BIOMETRIC PASSWORDS AND THE PRIVILEGE AGAINST SELF-INCRIMINATION♦

The implementation of biometric technology, such as fingerprint and retina scanners, has facilitated the increased security of confidential documents and personal information.[1] The iPhone, for example, allows its owner to merely touch his finger to a sensor and he is assured that no one else will have the ability to access the contents of his phone. However, with these advantages come unforeseen legal implications. The self-incrimination clause of the Fifth Amendment prevents an individual from serving as a witness against himself.[2] Although an individual is constitutionally protected from being forced to testify against himself, the Supreme Court has divided "testimony" into two categories: communicative and physical, with only the former receiving Fifth Amendment protection.[3]

The delineation of these categories prevents law enforcement officials from compelling a suspect to reveal the contents of his mind, which must be communicated, but declines to extend this privilege to physical evidence that is obtained from a suspect's body.[4] This delineation is laid out as follows: "the prohibition of compelling a man in a criminal court to be witness against himself is a prohibition of the use of physical or moral compulsion to extort communications from him, not an exclusion of his body as evidence when it may be material."[5] In the days when an individual's most intimate secrets could only be found within the depths of his own conscience, this type of doctrine made sense.

But what happens when physical evidence, like a fingerprint, is used in place of testimonial evidence, like a password? Both are currently used to guard highly private and personal information, and both are equally deserving of protection from unwarranted government

1 *See, e.g.*, Biometric Software Security Systems, PRIVARIS, http://www.privaris.com/biometric_software.html (last visited Nov. 8, 2014) ("Biometrics add an additional factor of authentication and are therefore a significant improvement in computer security.").

2 2 WILLIAM J. RICH, MODERN CONSTITUTIONAL LAW § 29:1 (3d ed. 2013).

3 Holt v. U.S., 218 U.S. 245, 252–53 (1910).

4 *Id.*

5 *Id.*

intrusion. The use of the fingerprint as a password is a direct link to communicative, as well as potentially incriminating, information, and serves as a replacement for the traditional numeric or alphabetic password, which has recently received Fifth Amendment protection from the judicial system.

Should compelling a person to provide his or her biometric password trigger the privilege against self-incrimination? This Note suggests that such compulsion, specifically of a fingerprint, ought to receive the same protection afforded by the Fifth Amendment privilege against self-incrimination to traditional testimonial evidence. Treating a fingerprint password in this way would be consistent with precedential Supreme Court holdings and would promote the rationale behind the Fifth Amendment,[6] especially its aim to ensure the right of each individual his privacy.[7]

INTRODUCTION 212
II. BACKGROUND OF THE SELF-INCRIMINATION CLAUSE..... 216
A. *Application of the Privilege: The Exclusion of Physical Evidence* 217
B. *The Testimonial Quality of a Physical Act* 219
C. *Limitations on the Privilege*..... 221
D. *The Foregone Conclusion Doctrine* 221
E. *Application of the Foregone Conclusion Doctrine* 223
III: THE PROBLEM CREATED BY BIOMETRIC PASSWORDS 225
A. *The Fingerprint: More Than a Method of Identification* . 226
B. *The Fifth Amendment and Password Protection* 227
IV. POSSIBLE OUTCOMES..... 228
A. *Applicable Recent Case Law* 231
B. *The Fingerprint as a Password Replacement*..... 234
CONCLUSION..... 235

INTRODUCTION

On September 19, 2013, thousands of consumers began lining up at Apple stores across the globe in anticipation of the early morning release of the iPhone 5c and 5s on September 20th.[8] Sales of the new iPhones were projected to exceed all previously released iPhone models. Several factors contributed to those projections: aside from excitement over new designs and technological features, the phones

6 *See* RICH, supra note 2.

7 *See id*. (quoting Murphy v. Comm'n of New York Harbor, 378 U,S. 52 (1964)).

8 Eric Mack, *Hordes hungry for the iPhone 5S and 5C line up at Apple Stores,* CNET (Sept. 29, 2013), http://news.cnet.com/8301-17938_105-57603798-1/hordes-hungry-for-the-iphone-5s-and-5c-line-up-at-apple-stores/.

were initially released in more countries than in previous years.[9] Additionally, this was the first time that Apple released two models at the same time.[10] Within just three days of the phones' release, combined sales of the 5c and 5s had surpassed nine million units—a record-breaking number for first weekend sales.[11] Demand for the phones exceeded the initial supply, and orders continued to be shipped to countries all over the world, including the United States, Australia, China, and Canada.[12]

Much of the appeal of the iPhone 5s was attributed to the many new features that it boasted, including the faster performing A7 processing chip, improved iSight® camera for higher-quality photographs, and advanced iOS 7 software.[13] However, the addition that created the most hype was arguably Apple's introduction of the TouchID™ finger sensor, "an innovative way to simply and securely unlock your iPhone with just the touch of a finger."[14] This technology allows the phone to take a high-resolution image of your finger, which is encrypted and stored locally on the phone's A7 chip.[15]

These new features have been accompanied by new concerns of iPhone users. For instance, some consumers had developed an initial fear that an individual's fingerprint data could be hacked by a thief or accessed by the government, via the iCloud or some other type of centralized database.[16] Reassurances from Apple that a user's fingerprint is loaded and stored locally on the device itself have alleviated these concerns.[17] Still, the transition from password security to biometric identification has created unintended legal dilemmas.

