SMU L. REV. 533, 544–45 (2017); *see also* Martin Kaste, *Your Smartphone Is a Crucial Police Tool, If They Can Crack It*, NPR (Mar. 25, 2014, 2:54 PM), http://www.npr.org/sections/alltechconsidered/2014/03/25/291925559/your-smartphone-is-a-crucial-police-tool-if-they-can-crack-it (noting that a smartphone has "[y]our calls, your emails, your calendar, your photos—not to mention the GPS data embedded in those photos—[which] could make a whole case, in one convenient package").

107. *See* Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27, 44 (2008).

108. *See* Riley v. California, 134 S. Ct. 2473, 2485 (2014) (holding that generally, officers can search a cellphone after obtaining a search warrant).

combination, cannot be compelled as it demands the use of one's mind, whereas a fingerprint or face, like a key, can be compelled, as it does not communicate any factual information.

A. Traditional Smartphone Passwords: A Combination to a Wall Safe

Courts have had limited exposure to cases dealing with individuals who are compelled to provide traditional[109] smartphone passwords and whether this violates the Self-Incrimination Clause. However, to understand how the *Doe* framework is applied, it is not necessary to focus only on cases that involve smartphones. Rather, cases in which individuals are compelled to produce their passwords for devices other than phones—such as laptops or computers—serve as reliable guideposts. This is because application of the *Doe* framework to a smartphone or computer[110] leads to the same question: Is revealing a password a testimonial communication or act?[111]

In *United States v. Kirschner*,[112] a Michigan District Court held that disclosure of a computer password was a testimonial communication.[113] Citing to *Doe*, the court reasoned that forcing the defendant to reveal his password would require him to use the contents of his own mind to disclose a fact—namely, his password.[114] The defendant would have to "divulge through his mental processes," since his password was something that he created.[115] And unlike past Supreme Court cases in which the self-incrimination privilege was not violated, such as when a defendant wrote a handwriting sample[116] or said a certain phrase,[117] the defendant in this case had communicated affirmative facts to the government which would be used for more than just identification purposes.

The Eleventh Circuit arrived at a similar result on this issue.[118] In *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, the court agreed with the defendant that requiring him to disclose his decryption password was testimonial, as it

109. By traditional, I mean a numeric or an alphanumeric password.
110. While the proceeding analysis will focus on the similarities between a smartphone and a computer, this application is certainly not limited to such a comparison. This analysis should apply when comparing a smartphone to any other device that can be password-protected by a user-created password.
111. *Cf.* Doe v. United States, 487 U.S. 201, 215 (1988).
112. 823 F. Supp. 2d 665 (E.D. Mich. 2010).
113. *Id.* at 668–69.
114. *Id.*
115. *Id.* at 669.
116. Gilbert v. California, 388 U.S. 263, 266 (1967).
117. United States v. Wade, 388 U.S. 218, 222–23 (1967).
118. *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012).

would require him to use the contents of his mind to disclose an explicit fact—similar to *Kirschner*.[119] Additionally, providing a decryption password would be the same as the defendant admitting he had the capability to decrypt the files, which in turn would be him admitting ownership.[120] This is an implicit assertion of fact, which is also testimonial under the *Doe* rule.

Although these two cases did not involve smartphones, the same line of reasoning easily applies to a smartphone password. Moreover, the few courts that have dealt with smartphone passwords, discussed below, have cited to *Kirschner* and *In re Grand Jury* in their reasoning. This shows that the type of device that the government is seeking to unlock is immaterial; the proper inquiry is whether the *act* of production itself is testimonial—nothing more.[121] Whether it is a smartphone or a computer, a user is disclosing some sort of numeric or alphanumeric password to allow access to the device, and thus conveying his or her knowledge.

Turning to smartphone passwords, the limited number of cases have generally held that disclosure of a smartphone password is a testimonial act. In *Securities and Exchange Commission v. Huang*, the SEC sought to compel production of defendants' passwords for their work-issued smartphones.[122] Notably, the SEC focused its testimonial analysis on the contents within the smartphones, arguing that the contents were not testimonial in nature.[123] This argument misunderstood *Doe*, however. The court recognized that the proper inquiry was not whether the *contents* were testimonial, but rather whether the *act* of producing the passwords was testimonial.[124] Agreeing with *Kirschner* and *In re Grand Jury*, the court ruled that disclosing a password is a testimonial

119. *Id.*
120. *See id.*
121. *Id.* at 1345–46.
122. No. 15-269, 2015 WL 5611644, at *1 (E.D. Pa. Sept. 23, 2015).
123. *Id.* at *2.
124. *Id.* A similar inquiry of focusing on the phone's contents was also conducted by the *State v. Stahl* court. *See* 206 So. 3d 124, 133–34 (Fla. Dist. Ct. App. 2016). In *Stahl*, because the court found that the contents in the defendant's smartphone had no testimonial significance, the court held that disclosure of the defendant's smartphone passcode was not a testimonial communication. *Id.* at 134, 137. But again, focusing on the contents of a password-protected device, as opposed to the password itself, is the incorrect analysis. This was not only recognized by the court in *SEC v. Huang*, 2015 WL 5611644, at *1, but it can also be inferred from the Supreme Court's reasoning in *United States v. Hubbell*, in which the Court stated that "[t]he 'compelled testimony' that is relevant in this case is not to be found in the contents of the documents produced in response to the subpoena. It is, rather, the testimony inherent in the act of producing those documents." United States v. Hubbell, 530 U.S. 27, 40 (2000) (quoting Kastigar v. United States, 406 U.S. 441, 460 (1972)).

communication because it "require[s] intrusion into the knowledge of [the] Defendants."[125]

Finally, the most applicable cases are those regarding iPhone passcodes. In *State v. Trant*,[126] the court denied the state's motion to compel the defendant's iPhone passcode, finding that disclosure of the passcode would be testimonial.[127] The court distinguished a password from evidence of physical characteristics—which are nontestimonial—and instead found that disclosure of a password was a "product of mental processes."[128]

In another state court case, *Commonwealth v. Baust*,[129] the police tried unlocking the defendant's iPhone, as it had a potentially incriminating recording.[130] The court held that the defendant could not be compelled to produce his passcode for the same reason as in *Kirschner*: The defendant would be required to "divulge through his mental processes" and "disclose the contents of his own mind" in disclosing his passcode.[131] A federal court reached the same result in *United States v. Sanchez*,[132] where it held that the defendant's compelled production of his iPhone passcode to an officer violated his right against self-incrimination.[133]

A traditional password, regardless of what device it is protecting, is contained within an individual's mind. Disclosure of a password gives the "combination to a wall safe," which can lead to incriminating information. Although the Supreme Court has never heard a case with respect to passwords being testimonial, the above cases illustrate how application of the *Doe* framework to passwords is consistent with existing Supreme Court precedent.[134] Namely, disclosing a smartphone password—numeric or alphanumeric—is a testimonial communication which falls under the protection of the Self-Incrimination Clause.[135]

125. *Huang*, 2015 WL 5611644, at *2.
126. No. CUMCDCR201502389, 2015 WL 7575496, at *1 (D. Me. Oct. 27, 2015).
127. *Id.* at *2–4. *But see Stahl*, 206 So. 3d at 133–35 (holding that disclosure of an iPhone passcode was not a testimonial communication).
128. *Trant*, 2015 WL 7575496, at *2.
129. No. CR14-1439, 2014 WL 10355635, at *1 (Va. Cir. Ct. Oct. 28, 2014).
130. *Id.* at *1.
131. *Id.* at *4.
132. 334 F. Supp. 3d 1284 (N.D. Ga. Sept. 12, 2018), *appeal filed* No. 18-15289 (11th Cir. Dec. 26, 2018).
133. *Id.* at 1298.
134. Joshua A. Engel, *Rethinking the Application of the Fifth Amendment to Passwords and Encryption in the Age of Cloud Computing*, 33 WHITTIER L. REV. 543, 555 (2012).
135. *E.g.*, *id.* at 550.

B. Biometric Smartphone Passwords: A Key to a Wall Safe

Although the *Doe* framework may protect users from disclosing traditional smartphone passwords, the reality is that society is moving toward an era of biometric authentication.[136] When the *Doe* framework is applied to biometric passwords, it appears that individuals would be seeking protection for a "key to a wall safe," because an individual does not have to communicate to unlock a smartphone, say, with his or her face. Such an act does not receive the same protection as a "combination to a wall safe."

In *Commonwealth v. Baust*, discussed above, the court found that the defendant could not be compelled to produce his iPhone passcode, since he would be required to communicate a fact.[137] However, the court still ordered the defendant to unlock his phone.[138] In addition to his passcode, the defendant also had a biometric password, which could be activated simply by placing the defendant's finger on his phone's home button.[139] This allowed the court to go around the defendant's passcode by arguing "[t]he fingerprint . . . does not require the witness to divulge anything through his mental processes. . . . and does not require [the] Defendant to 'communicate any knowledge' at all."[140]

Interestingly enough, despite making these distinctions between a fingerprint and passcode, the *Baust* court specifically acknowledged that the defendant's fingerprint and passcode were functionally equivalent.[141] Yet, because the fingerprint did not fall within the *Doe* definition of "testimonial," the police were still allowed to access the defendant's phone through his biometric password.[142]

The Minnesota Court of Appeals reached a similar result in *State v. Diamond*,[143] in which the defendant refused to provide his fingerprint to unlock

136. *See supra* notes 44–47 and accompanying text (explaining the different types of biometric authentication that technology companies are adopting).
137. *See* No. CR14–1439, 2014 WL 10355635, at *4 (Va. Cir. Ct. Oct. 28, 2014).
138. *Id.*
139. *See id.* at *1.
140. *Id.* at *4.
141. *Id.* ("[T]he Defendant cannot be compelled to produce his passcode to access his smartphone but he can be compelled to produce his fingerprint *to do the same*." (emphasis added)).
142. *Id.* A staff attorney at the Electronic Frontier Foundation has described the compelling of an individual to unlock a phone using a fingerprint as a "clever end-run" around constitutional rights, since it "does not technically count as handing over a self-incriminating password." Karen Turner, *Feds Use Search Warrants to Get Into Fingerprint-Locked Phones*, WASH. POST (Oct. 18, 2016), http://www.washingtonpost.com/news/the-switch/wp/2016/10/18/feds-use-search-warrants-to-get-into-fingerprint-locked-phones [http://perma.cc/Y6PC-LECJ].
143. 890 N.W.2d 143 (Minn. Ct. App. 2017).

his smartphone.[144] In holding that the defendant's fingerprint could be compelled, the court reasoned that the defendant was not disclosing any knowledge, using any mental capacity, or speaking his guilt by placing his fingerprint on his phone.[145] The court emphasized that such an action is distinct from providing a traditional password, which involves a certain level of mental capacity.[146]

Part of the problem with the *Diamond* court's reasoning is in how the court understood a fingerprint in the context of a smartphone. Its mistaken views were evidenced by the court's assertion that a fingerprint is no more testimonial than a handwriting exemplar, speaking in a lineup, or wearing particular clothing.[147] The court was of course referencing *Gilbert*, *Wade*, and *Holt*.[148] However, in all of these cases, the compelled communication or act served one main purpose: identification.

For example, in *Gilbert*, the government needed to compare a note written by the defendant to a note that was used to rob a bank to determine whether the defendant robbed the bank.[149] On the other hand, when using a fingerprint to unlock a smartphone, the fingerprint is not helping the government identify the source of an unknown fingerprint. Rather, it is serving the functional equivalence of a password by allowing access to a phone, thereby giving access to a flood of personal information about the smartphone's owner. True, fingerprints can be used for identification in other contexts, such as when one is comparing a suspect's fingerprints to fingerprints found at the scene of a crime. But the context here is different; a fingerprint that unlocks a smartphone serves a different function than a suspect's fingerprint that is compared to a fingerprint at a crime scene.