---

9 Charles Arthur, *iPhone 5s and 5c sell 9m in record weekend as Apple shrugs off doubters*, THE GUARDIAN (Sept. 23, 2013), http://www.theguardian.com/technology/2013/sep/23/iphone-5s-5c-apple-record-nine-million (The higher figure is in part due to the new phones going on sale in many more territories than in 2012 and preceding years.).

10 *See id. See also* Poornima Gupta & Jennifer Saba, Apple polishes forecast after selling 9 million new iPhones, REUTERS (Sept. 23, 2013), http://www.reuters.com/article/2013/09/23/us-apple-iphone-idUSBRE98J0LD20130923 ("Sales of the new models were nearly double those of the iPhone 5's 5 million in the first weekend after its launch a year ago, and far surpassed the roughly 6 million that analysts had projected.").

11 Press Release, Apple Inc., First Weekend iPhone Sales Top Nine Million, Sets New Record (Sept. 23, 2013), http://www.apple.com/pr/library/2013/09/23First-Weekend-iPhone-Sales-Top-Nine-Million-Sets-New-Record.html.

12 *Id*.

13 Press Release, Apple Inc., Apple Announces iPhone 5s—The Most Forward-Thinking Smartphone in the World (Sept. 10, 2013), http://www.apple.com/pr/library/2013/09/10Apple-Announces-iPhone-5s-The-Most-Forward-Thinking-Smartphone-in-the-World.html.

14 *Id. See also*, Press Release, Apple Inc., iPhone 5s & iPhone 5c Arrive on Friday, September 20 (Sept. 17, 2013), http://www.apple.com/pr/library/2013/09/16iPhone-5s-iPhone-5c-Arrive-on-Friday-September-20.html.

15 Press Release, Apple Inc., *supra* note 13.

16 Brandon Griggs, *How secure is your iPhone 5s fingerprint?*, CNN (Sept. 15, 2013), http://www.cnn.com/2013/09/12/tech/mobile/iphone-fingerprint-privacy.

17 *Id.*

A great number of modern constitutional law questions surround the struggle to adapt to circumstances that could never have been contemplated at the time of the document's drafting. Often, this struggle is the result of changing societal expectations and developments in technology. At first glance, the iPhone's fingerprint reader may appear to be a minor change in the design and implementation of the latest cell phone to hit the market. Nevertheless, it has the potential to implicate unforeseen legal issues. Previous versions of the iPhone have offered users the option of creating a 4-digit password to protect their device from prying eyes. The newer models eliminate the necessity of memorizing a password in favor of the fingerprint sensor. Designed for easier access and greater security, the TouchID™ finger sensor also raises the question of how the judicial system might treat a subpoena compelling the use of a fingerprint to unlock this type of device. Could government compulsion in this instance trigger an individual's Fifth Amendment rights?

The Fifth Amendment applies to an individual only when he is compelled to make a testimonial statement that is incriminating.[18] The protection extends to any disclosure, "in the form of oral testimony, documents or chattels, sought by legal process against him or her as a witness. The privilege encompasses compelled statements that lead to discovery of incriminating evidence even though the statements themselves are not incriminating and are not introduced into evidence."[19]

As previously mentioned, compulsions have traditionally been categorized as either physical or communicative. The line differentiating physical and testimonial evidence has become blurred by the development of new technology such as the iPhone 5s and its successors. The use of a fingerprint scanner to guard an iPhone's contents from intruders creates a legal problem when physical evidence that is easily obtainable from a suspect's body, i.e., the fingerprint, is used in place of communicative or testimonial evidence, such as an alphanumeric password.[20]

Admittedly, the introduction of the TouchID™ finger sensor does not pose a completely novel legal question, as Apple is not the first company to incorporate biometric technology into personal electronic devices. The technology has previously been integrated into laptops, and has previously been available for tablets and mobile phones.[21]

18 Paul M. Coltoff et al., 31 N.Y. Jur. 2d Criminal. Law: Procedure. § 549 (2014).

19 *Id.*

20 United States v. Kirschner, 823 F. Supp. 2d 665, 668 (E.D. Mich. 2010).

21 *See* Avram Piltch, Lenovo ThinkPad T430u Hands-On: First Ultrabook with Power-On Fingerprint Reader, Removable Bottom, LAPTOP MAG (Jan. 10, 2012), http://blog.laptopmag.com/lenovo-thinkpad-t430u-hands-on-first-ultrabook-with-fingerprint-reader-removable-bottom;

However, the widely popular iPhone places biometric password technology in a mainstream market like never before. On November 1, 2013, the iPhone 5s and iPhone 5c became available for purchase in more than 25 countries around the globe.[22]

Considering the large volume of consumers now utilizing fingerprint sensor scanners on the iPhone, it seems likely that a court will have to address the constitutional protection given to biometric passwords in the near future. This Note will discuss how a court should rule if presented with the question of whether law enforcement could compel an individual to unlock an iPhone, or a similar device secured with a biometric password, through the use of his fingerprint. More specifically, this Note seeks to address the implications of what would occur if a suspect were issued a subpoena compelling him to unlock an iPhone or other digital device with his fingerprint, and whether such a compulsion would be permissible within the confines of the Fifth Amendment. This scenario presents the courts with an issue of first impression, because in the past, a fingerprint was merely used as a method of identification. Now the circumstances are different, because a fingerprint is often used to safeguard private information.