It is also worth exploring warrants that have been issued to illustrate application of the law. In February 2016, a district court judge in the Central District of California issued a warrant that read: "Law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of the person covered by this warrant onto the Touch ID sensor of the Apple iPhone seized."[150] This warrant was allegedly one of the first of its type to be issued.[151] And just a few

144. *Id.* at 146.
145. *Id.* at 150–51.
146. *Id.* The *Diamond* court was agreeing with *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (11th Cir. 2012), discussed *supra* Subpart II.A, that disclosing a decryption password amounts to a testimonial act. *Id.* at 1346.
147. *See Diamond*, 890 N.W.2d at 150.
148. For a discussion of these cases with respect to the Self-Incrimination Clause, see *supra* Subparts II.A–II.B.
149. Gilbert v. California, 388 U.S. 263, 266–67 (1967).
150. Brewster, *supra* note 12.
151. *Id.*

months later, a similar warrant was issued—also in the Central District.[152] Surprisingly, the second warrant was even more far-reaching than the February warrant. The government, in its memorandum, asked for "authorization to depress the fingerprints and thumbprints of *every person* who is located at the SUBJECT PREMISES during the execution of the search and who is reasonably believed by law enforcement to be the user of a fingerprint sensor-enabled device . . . ."[153] Thus, not only were law enforcement officials given the authority to bypass a phone's biometric password, but they were allowed to engage in a guessing game in which they would press multiple individuals' fingerprints on a phone until that phone unlocked.

C. Applying the Framework to the iPhone X

In August 2018, the FBI forced an iPhone X user to unlock his iPhone using Face ID.[154] The FBI seized the phone pursuant to a search warrant, and then told the individual to put his face in front of the phone.[155] Significantly, this is the first known case of an individual being compelled to unlock an iPhone using his or her face.[156] It certainly will not be the last case, as the growing prevalence of facial recognition technology will force courts to grapple with this issue.[157] Are courts likely to follow this precedent, or will they extend Fifth Amendment protection to individuals who use their face as their password?

Given how courts have applied the *Doe* framework to fingerprint passwords, it is likely that individuals who use Face ID and similar technologies cannot invoke

152. Thomas Brewster, *Feds Walk Into a Building, Demand Everyone's Fingerprints to Open Phones*, FORBES (Oct. 16, 2016, 12:30 PM), http://www.forbes.com/sites/thomasbrewster/2016/10/16/doj-demands-mass-fingerprint-seizure-to-open-iphones [http://perma.cc/5QCA-45MU].

153. *Id.* (first emphasis added); *see also* Memorandum of Points and Authorities in Support of Search Warrant Application, *In re* Apple iPhone Seized During Execution of a Search Warrant, No. ED 15-0451M, 2016 WL 618401, at *1 (C.D. Cal. May 9, 2016), http://www.documentcloud.org/documents/3143273-Mass-Fingerprint-Case-Redacted-Copy-1.html.

154. Thomas Brewster, *Feds Force Suspect to Unlock an Apple iPhone X With Their Face*, FORBES (Sept. 30, 2018, 10:01 AM), http://www.forbes.com/sites/thomasbrewster/ 2018/09/30/feds-force-suspect-to-unlock-apple-iphone-x-with-their-face [http://perma.cc/7LFP-GGSV].

155. *Id.*

156. *Id.*

157. *See supra* notes 44–45 and accompanying text. Notably, the interplay between biometric passwords and the Fifth Amendment quickly arose with the advent of fingerprint passwords. Apple released the iPhone 5s in September 2013, which gave users the ability to use fingerprint passwords. *See* Press Release, Apple, *supra* note 31. *Commonwealth v. Baust*, which held that fingerprint passwords can be compelled, was decided just over a year later, in October 2014. No. CR14-1439, 2014 WL 10355635, at *4 (Va. Cir. Ct. Oct. 28, 2014).

the Fifth Amendment. If one accepts the premise that a fingerprint password does not require an individual to communicate knowledge of factual information to the government,[158] then naturally, one should accept the argument that an individual's face password also does not communicate knowledge when it is used to unlock a phone. Both instances do not require verbal communication, and in neither case is the individual explicitly conveying the contents of his or her mind. Additionally, an individual's face is bodily evidence that can serve as an identifying characteristic.[159] This allows courts to wrongfully point to cases such as *Holt* and *Schmerber* to argue that compelled disclosure of physical evidence is not testimonial evidence.[160]

Therefore, under the current *Doe* framework, future courts will likely conclude that compelling people to unlock their phone with their face does not violate the Self-Incrimination Clause.[161] Put another way, courts will view an individual's face as a "key to a wall safe." But even if a biometric password amounts to a "key to a wall safe," there is a fundamental question that courts are sidestepping: What happens when that same wall safe can be opened by both a combination and a key?

D. Why the Framework Must Evolve

Just because an application of *Doe* would allow law enforcement to compel an individual to open a smartphone by using that individual's face, it does not mean that this result is proper. Rather, an application of the current *Doe* framework to Face ID—and more broadly, biometric authentication—can lead to many negative externalities, both from a legal and practical point of view.

158. *See, e.g.*, *Baust*, 2014 WL 10355635, at *4 (holding that a defendant could be compelled to unlock his iPhone using his fingerprint because it did not require him to "communicate any knowledge").
159. *Cf.* Lemus, *supra* note 106, at 553–54.
160. *See, e.g.*, State v. Diamond, 890 N.W.2d 143, 150–51 (Minn. Ct. App. 2017) ("[T]he task that [the defendant] was compelled to perform—to provide his fingerprint—is no more testimonial than furnishing a blood sample, providing handwriting or voice exemplars, standing in a lineup, or wearing particular clothing.").
161. *See* Jay Stanley, *Apple's Use of Face Recognition in the New iPhone: Implications*, ACLU (Sept. 14, 2017, 3:15 PM), http://www.aclu.org/blog/privacy-technology/surveillance-technologies/apples-use-face-recognition-new-iphone [http://perma.cc/U7LS-H67K] (hypothesizing that courts will approach Face ID in the same way that they approached Touch ID); *cf.* Lemus, *supra* note 106, at 553 (concluding that courts would likely find that compelled production of a fingerprint is a nontestimonial act).

1. Legal Consequences

The legal consequences of the current framework are simple. If courts continue on their current trajectory, and there is no change in the *Doe* framework, then individuals who elect to use technologically safer passwords, such as Face ID, waive their Fifth Amendment rights. But just because an individual owns an iPhone X does not mean that Face ID must be activated.[162] Rather, an individual can just choose not to activate Face ID and instead use a passcode or alphanumeric password.[163] This means that individuals will be able to choose the law that applies to them based on the type of password they set. The result of this is that individuals who elect for more security are forced to give up legal protections.[164]

Additionally, those who are tech-savvy will more likely be able to protect their phone's contents from disclosure if a police officer seeks to execute a warrant. A subtle feature of the iPhone X allows users to turn off facial recognition technology discreetly. For example, an iPhone X user can deactivate Face ID by pressing and holding the side button at the same time as one of the volume buttons for about two seconds.[165] Deactivating Face ID forces the user—or anyone who has access to the user's phone—to input the user's password to unlock the iPhone.[166]

162. *Can You Use iPhone X, XS, XR Without Face ID? Yes! Face ID Questions, Answered*, OS X DAILY (Nov. 10, 2017), http://osxdaily.com/2017/11/10/can-use-iphone-x-without-face-id [http://perma.cc/VBU8-GEXU].

163. *Id.*

164. However, all individuals who use smartphones—regardless of the type of password that they use—are at risk of having law enforcement bypass their password through the use of a third party to unlock the phone. Recently, Apple and the government clashed on this issue, when Apple refused to assist the FBI in unlocking the San Bernardino gunman's smartphone. *See* Weber, *supra* note 19, at 476. The clash ended when the government accessed the phone without the assistance from Apple. *Id.* at 477. However, this left open the question of whether smartphone manufacturers, such as Apple and Google, can be compelled to assist the government in unlocking a device that the company manufactured. *See id.* Until now, the Supreme Court has not ruled on this issue. *See id.* at 485. However, just as with the San Bernardino case, there are independent companies that offer devices that can crack a smartphone password. *See, e.g.*, Zack Whittaker, *For $15,000, GrayKey Promises to Crack iPhone Passcodes for Police*, ZDNET (Mar. 19, 2018, 12:32 PM), http://www.zdnet.com/article/graykey-box-promises-to-unlock-iphones-for-police [http://perma.cc/5ZL2-YVWB] (discussing a private company that sells a $15,000 product to police departments to assist them in cracking iPhone passcodes).

165. APPLE, *supra* note 9, at 2. Another way that Face ID can be deactivated is by restarting the iPhone. APPLE, *supra* note 9, at 2; *see also* Jake Peterson, *Quickly Turn Off Face ID on the iPhone X*, GADGET HACKS (Nov. 4, 2017, 10:13 AM), http://ios.gadgethacks.com/how-to/quickly-turn-off-face-id-iphone-x-0180055 [http://perma.cc/X6CT-GKUM] (explaining the different ways in which Face ID can be deactivated, which forces the user to input his or her password to access the phone).

166. *See* Peterson, *supra* note 165.

One can imagine a situation in which this subtle trick could protect an individual. If officers execute a warrant to seize an iPhone X, and the phone has Face ID activated, then technically, the officers could unlock the phone by pointing the phone toward the user's face.[167] But if the iPhone user quickly and subtly deactivated Face ID prior to the warrant's execution, then the officers could not ask the individual for the numeric or alphanumeric password. While such a mechanism is quick and requires no expertise, it must be known by the user in the first place. Given that the explanation for this mechanism is buried in an online PDF that most iPhone users will probably never read,[168] the chances that an individual would even know this appear slim. Essentially, the law would be rewarding tech-savvy smartphone users.

Another legal consequence is that the lack of protection of biometric passwords could bleed into a lack of protection for traditional passwords. For example, in *State v. Stahl*, the court refused to grant protection to an individual's iPhone passcode.[169] But in so holding, the court stated that it was "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."[170] Essentially, the court tried to level the playing field between all smartphone users by taking away legal protection from those who use traditional passwords, as opposed to granting legal protection to those who use biometric passwords. Given that the *Doe* framework should protect traditional passwords, this result illustrates a regression of the law.

Finally, biometric authentication is not going anywhere. Quite the contrary, it seems to be expanding. Apple has been incredibly successful with the iPhone X, and other technology companies have already explored the possibility of implementing facial recognition in future devices.[171] The more that individuals

167. In fact, a similar situation actually occurred. As mentioned *supra* Subpart III.C, police officers unlocked an iPhone X by executing a warrant and instructing the individual to look directly at his iPhone. *See supra* notes 154–156. Had this individual disabled Face ID, the police officers could not have compelled him to unlock his iPhone using his passcode.

168. *See* APPLE, *supra* note 9. When a consumer purchases an iPhone X, the consumer receives a written manual and instructions. However, these materials do not explain how to quickly deactivate Face ID in the same way described in the online PDF. HELLO: WELCOME TO IPHONE, APPLE (2018) (iPhone X manual on file with author).

169. State v. Stahl, 206 So. 3d 124, 136–37 (Fla. Dist. Ct. App. 2016).

170. *Id.* at 135. Of course, the court's reasoning was premised on its belief that producing a biometric password is not testimonial and that biometric passwords would therefore not receive Fifth Amendment protection.

171. *See supra* notes 44–45 and accompanying text (explaining how smartphone and non-smartphone companies alike have already begun implementing, or are in the process of implementing, facial recognition technology in their devices).

possess devices that are protected by biometric passwords, naturally, the more we can expect to see instances of individuals being forced to incriminate themselves. And as such technologies become more common, it is even possible that traditional passwords will be eliminated altogether in lieu of biometric passwords. This would be the worst-case scenario for technology users from a legal standpoint, since there would be no legal protection to fall back on should one elect to forgo a biometric password.

2. Practical Consequences

Setting aside legal consequences, there are also practical reasons why the law should evolve. As discussed in Part I, smartphones are a staple in day-to-day life, and they are only becoming more popular. Yet many security concerns were also explored in Part I. Traditional passwords can be hacked easily, and the difference in security between a traditional password and biometric password is too significant to go unnoticed.[172] Thus, without a biometric password, individuals who divulge private information into their smartphones are exposed to increased security risks.

This throws people into a dilemma: They can choose either legal protection or increased security, but they cannot have both. And whichever option they choose will force them to have less of the other. If an individual uses Face ID because she wants to decrease the chance of her iPhone X being hacked, she thereby puts herself at risk of having to incriminate herself in the future. But if an individual disables Face ID to increase her legal protection against self-incrimination, then she is exposing herself to an increased risk of having her password hacked.