In Part II, this Note will discuss the background and development of the Fifth Amendment's privilege against self-incrimination clause. The clause was originally included in the Bill of Rights to protect the innocent but also advances other policy goals, including the protection of individual privacy.[23] Over the years the court has utilized two main approaches to guide its interpretation of the self-incrimination clause: the physical/communicative dichotomy and the foregone conclusion doctrine. In recent years, however, it seems that a shift away from a classification system has occurred in favor of an individual case-by-case analysis.

Part III will explore the legal questions created by the use of biometric passwords, and why the current framework for the application of the privilege against self-incrimination clause is unequipped to resolve the aforementioned questions. Particularly, that the current framework is ill suited for cases where technology can now perform tasks that traditionally required human action.

Part IV will use previous case law to predict how the Supreme Court would rule if presented with the issue of a government official

see also Fingerprint Scanners enabled for Android tablets & mobiles, PLANET BIOMETRICS (Sept. 26, 2012), http://www.planetbiometrics.com/article-details/i/1272.

22 Press Release, Apple Inc., iPhone 5s & iPhone 5c Arrive in Italy, Russia, Spain & More Than 25 Countries on Friday, October 25 (Oct. 9, 2013), http://www.apple.com/pr/library/2013/10/09iPhone-5s-iPhone-5c-Arrive-in-Italy-Russia-Spain-More-Than-25-Countries-on-Friday-October-25.html.

23 *See* RICH, supra note 2.

compelling the use of a fingerprint to unlock its owner's phone, concluding that in the context of the judicial framework differentiating between communicative and physical evidence, a biometric password is ultimately communicative evidence deserving of constitutional protection. The two categories of interpretation used by the Court have been more of guide rather than a strict classification system, and the Supreme Court has admitted that each situation must be examined on a case-by-case basis. A biometric password such as a fingerprint does not fit neatly into either category, but an examination of the logic developed by the Supreme Court in precedential cases suggests that a fingerprint, when used as a password rather than as a method of identification, possesses the testimonial qualities that should entitle it to the Fifth Amendment privilege against self-incrimination.

II. BACKGROUND OF THE SELF-INCRIMINATION CLAUSE

The self-incrimination clause of the Fifth Amendment provides, "[n]o person . . . shall be compelled in any criminal case to be a witness against himself."[24] It has been left to the lower courts to determine exactly what serving as a witness against oneself entails. Over time, the courts developed a distinction between two types of evidence that can be used to incriminate a suspect: "communications" or "testimonial" evidence, and "bodily" evidence, with only the former receiving Fifth Amendment protection.[25]

The Fifth Amendment privilege first developed from the English principle that an individual could not be expected to testify against himself under oath – whether before a tribunal in a proceeding for a criminal prosecution, before a magistrate investigating an accusation against the suspect, or in a court of equity or common law.[26] After the American Revolution this policy was adopted in several states, and eventually proposed for inclusion into a federal bill of rights.[27] Although its original intent was to protect the interests of the innocent and to further the truth, the purpose of the privilege against self-incrimination has expanded over the years. Application of the privilege has broadened partly in order to adapt to changing societal needs and goals, and partly because of a failure of the court to identify any clear policy objectives for the privilege.[28]

24 U.S. Const. amend. V.

25 *See* Holt v. United States, 218 U.S. 245 (1910).

26 The Constitution of the United States of America Analysis and Interpretation: Analysis of Cases Decided by the Supreme Court of the United States to June 28, 2002, 1361-64, S. Doc. No. 108-17 (2004), http://www.gpo.gov/fdsys/pkg/CDOC-108sdoc17/pdf/CDOC-108sdoc17.pdf.

27 *Id.*

28 *Id.* at 1393 (The following statements are illustrative: "in England and the colonies the privilege was narrower than the interpretation now prevailing, a common situation reflecting the

Today it seems that the court "has settled upon the principle that the clause serves two interrelated interests: the preservation of an accusatorial system of criminal justice, which goes to the integrity of the judicial system, and the preservation of personal privacy from unwarranted governmental intrusion."[29] To further these goals, and to help determine when the Fifth Amendment privilege against self-incrimination should apply, the court has used the distinction between communicative and physical evidence as a useful categorization tool. It can be inferred that information that must be communicated, such as a thought or belief, obtains greater privacy than evidence that can be obtained merely by observing or touching an individual.

A. *Application of the Privilege: The Exclusion of Physical Evidence*

The first case to make the evidentiary distinction between communicative and physical evidence was *Holt v. United States*, where the forcing of a prisoner to put on a blouse so that a witness could identify him was not a compulsion subject to Fifth Amendment protection.[30] The plaintiff was convicted for murder and claimed that evidence obtained while he was under duress should not be admissible in court. On appeal, the Supreme Court denied this objection. Justice Holmes concluded in his opinion, "the prohibition of compelling a man in a criminal court to be a witness against himself is a prohibition of the use of physical or moral compulsion to extort communications from him, not an exclusion of his body as evidence when it may be material."[31] He justified this interpretation by explaining that excluding the use of the body to obtain evidence was illogical because it would prevent a jury from using practical means to identify a suspect, such as comparing a suspect's features with a photograph.[32]

Courts have continuously upheld the doctrine articulated by Justice Holmes where the compulsion to produce physical or "bodily evidence" does not violate the Fifth Amendment. That doctrine has been expanded to include other forms of evidence obtained from an individual's body, including blood samples, writing samples and the results of breath analyzer tests.[33] In *Schmerber v. California*, the plaintiff alleged that his Fifth Amendment privilege against self-incrimination had been violated when a police officer instructed a physician to obtain a blood sample

gradual expansion, or occasional contracting, of constitution guarantees" and "[t]he difficulty is that the Court has generally failed to articulate the policy objectives underlying the privilege, usually citing a 'complex of values' when it has attempted to state the interests served by it.").

29 *Id.* at 1393.

30 Holt, 218 U.S. 245.

31 *Id.* at 252–53.

32 *Id.* at 253.

33 *See* Schmerber v. California, 384 U.S. 757 (1966); Gilbert v. California, 388 U.S. 263 (1967).

without his consent; the sample was used to analyze the alcohol content of the plaintiff's blood after he had been arrested for drunk driving.[34] In *Schmerber*, the Court narrowly interpreted the Fifth Amendment privilege against self-incrimination and held that the clause is only implicated when an individual has the right to remain silent, unless he chooses to speak of his own free will.[35] Because the evidence was obtained from Schmerber's body, and he had in no way been compelled to speak or to produce communicative evidence, his Fifth Amendment rights had not been violated.[36] This case adopted a quite literal interpretation of the clause, where the privilege was not triggered because there was no verbal or written testimony involved.

Under such a literal interpretation of the Fifth Amendment, the compelled act of unlocking a phone with a fingerprint might receive the same treatment as a blood sample by the *Schmerber* court. The *Schmerber* court held that there was no Fifth Amendment violation, not because a blood sample was "physical" evidence, but rather because drawing the suspect's blood did not involve forcing him to communicate.[37] Similarly, pressing a finger to a sensor does not produce testimony in the literal sense. The court in *Schmerber* restricted the self-incrimination clause to a limited application where testimony only in the strictest sense was protected, and any other compelled act fell outside of the scope of protection.

The Court likely adopted this interpretation because it allowed them to follow a "bright line" rule instead of attempting to make a more fully articulated distinction between physical and testimonial evidence.[38] The *Schmerber* court noted that although the two categories of physical and testimonial evidence often can be utilized as a useful framework, trying to make such a distinction had the potential to lead to incongruous results.[39] For example, there is the possibility that a suspect's physical person could be used to elicit an essentially testimonial response.[40] Writing for the majority, Justice Brennan used the example of a lie detector test, which essentially measures changes in bodily function to determine a suspect's guilt or innocence.[41] This example illustrates the difficult situation where the line between physical and testimonial evidence becomes blurry.[42] The *Schmerber*

34 Schmerber, 384 U.S. at 758–59.
35 *Id.* at 763.
36 *Id.* at 765.
37 *Id.* at 761.
38 *Id.* at 764.
39 *Id.*
40 *Id.*
41 *Id.*
42 *Id.*

Court chose to avoid the very difficult issue of addressing the potential testimonial quality of an intoxicated suspect's blood sample, and instead, it opted for the strict exclusion of non-communicative evidence.

However, this early case is not indicative of the Supreme Court's subsequent treatment of evidence obtained from a suspect's physical person. In fact, Justice Black's dissent in *Schmerber* foresaw the approach that the Supreme Court would take in the future to evaluate the testimonial qualities of physical evidence.[43] Justice Black opposed the majority's strict interpretation of the Fifth Amendment, arguing that compelling an individual to allow a doctor to puncture the plaintiff's blood vessels in order to analyze his blood's alcoholic content was the equivalent of forcing him to testify against himself.[44] Although not oral testimony, the blood sample communicated to a court and jury that Schmerber was drunk and, consequently, guilty.[45]

> The sole purpose of this project which proved to be successful was to obtain 'testimony' from some person to prove that petitioner had alcohol in his blood at the time he was arrested. I think it unfortunate that the Court rests so heavily . . . on the words 'testimonial' and 'communicative.'[46]

Years later, the Supreme Court's dissatisfaction with the dichotomy between physical and communicative evidence has continued to persist, resulting in confusion over how to apply the privilege against self-incrimination in modern case law. Instead of attempting to resolve the confusion surrounding the physical and communicative distinction, the Court has continued to apply the framework on a case-by-case basis. On one hand, this method is useful because it provides for flexibility when new or unusual circumstances arise, such as the discussion here on biometric passwords. However, the downside of a case-based analysis is that civilians are prevented from foreseeing the consequences of their actions or to what extent their actions are protected. In a society where individual privacy is so highly valued, it is especially necessary that individuals know how much of their confidential information is accessible to the government.