While forcing individuals to make such a choice may seem unfair, the real harm is that it disincentivizes individuals from adopting emerging technologies. Individuals may forgo biometric passwords and instead elect legal protection, especially if increased litigation sheds light onto the legal consequences of using a biometric password.[173] However, the main utility of Face ID and other forms of biometric passwords is rooted in the increased security that they provide. These biometric passwords are needed to meet the increased security

172. *See supra* notes 21–27, 33–35, 46–47 and accompanying text (discussing the shortcomings of traditional passwords).

173. It is quite possible that there would be increased litigation over compelling an individual to produce his or her face to unlock an iPhone X. In his Comment, Efren Lemus argues that there is a "growing governmental interest in accessing the information stored in its citizens' mobile devices." Lemus, *supra* note 106, at 544. To support this, Lemus cites that "[i]n 2012, federal and local law enforcement agencies made more than 1.1 million requests for the personal cellphone data of Americans." *Id.* (citation omitted).

demands of consumers in an era dominated by smartphones. But by disincentivizing the use of biometric passwords, the current legal framework prevents consumers from taking full advantage of technologies that allow them to protect themselves.

Additionally, society may eventually reach a point in which traditional passwords are no longer an option for smartphones. In this case, users would be forced to use a biometric password if they want to password-protect their device. This is not an unrealistic trajectory, since biometric passwords provide increased security to smartphone users, and smartphone users have made it clear that they prefer such passwords.[174] Of course, this leads to another dilemma: Individuals will have to forgo use of a smartphone altogether if they want to avail themselves of increased legal protections, or they can accept the potential legal consequences so that they may enjoy the benefits and conveniences of a smartphone. Outdated legal rules should not deter individuals from adopting new technologies, especially when those technologies provide social benefits.

But of course, smartphones—let alone Face ID—were probably not a technology that the Supreme Court foresaw when it was deciding cases such as *Doe*, *Wade*, and *Gilbert*.[175] When the Justices framed the rule of what constitutes a testimonial act, they did so in light of the information they had in front of them. So, it is understandable why there is currently a mismatch between technology and the law. But just because it is understandable does not mean that it is acceptable. Technology should not backtrack to meet the law. Rather, the law should progress to keep pace with technology.

IV. A NEW FRAMEWORK

The Fifth Amendment must extend protection to guard against compelled disclosure of biometric passwords. In the case of an iPhone X, an individual should not be compelled to use his or her face to unlock the phone. However, it is likely that courts will arrive at this conclusion only if the *Doe* framework evolves to

174. *See* Press Release, IBM, *supra* note 46. In a related context, the appeal of biometric passwords has led Microsoft and Facebook to make efforts at completely eliminating traditional passwords in lieu of biometric passwords. Selena Larson, *Beyond Passwords: Companies Use Fingerprints and Digital Behavior to ID Employees*, CNN (Mar. 18, 2018, 3:53 PM), http://money.cnn.com/2018/03/18/technology/biometrics-workplace/index.html [http://perma.cc/JT6A-LR5P]. This illustrates how biometric passwords are not only supplementing traditional passwords but can actually replace them.

175. Notably, in 2014 Chief Justice Roberts of the Supreme Court wrote that "[a] smart phone . . . was unheard of ten years ago . . . ." *Riley v. California*, 134 S. Ct. 2473, 2484 (2014). *Doe*, on the other hand, was decided in 1988. Doe v. United States, 487 U.S. 201 (1988).

recognize that a subset of compelled acts—that do not facially appear testimonial—merit a similar degree of constitutional protection as testimonial acts. Only by adapting the law in this way can courts remain true to the values that underlie the current doctrine.

A. Taking *Doe* One Step Further

This Comment proposes an expansion of the *Doe* framework through a two-step analysis. Step one is the traditional *Doe* question: Is the compelled act testimonial in nature? If it is testimonial, then the inquiry is finished because the act is protected by the Fifth Amendment.[176] But if it is not, step two asks: Does the compelled act evolve from a testimonial act? If the answer is yes, then the compelled act is also testimonial in nature, which merits protection under the Fifth Amendment.

Applying this framework to the iPhone X would proceed as follows. First, is compelling an individual to unlock an iPhone with his or her face testimonial? Given the cases and warrants that have already been issued, a court would probably rule that it is not.[177]

Second, is unlocking an iPhone with someone's face an act that evolved from a testimonial act? It is in this step that iPhone users would find protection. This is because using a face to unlock an iPhone is an act that evolved from inputting a passcode into an iPhone. And generally, inputting an iPhone passcode is considered a testimonial act.[178]

How does one prove that Face ID evolved from iPhone passcodes? First, one can simply look at Apple's press statements. Although some may see Face ID as a technology that was developed for convenience purposes, Apple has made it clear that Face ID was developed to provide increased security to iPhone users.[179] And of course, the reason that passcodes were created for iPhones (or for any device) was to provide users with security. Thus, Face ID can be thought of as providing additional security. More specifically, Face ID was created to have the functional equivalence of a passcode, but in a more secure manner.

176. *See supra* Subpart II.B.
177. *See supra* Subpart III.C.
178. *See supra* text accompanying notes 122–135.
179. *See* Press Release, Apple, *supra* note 1 ("Face ID on iPhone X introduces a revolutionary new way to *securely* unlock, authenticate[,] and pay." (emphasis added)); *see also About Face ID Advanced Technology*, *supra* note 30 ("Learn how Face ID helps *protect* your information on your iPhone . . . ." (emphasis added)); APPLE, *supra* note 9, at 3 ("Face ID is designed to . . . provide robust authentication with a low false match rate, and mitigate both digital and physical spoofing.").