B. *The Testimonial Quality of a Physical Act*

The question of whether the production of bodily evidence could maintain a testimonial quality, briefly touched upon in the *Schmerber*

43 *Id.* at 773–75 (Black, J., dissenting).
44 *Id.*
45 *Id.*
46 *Id.* at 774.

dissent, was revisited in *Doe v. United States*.[47] However, the Court avoided a definitive resolution of the question by focusing instead on the narrow issue presented by this particular case, that compelling the suspect of a criminal investigation to sign a directive authorizing foreign banks to release his account records was not a violation of the Fifth Amendment.[48]

The district court had held that, by signing the release, Doe was performing a testimonial act because his signature served as an admission of his control of the accounts. Thus, the signature could be used to prove his guilt.[49] On appeal the Supreme Court agreed that Doe's signature on the directive could potentially be incriminating because it provided a link in the chain that would lead the government to the suspect's indictment. Nevertheless, the Court ultimately held that compelling his signature was not a violation of the privilege against self-incrimination. The *Doe* Court accepted the government's argument that the act itself had no testimonial quality, "because neither the directive itself nor Doe's execution of the form discloses or communicates facts or information."[50] The consent directive was worded in such a way that it authorized the foreign banks to release any and all account records over which Doe had a right of withdrawal, without acknowledging that such accounts existed or that the petitioner had control over them.[51] Because it did not convey any information to the government, either implicitly or explicitly, Doe's signature had no testimonial significance.[52]

Here, the issue debated in *Schmerber* resurfaces. By signing his name to the directive, Doe was arguably communicating to a court and jury that he was connected to the suspected crime. But, because Doe's release of the documents did not expressly indicate his ownership of them, the privilege was not triggered. Justice Stevens' dissent is indicative of the ever-present challenge faced by the Supreme Court in attempting to delineate between physical and testimonial evidence.[53] Stevens argued that forcing Doe to sign the directive was synonymous with compelling him to use his mind to aid the government, and as a result should be treated as a testimonial act rather than as the physical production of evidence.[54]

Although the Court's holding would indicate otherwise, it seems

47 Doe v. United States, 487 U.S. 201 (1988).
48 *Id.*
49 *Id.* at 204.
50 *Id.* at 208.
51 *Id.* at 201.
52 *Id.*
53 *Id.* at 219–20 (Stevens, J., dissenting).
54 *Id.*

that having the authority to release confidential documents, although not necessarily indicative of ownership, is evidence of some degree of control and would tell a jury that Doe was connected to the bank account. A similar issue would likely arise in a case concerning a fingerprint used to lock an iPhone: although a phone could certainly contain files not owned or created by the fingerprint's owner, the fact that a person has the authority to access that information seems like strong evidence of a connection to the suspected criminal activity.

The question of whether the production of physical evidence could retain a testimonial quality ought to play a key role in a court's determination of how to treat biometric passwords. As preciously discussed, it has been established that a signature is purely bodily evidence.[55] But if the facts had been slightly different in *Doe*, the petitioner's act of signing the directive may have triggered the privilege against self-incrimination. Similarly, under the right circumstances a fingerprint should also be eligible for Fifth Amendment protection. If the Supreme Court were to hold that a physical act could retain a testimonial quality, thus setting a precedent that has long been deliberated in dicta and dissents, then potentially incriminating physical compulsions could become entitled to Fifth Amendment protection.

C. *Limitations on the Privilege*

There are two situations that prevent a suspect from invoking his privilege against self-incrimination. The first arises if the suspect receives a grant of immunity. The government can compel an individual to testify against himself, so long as any information acquired from his compelled testimony cannot later be used against him.[56] A court cannot issue this immunity; a government prosecutor must apply it for it.[57] The second situation, known as the "foregone conclusion doctrine," is discussed in detail below.

D. *The Foregone Conclusion Doctrine*

The government may also use compelled testimonial evidence if the information obtained from the compulsion was a foregone conclusion. The Supreme Court established this doctrine in *Fisher v. United States*, where taxpayers were summoned to produce documents related to an investigation of possible civil or criminal liability under the federal income tax laws.[58] The defendant taxpayers argued that because

55 *Id.* at 201.

56 Rich, Modern Constitutional Law, *supra* note 2.

57 *See* 18 U.S.C.A. §§ 6002–03 (2010).

58 Fisher v. United States, 425 U.S. 391 (1976). In *Fisher*, the Supreme Court considered two cases, one in the Fifth Circuit and one in the Third Circuit. In both cases, the IRS issued a summons to obtain documents taxpayers had given to their attorneys. When the attorneys denied

the documents would incriminate them, a subpoena compelling production of the papers violated the privilege against self-incrimination. Here, the Supreme Court disagreed, holding that though the production of the papers involved compulsion, "it does not compel oral testimony; nor would it ordinarily compel the taxpayer to restate, repeat, or affirm the truth of the contents of the documents sought."[59]

The Court also explained that even though the government forced production of the papers, the documents themselves were voluntarily created, so they could not be said to contain compelled evidence.[60] In other words, the defendants were not compelled to *produce* incriminating evidence, only to hand over information that was already in existence.[61] Therefore, the Court held that however incriminating the documents themselves might have been, the act of producing them in itself did not rise to the level of testimony protected by the Fifth Amendment.[62] As a result, the taxpayers could not avoid the subpoena just because the compulsion could lead to prosecution.[63]

Although the compulsion in *Fisher* was aimed at the performance of a physical action, handing over the incriminating documents was arguably testimonial in that it indicated the petitioners' control over the documents. The Supreme Court acknowledged that the act of production itself could exhibit testimonial qualities, and that "these questions perhaps do not lend themselves to categorical answers."[64] Justice White, writing for the majority, concluded that, "the act of producing evidence in response to a subpoena nevertheless has communicative aspects of its own," because it concedes the defendant's ownership and acknowledgement of the contents of the evidence produced.[65] However, the Court indicated that the nature of the act of production should be determined on a case-by-case basis, and in *Fisher*, the testimonial aspect of producing the papers did not reach a level that warranted constitutional protection.

The Courts in *Schmerber*, *Doe* and *Fisher* ultimately reached the same result, holding that a defendant's incriminating act, even if implicitly communicative, was not entitled to constitutional protection. But in *Fisher*, the reasoning behind the decision was different than that used in the preceding cases. Fisher's act was not non-communicative

the summons and invoked the Fifth Amendment privilege, the IRS brought an enforcement action. Both district courts ordered the attorneys to comply with the summons, and the decisions were appealed.

59 *Id.* at 409.

60 *Id.* at 409–10.

61 *Id.*

62 *Id.* at 410–11.

63 *Id.* at 410.

64 *Id.*

65 *Id.*

because it was physical; rather, it was non-communicative because it did not provide the government with any information that it did not already know. Thus, *Fisher* introduced a new guideline to help the court reach its decision, one that moved beyond placing the defendant's action into a strict classification of either communicative or physical evidence.

The reasoning used by the *Fisher* court to reach its decision is what has come to be known as the "foregone conclusion" doctrine.[66] This doctrine suggests that if the government is not relying on a defendant's compelled testimony for substantive information, then the contents obtained are a "foregone conclusion," and "no constitutional rights are touched. The question is not of testimony but of surrender."[67] In *Fisher*, the government knew who had owned and prepared the documents, as well as their location. The testimony of the defendant, regardless of whether it was communicative or physical, added little to the government's information, so the defendant's cooperation did nothing to aid the government's case against him. If the circumstances had been different, and Fisher's production of the documents would have served as an admission of his guilt, then the Court may have reached a different result.

E. *Application of the Foregone Conclusion Doctrine*

The foregone conclusion doctrine has become a useful tool in the Supreme Court's attempt to interpret the privilege against self-incrimination. For example, the government was forced to dismiss charges against a defendant who had been indicted for several federal crimes in *United States v. Hubbell*.[68] The defendant moved for dismissal because his tax and fraud charges were dependent on evidence produced under compulsion and in violation of his Fifth Amendment rights.[69] On appeal, the government could not show that it had any way of knowing the location or ownership of the documents without obtaining the documents themselves.[70] Because the government did not have any associated facts prior to Hubbell's production of the documents, any information obtained as a result of the compulsion was not a foregone conclusion. Justice Stevens, writing for the majority, explained that "the testimonial aspect of respondent's act of producing subpoenaed documents was the first step in a chain of evidence that led to this

66 *See* United States v. Hubbell, 530 U.S. 27 (2000); United States. v. Fricosu, 841 F. Supp. 2d 1232 (D. Colo. 2012).

67 Fisher, 425 U.S. at 411 (citing In re Harris, 221 U.S. 274, 279 (1911)).

68 530 U.S. 27 (2000)

69 *Id.*

70 *Id.* at 32.

prosecution."[71] The Court reasoned that the defendant was required to use the "contents of his own mind" in order to identify and locate hundreds of documents requested by the government.[72] Hubbell's act of production retained the requisite level of testimonial quality required thus entitling his actions to constitutional protection.

Unlike *Fisher*, which also involved a subpoena compelling the production of incriminating documents, the government in *Hubbell* would not have been able to obtain the information necessary for Hubbell's indictment without his cooperation. Hubbell was undeniably assisting in his own conviction. Such a compulsion showed blatant disregard of the self-incrimination clause.

The foregone conclusion doctrine would have an important effect on the outcome of a case involving the compulsion of a fingerprint for the purpose of unlocking a cellular phone or similar device. Just like signing a document could serve as an admission of guilt and a communication of knowledge to the government, so too could the act of pressing a finger on the scanner of a digital device. Perhaps even more so; since providing law enforcement officials with access to a locked device indicates knowledge and ownership of all files and documents stored within, doing so may effectively aid the government in its case against the device's owner. Only those who register their fingerprint with the device can use it as a security measure. A strong argument could be made that having an individual's fingerprint registered on a device testifies to his ownership, or at the very least control of, the phone.

Whether the foregone conclusion doctrine would ultimately apply in a case would require more fact-specific information. As previously mentioned, the standard is whether or not the compulsion adds anything to the government's knowledge.[73] In the context of a cell phone, this could be anything from a text message detailing the events of a certain day, to an individual's contact information. Therefore, just because the registration of a fingerprint may attest to a phone's ownership, it would not necessarily act as a bar to Fifth Amendment protection.