Additionally, one can look at how iPhones operate and see the interaction between Face ID and a passcode. A user cannot activate Face ID on the iPhone X unless that user also sets up a passcode.[180] The user does not actually have to use the passcode, but it must still be activated in order to activate Face ID. This is because if Face ID cannot successfully recognize the original owner's face five times in a row, Face ID becomes disabled, which then forces the user to input his or her passcode in order to access the phone.[181] This means that Face ID and an iPhone passcode are not independent from each other but, rather, interdependent, since they work hand-in-hand to provide an iPhone user with the most advanced security.[182]

Finally, and most importantly, individuals have come to understand that both Face ID and a passcode share a commonality in that they are just different types of passwords. This is because, based on the purpose they serve, both are functionally equivalent in that they prevent intruders from accessing an individual's iPhone. And they both are able to serve this purpose by being unique and private to the owner of the phone. The only real difference is that one is more technologically advanced than the other. Thus, one can conclude that Face ID "evolved" from passcodes, in satisfaction of step two of the proposed framework, which would merit protecting Face ID passwords as testimonial.

B. Why the Framework Works

This proposed framework should be adopted by courts for three reasons. First, it is consistent with the principles of privacy that are rooted within the Self-Incrimination Clause. Second, it allows for equal treatment of all smartphone users. And finally, it takes into consideration that communication today is not the same as communication when *Doe* was issued.

180. APPLE, *supra* note 9, at 2.

181. *Id.* at 2. A user must also input his or her passcode if the iPhone is restarted, if the iPhone has not been "unlocked for more than 48 hours," or if the "passcode hasn't been used to unlock the device in the last 156 hours" and "Face ID has not unlocked the device in the last 4 hours." *Id.* at 2. There are other circumstances that require a user to input a passcode in lieu of Face ID, which can be found in Apple's online manual for Face ID. *See id.* at 2.

182. While this interdependence could become obsolete in the future if biometric passwords completely replace traditional passwords, this would not defeat the analysis. With respect to whether a certain act "evolved" from a testimonial act, a future court would find that biometric passwords and traditional passwords were at some point interdependent, since that is how they are currently related.

1. Principles of Privacy

With respect to the policies rooted in the Self-Incrimination Clause, the Supreme Court has stated, on multiple occasions, that the Self-Incrimination Clause is meant to protect an individual's right to privacy.[183] For example, in the landmark privacy case of *Griswold v. Connecticut*, Justice Douglas, writing for the majority, discussed some of the guarantees contained within the Bill of Rights.[184] In doing so, he argued that certain Amendments contain "zones of privacy."[185] Particularly, he found a zone of privacy in the Self-Incrimination Clause, arguing that it "enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment."[186] This was not unfounded, as Justice Douglas cited to a previous Supreme Court case, in which the Court recognized that the Fifth Amendment served to protect against "governmental invasions of . . . 'the privacies of life.'"[187]

The guarantee of privacy also finds similar support in legal scholarship.[188] Some scholarship suggests that the Self-Incrimination Clause was created in order to protect individuals from the condemnation and moral judgment that one who

183. *See, e.g.*, Murphy v. Waterfront Comm'n of N.Y. Harbor, 378 U.S. 52, 55 (1964) *abrogated by* United States v. Balsys, 524 U.S. 666 (1988) (explaining that the Self-Incrimination Clause "reflects . . . our respect for the inviolability of the human personality and of the right of each individual 'to a private enclave where he may lead a private life.'" (quoting United States v. Grunewald, 233 F.2d 556, 581–82 (2d Cir. 1956))); *see also* Miranda v. Arizona, 384 U.S. 436, 460 (1966); Tehan v. United States *ex rel.* Shott, 382 U.S. 406, 416 (1966); Griswold v. Connecticut, 381 U.S. 479, 484 (1965); United States v. White, 322 U.S. 694, 699–701 (1944); *cf.* Boyd v. United States, 116 U.S. 616, 630 (1886).

184. *See Griswold*, 381 U.S. at 484 ("The foregoing cases suggest that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance.").

185. *Id.*

186. *Id.*; *see generally* R. H. Clark, *Constitutional Sources of the Penumbral Right to Privacy*, 19 VILL. L. REV. 833, 871–81 (1974) (discussing the guarantees of privacy found in the Self-Incrimination Clause).

187. *Griswold*, 381 U.S. at 484 (quoting *Boyd*, 116 U.S. at 630).

188. *See, e.g.*, Robert S. Gerstein, *Privacy and Self-Incrimination*, 80 ETHICS 87, 90 (1970) (arguing that the self-incrimination privilege is supported by privacy rights and that compelled information is a "special sort of information" which is "particularly important for the individual to be able to control"); Robert B. McKay, *Self-Incrimination and the New Privacy*, 1967 SUP. CT. REV. 193, 210–12 (arguing that the privilege against self-incrimination has "deep roots" of privacy); *cf.* Peter Arenella, Schmerber *and the Privilege Against Self-Incrimination: A Reappraisal*, 20 AM. CRIM. L. REV 31, 42 (1982) (identifying the substantive value of mental privacy at the heart of the privilege). Another Comment has even suggested that with respect to biometric passwords, courts should abandon the testimonial distinction between physical acts and communications altogether, and instead limit the government's access to individuals' smartphones on the basis of privacy. *See* Lemus, *supra* note 106, at 554–56.

confesses his guilt must confront from within his community.[189] The argument suggests that it is the individual's public admission which leads to condemnation.[190] In other words, it is the intrusiveness into an individual's private life which justifies protecting that individual from self-incrimination.[191]

Other scholarship is in accordance with Justice Douglas's view that there are zones of privacy within the Bill of Rights. For example, Robert B. McKay explored how the provisions of the Bill of Rights reinforce each other, and how the relationship between the Fourth and Fifth Amendment reinforces the privacy interest found in the Fifth Amendment.[192] In discussing these two Amendments, McKay notes:

> If it is not at once obvious why the Fourth and Fifth Amendments reinforce each other's commands and prohibitions, brief reflection will demonstrate their close kinship. A search without a warrant is like an unwarranted demand for the production of private papers, and both should be forbidden for reasons that have as their common denominator the twin policy objectives of preserving morality of government and preserving the privacy of the individual.[193]

In turning to the proposed framework, the extended protection will help make the zone of privacy that can be found in the Self-Incrimination Clause more realistic for smartphone users. On the most fundamental level, the new framework would provide protection from compelled disclosure of a password, which is an extremely sensitive piece of information. In its nature, a password is considered private—whether biometric or not—since it is meant to be unique, not usually shared with others, and something that no one besides its creator should know. And notably, a biometric password is even more private in its nature, since the "password" is located on an individual's body.