The previously discussed doctrine and case law have allowed the Supreme Court to develop a flexible framework through which to determine whether a compelled act is testimonial within the confines of the Fifth Amendment. Today, the court continues to look at the individual facts and circumstances of particular cases rather than adopting narrow guidelines. Although there has been a great deal of progress since the early decisions that classified evidence as strictly

71 *Id.* at 42.

72 *Id.* at 43 (quoting Curico v. United States, 354 U.S. 118, 128 (1957)).

73 *Supra* note 67.

"communicative" or "physical," the development of technology requires the Court to continuously reevaluate Fifth Amendment interpretations, creating a need for a constant reevaluation of the current doctrine. Perhaps the Supreme Court's decision to examine each case on an individual basis, rather than to delineate specific rules, is the practical route to take as technological advancements continue to introduce new factual scenarios to the testimonial landscape.

III: THE PROBLEM CREATED BY BIOMETRIC PASSWORDS

If evidence obtained from a suspect's person is considered "physical" evidence, it follows that compelling an individual to provide law enforcement officials with a fingerprint would fall neatly within the categorical framework utilized by the judicial system, and thus be excluded from Fifth Amendment protection. It would seem that a fingerprint is clearly "physical" evidence obtained from the body. In explaining the Court's decision in *Schmerber*, Justice Brennan, writing for the majority, stated that "both federal and state courts have usually held that it offers no protection against compulsion to submit to fingerprinting, photographing, or measurements, to write or speak for identification, to appear in court, to stand, to assume a stance, to walk, or to make a particular gesture."[74]

This position is affirmed by state criminal procedure statutes which allow law enforcement officials to compel the production of an individual's fingerprint while offering minimal opportunity for protection against such compulsion to the suspect himself.[75] Consider the following New York statute:

> Following an arrest, or following the arraignment upon a local criminal court accusatory instrument of a defendant whose court attendance has been secured by a summons or an appearance ticket under circumstances described in sections 130.60 and 150.70, the arresting or other appropriate police officer or agency must take or cause to be taken fingerprints of the arrested person or defendant if an offense which is the subject of the arrest or which is charged in the accusatory instrument filed is:
>
> (a) A felony; or
>
> (b) A misdemeanor defined in the penal law; or
>
> (c) A misdemeanor defined outside the penal law which would constitute a felony if such person had a previous judgment of conviction for a crime; or

74 Schmerber, 384 U.S. 757, 763.

75 *See* N.Y. CODE CRIM. PROC.§ 160.10 (McKinney 2010).

> (d) Loitering for the purpose of engaging in a prostitution offense as defined in subdivision two of section 240.37 of the penal law.[76]

Further, the police officer may have cause to procure a suspect's fingerprints if he is unable to ascertain the suspect's identity, believes the identity provided by the suspect is falsified, or has reason to believe the suspect is being sought by law enforcement for another offense.[77] This statute and similar laws in other states make it relatively easy for a police officer to justify the compelling a suspect to provide a fingerprint.

A. *The Fingerprint: More Than a Method of Identification*

The barriers to obtaining a suspect's fingerprints are relatively low because compelling a suspect to provide law enforcement officials with his fingerprint is not considered to be an intrusion on something that is personal to the individual; rather, it is considered to be a freely available method of identification, akin to a photograph.[78] But as technology develops, a fingerprint (as well as other biometric identifiers) no longer serves this singular purpose. It is also used to guard information possibly even more personal than an individual's identity. A fingerprint must also be understood as something private and subject to protection, like a password, rather than a photograph that is easily obtainable by the public, so that the courts will begin to view circumstances through a different lens.

It is fathomable to imagine that physical testimony such as a fingerprint could take on the communicative qualities of testimonial evidence. As discussed in Part II, seemingly volitional acts, such as signing a document or producing documentation, can sometimes take on testimonial qualities that make the determination of their entitlement to Fifth Amendment protection more challenging for the judicial system. Although a fingerprint itself is evidence obtained from a suspect's body, when it functions as the lock on a cellular device, it arguably possesses qualities of testimonial evidence because the use of the fingerprint is a direct link to communicative, as well as potentially incriminating information, and the fingerprint itself serves as a replacement for the traditional numeric or alphabetic password, which has received Fifth Amendment protection from the courts.[79] The fingerprint is no longer merely an identifying physical characteristic outside of the scope of

76 *Id.*

77 *Id.* § 160.10(2).

78 *Supra* note 32.

79 United States v. Kirschner, 823 F. Supp. 2d 665 (E.D. Mich. 2010).

Fifth Amendment protection.

B. *The Fifth Amendment and Password Protection*

The cases in which a court has been asked to apply the privilege against self-incrimination to the compelled disclosure of a password are limited. However, it has been established that a password can be testimonial evidence entitled to Fifth Amendment protection. In *United States v. Kirschner*, the defendant refused to provide a Federal grand jury with all of the passwords associated with his computer, pursuant to a subpoena issued by an Assistant U.S. Attorney.[80] The subpoena was dispensed in order to secure evidence that Kirschner was in possession of child pornography.[81] The defendant argued that being forced to produce the passwords violated his constitutional rights, because the passwords would provide the government with access to incriminating evidence stored on his computer.[82] The district court agreed with the defendant, holding that compelling Kirschner to produce passwords required him to make a "testimonial" communication and was thus a violation of the privilege.[83] The argument was that the act of production was testimonial because Kirschner was being forced to divulge through his mental processes knowledge that would be used to indict him.[84] The *Kirschner* court based its decision on Supreme Court precedent, citing *Doe v. United States* as controlling.[85]

This holding complies with the court's most traditional view of communicative evidence. The privilege protects an individual from incrimination through his own testimony.[86] Kirschner's knowledge of the password securing his computer would surely attest to his control and awareness of the contents of the machine. A password is something that only he would know, and forcing him to communicate this information was tantamount to forcing him to testify against himself.