189. *See* Gerstein, *supra* note 188, at 90–91.
190. *See id.*
191. *See id.* at 92 ("It is this self-knowledge which is revealed to the public in the process of self-incrimination; what is involved is the laying bare of the innermost recesses of conscience."). *But cf.* David Dolinko, *Is There a Rationale for the Privilege Against Self-Incrimination?*, 33 UCLA L. REV. 1063, 1108–09 (1986) (rejecting privacy as a justification for the Self-Incrimination Clause, since the privilege protects an individual's private information from disclosure only if the individual is compelled, but not if the information is disclosed by someone else).
192. McKay, *supra* note 188, at 211–12.
193. *Id.* at 212. To further support his argument that the Amendments give meaning to each other, McKay also argues that there is a relationship between the First and Fifth Amendments. *Id.* at 212–13. He states that the "First Amendment notion that no man may be compelled to worship or to speak in any particular way—or at all—may be regarded as an enlarged version of the more specific Fifth Amendment notion that no man shall be required to convict himself out of his own mouth." *Id.* at 212.

But even more importantly, the proposed framework will protect the information that a password seeks to protect, which are the contents within a smartphone. Once a device is password-protected, an individual has a certain privacy interest over that device. Even the Supreme Court has agreed that there is something inherently different about individuals' privacy interests with respect to their cellphones. In the landmark *Riley v. California* case, which made it illegal to conduct a warrantless search of a cellphone, Chief Justice Roberts remarked that "[m]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'"[194] And the ability to password-protect a smartphone with a physical feature may lead to an even greater amount of sensitive information being stored on smartphones, since biometric passwords may give individuals a newfound sense of security.[195] Thus, the proposed framework aims to fill this gap between smartphone users' expectations of privacy and the reality of their privacy rights. By protecting smartphone users from being compelled to disclose their biometric passwords, the proposed framework will help smartphone users realize the "zone of privacy" to which they should be entitled.

2. Equal Treatment

Second, the proposed framework will allow for consistency among self-incrimination cases involving smartphone passwords. With the current *Doe* framework, an application of the law creates a distinction between two types of technology users. On the one hand, there are those who use a biometric password (or a biometric password along with a traditional password). On the other hand, there are those who exclusively use a traditional password. Individuals in the former group lose their ability to assert the right to be free from self-incrimination merely because they chose to adopt a more secure technology.[196]

194. Riley v. California, 134 S. Ct. 2473, 2494–95 (2014) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)). In *Riley*, Chief Justice Roberts remarked that a smartphone is "based on technology nearly inconceivable just a few decades ago, when *Chimel* and *Robinson* were decided." *Id.* at 2484 (citing Chimel v. California, 395 U.S. 752 (1969); United States v. Robinson, 414 U.S. 218 (1973)). *Chimel* and *Robinson* were landmark cases in developing the search and seizure doctrine. *Id.* at 2483. Thus, *Riley* serves as a great example of the Supreme Court developing the law further (specifically, the search and seizure clause of the Fourth Amendment) in order to adapt to cellphones, which were a new technology. *See id.* at 2484–85.

195. *See supra* Subpart I.C.

196. This inconsistency in the law was even recognized by a court that believed that unlocking a phone with a biometric password cannot violate the Self-Incrimination Clause. In *State v. Stahl*, the court stated that the Fifth Amendment should not create a division between smartphone users based on the type of password that they use. *See* 206 So. 3d 124, 135

Thus, two individuals who possess the same type of phone, are charged with the same crime, and have the same incriminating information on their phones could not assert the same Constitutional rights if they used different types of passwords.[197] As a result, the law is essentially punishing those who are behaving in a practical manner and deterring individuals from taking advantage of a technology that provides them with increased security.

This is not to suggest that smartphone users should always be able to successfully plead the Fifth. For example, if the government can satisfy the foregone conclusion doctrine, then yes, the government should be able to overcome an individual's right to be free from self-incrimination.[198] And if an individual does not have a password, then that individual cannot avail him– or herself of the Fifth Amendment. Rather, this framework suggests eliminating arbitrary line-drawing between those who can and cannot reach for the Self-Incrimination Clause. And in the case of passwords, it is arbitrary to force a subset of smartphone users to waive their Fifth Amendment rights when those users are still using a password, albeit a biometric one.

3. Redefining Communication

Finally, and most importantly, the proposed framework works because it is not an overhaul of the *Doe* framework. Nor is it calling for a radical test. In fact, this framework retains the central inquiry that courts use in determining if something is testimonial, which is whether the individual is communicating information. What this framework adds, however, is that it allows for evolving considerations of how individuals communicate information, particularly with the growth of new technology.

Now, individuals no longer have to speak to someone in order to communicate their password. Nor do individuals have to write anything in order to communicate it.[199] As oxymoronic as it may sound, communication can be

(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."). The court still held that either password—alphanumeric or biometric—should not be protected as testimonial. *See id.* But the court still recognized that application of the Fifth Amendment to smartphones can lead to inconsistent results.

197. *See supra* Introduction.

198. *See supra* Subpart II.C (explaining how an individual can be compelled to give a password if the government already knows the information that it seeks to compel).

199. Notably, Justice Brennan recognized how the Fifth Amendment cannot be applied mechanically when it comes to physical evidence. In *Schmerber*, Brennan gave the example of lie detector tests, explaining that although they do not require an individual

silent. In the case of the iPhone X, if a law enforcement officer asked, "what is your password?" instead of responding "1234," an individual can simply look at his iPhone X in order to unlock it. Even though the individual is not saying anything, at the heart of his action, the individual is still communicating a password. But of course, under the current *Doe* framework, such a communication may not equate to disclosing "the contents of one's mind." Hence, a new framework, such as the one proposed, must be adopted.

C. Resistance to the Framework

The proposed framework will not be free from critique. The most likely attack will assert that biometric passwords cannot be protected under the Self-Incrimination Clause because a biometric password is a physical trait.[200] This argument has merit, since the Supreme Court has ruled that compelling an individual to display physical characteristics is generally not tantamount to a testimonial act.[201] At first glance, a biometric password, such as an individual's face or fingerprint, seems to fall neatly into this category of physical characteristics that are not protected under the Fifth Amendment.

However, physical characteristics, when used as a password, are different than when used for identification purposes. In the case of a handwriting exemplar, for example, the defendant was asked to display a physical characteristic so that a third party (jury or law enforcement) could compare the defendant's physical characteristic to some benchmark.[202] The same was true when a defendant was compelled to wear a certain article of clothing—it was to allow a jury to make its own determination of whether the defendant was guilty.[203] In both cases, the physical characteristics were used for identification by way of comparison, and the truth of the defendants' statements were irrelevant. With a biometric password, the compelled individual is not forcing over a physical characteristic for purposes of any comparison. There is no third party making an independent determination

to communicate, and by nature, are considered "physical evidence" since they measure changes in body function, such tests "may actually be directed to eliciting responses which are essentially testimonial." Schmerber v. California, 384 U.S 757, 764 (1966).

200. *See e.g.*, Erin M. Sales, Note, *The "Biometric Revolution": An Erosion of the Fifth Amendment Privilege to Be Free From Self-Incrimination*, 69 U. MIAMI L. REV. 193, 223 (2014) (arguing that the Supreme Court would likely treat biometric authentication just like any other compelled exhibition of physical characteristics used for identification purposes, which are not protected under the Self-Incrimination Clause).

201. *See, e.g.*, Gilbert v. California, 388 U.S. 263 (1967); United States v. Wade, 388 U.S. 218 (1967); Holt v. United States, 218 U.S. 245 (1910).

202. *See supra* text accompanying notes 74–79 (discussing *Gilbert*).

203. *See supra* text accompanying notes 53–55 (discussing *Holt*).

of the individual's guilt based on the biometric password that the individual discloses. Rather, the individual's physical characteristic serves as a means to access even more information which in turn can be used against that individual. Thus, even though a biometric password is a physical characteristic, it does not serve the same purpose as other physical characteristics that do not receive Fifth Amendment protection.

Another potential criticism is that the proposed framework would open the door for too much protection. If a biometric password, such as a fingerprint, is granted protection, then what will stop an individual from pleading the Fifth in other contexts where his or her fingerprint can be compelled? For example, what if an officer seeks an individual's fingerprint so that it can be compared to a fingerprint at a crime scene? If a fingerprint can be protected in one context (when it serves as a password), then it can surely be protected in another (when it serves as a means of comparison).

The answer to this concern is that step two of the proposed framework limits when a physical feature, such as a fingerprint, can be protected. This is because in order to grant Fifth Amendment protection to a compelled act, step two of the framework requires a court to specifically find that the compelled act evolved from a testimonial act. While it can certainly be argued that a fingerprint password evolved from a traditional password,[204] it cannot be argued that a fingerprint that is used for purposes of a crime-scene identification evolved from a traditional password or other testimonial act. Context is crucial, and in this example, a fingerprint being used for a password and a fingerprint used for a crime scene investigation are two completely separate contexts. Thus, even though the proposed framework seeks to expand the kinds of communications and acts that are protected under the Self-Incrimination Clause, it does so reasonably and within limits.

D. Scope: Beyond the iPhone X

Although this Comment uses the iPhone X as a case in point, it is not meant to suggest that the problem of the self-incrimination privilege as it pertains to biometric authentication is limited to the iPhone X. Nor does it suggest that the proposed two-step framework can protect only iPhone X users.

Rather, the iPhone X serves as a model to highlight a legal problem that is occurring with biometric passwords. This is particularly true because it is a recent

204. *Cf. supra* Subpart IV.A (arguing that Face ID is a type of password that evolved from a traditional password). The analysis would essentially be the same whether the biometric password is Face ID or a fingerprint.

technology that is impacting other smartphone companies' future products and strategies. And this is critical, since it is estimated that more than one billion smartphones will have facial recognition software by 2020.[205] In turn, this increases the likelihood that the self-incrimination issues that arise with biometric passwords will be further litigated. So, if there is going to be litigation that drives the change for self-incrimination law, it is likely to come from a case involving a smartphone with facial recognition—whether it be the iPhone X or some other smartphone that incorporates the same technology.[206]

But setting aside the iPhone X, the issue of self-incrimination with biometric passwords will become more pervasive as biometric passwords overtake traditional passwords. This is no longer just a likelihood, but it is a reality. Companies in a variety of sectors are aggressively investing in biometric authentication, and some have even commented that they want to get rid of regular passwords altogether.[207] Yet if biometric passwords are not protected from disclosure under the Fifth Amendment even while traditional passwords are still being used, there is even less of a chance that such biometric passwords would be protected if they ever become complete substitutes for traditional passwords.

CONCLUSION

For any biometric password, as well as any device protected by such a password, the analysis under the current *Doe* framework should lead to the same result. That is, an individual cannot withhold his or her biometric password on self-incrimination grounds. This is because based on the current test for what constitutes a testimonial communication or act, a court would have difficulty in determining that the unlocking of a device using one's physical features is testimonial. But the testimonial test was created before biometric passwords existed and became widespread. This should be of great concern to all technology users as society transitions into an era of biometric authentication.

The proposed framework aims to redefine what is protected as testimonial information under the Self-Incrimination Clause by adding an additional step to the traditional inquiry. It seeks to extend protection to individuals who may otherwise lose the privilege against self-incrimination merely because they

205. Hollander, *supra* note 4.

206. It would not be unprecedented for a smartphone to lead the way in influencing constitutional criminal law. In *Riley v. California*, a smartphone was the driving factor behind the Supreme Court's updating of Fourth Amendment "search and seizure" doctrine. *See* 134 S. Ct. 2473, 2494–95 (2014).

207. *See, e.g.*, Larson, *supra* note 174.

adopted a superior password. The framework would allow users who have biometric passwords—regardless of the device and regardless of the physical feature that serves as a password—to avail themselves of the Self-Incrimination Clause. This in turn will allow individuals to take all appropriate measures to protect their devices from thieves and hackers without the law deterring the adoption of biometric passwords.

Whether it be through the proposed framework in this Comment or a new but similar framework, the current *Doe* framework must evolve. Technology will not backtrack in order to meet the law as it stands. Rather, technology will continue to grow. And should courts desire to produce consistent rules and remain true to the values embedded in the Fifth Amendment, they must recognize that the current application of the Fifth Amendment must evolve.