Looking back to the influential *Doe* case, the Supreme Court utilized the analogy of using a key versus a combination to unlock a safe, in order to differentiate between physical and testimonial evidence.[87] Justice Stevens noted in his dissent that, "[the suspect] may in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to

80 *Id.*
81 *Id.*
82 *Id.* at 668.
83 *Id.* at 668-69.
84 *Id.*
85 *Id.* at 668–69.
86 *Supra* note 31.
87 Doe v. United States, 487 U.S. 201 (1988).

reveal the combination to his wall safe – by word or deed."[88] Turning a key merely requires a thoughtless, volitional movement – anyone who acquires it can obtain the same information without the possession of any special knowledge. A password, on the other hand, is the unique creation of its owner and cannot be shared with others unless he reveals to them the contents of his mind. Thus, a password falls squarely within the constitutional protection granted by the Fifth Amendment privilege against self-incrimination. In *Kirschner*, the example can be applied in its most literal form. If Kirschner had revealed his password to the government, that password would then be used to aid the government with his indictment.

The Supreme Court has implicitly established that a suspect may invoke the Fifth Amendment in order to prevent the government from compelling him to produce a combination or password, and the lower courts have ruled in accordance with this view. While the compulsion of a fingerprint has, before now, been undeserving of similar protection, determining how a court might weigh in on a fingerprint used as a password should result in an outcome favoring protection. Reaching such a conclusion requires an examination of the underlying goals and purposes of the analytical framework as it is currently used. To make an educated determination on how a court might rule if presented with such a situation, this Note will follow the same guidelines utilized by the Supreme Court in its case-by-case analysis of precedential case law.

IV. POSSIBLE OUTCOMES

The implementation of biometric passwords such as a retinal scan or fingerprint scanner allows physical evidence to achieve the same results as a traditional password comprised of letters and numbers. Does the application of biometric identification on a digital device prevent an individual form invoking his Fifth Amendment right against self-incrimination? This Note proposes that if a traditional alphabetic or numeric password, stored in the mind of its owner, is entitled to constitutional protection, then its modern technological counterpart should receive similar constitutional safeguards. The compulsion of a suspect by law enforcement to unlock an iPhone or similar device through the use of his fingerprint falls well within the scope of rights afforded by the Fifth Amendment privilege against self-incrimination, and furthers the policy goals espoused by the Fifth Amendment.

Traditionally, the government offered no constitutional protection to the compelled production of a fingerprint because it was used to identify individuals who were suspected of violating the law.[89]

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

89 *Supra* note 75.

Although this is still the case today, a fingerprint also serves additional purposes. The use of a fingerprint to safeguard confidential and personal information entirely changes the legal dynamic and expands the quantity and quality of information that the compulsion of a fingerprint can produce. As a result, in certain contexts its treatment by the law must also change. Mainly, the purpose of a fingerprint has expanded in two important ways: (1) the use of a fingerprint can be used as a direct link to communicative, as well as potentially incriminating, information, and (2) the fingerprint itself serves as a replacement for the traditional numeric or alphabetic password, which has received Fifth Amendment protection from the courts.

For these reasons, a fingerprint should be treated like any other physical act capable of acquiring testimonial qualities. The treatment of a fingerprint solely as an identifying physical characteristic is outdated. The standards under which law enforcement officials can obtain a fingerprint should be different depending on the context in which the fingerprint is being used. As a method of identification, a fingerprint should retain its classification as freely obtainable bodily evidence.[90] An iPhone owner preloads his fingerprint onto the memory of his device to ensure his privacy and only he, as the owner, can access the device.[91] Obviously, if his fingerprint can unlock the phone, then it is stored on the memory of the iPhone and has been previously used to access its contents. A court would easily come to the conclusion that he is the owner of the phone as well as its contents.

In this regard, it would seem that producing evidence by unlocking a phone would unavoidably possess testimonial quality. It is well established that testimony is inherent in the act of production.[92] Providing a government official with access to digital files is the modern equivalent of producing physical documents. Today, everything from bank records and telephone bills to personal correspondence is created and stored in digital form. Sometimes these digital files supplement physical hardcopies, but often they replace them altogether. Thus, the same argument that was applicable in *Hubbell* and other precedential cases is applicable here: if compelled production is admitting knowledge of the location, contents, or ownership of the files, then the act of production is testimonial in nature.[93]

It is true that pressing a finger to the sensor on an electronic device is a volitional movement regardless of what purpose the act is serving. However, in modern cases there has clearly been a shift away from the

90 N.Y. Crim. Proc. Law § 160.10.

91 *See* Press Release, Apple Inc., *supra* note 13.

92 *See* Hubbell, 530 U.S. 27.

93 *Id.*

strict categories of communicative versus physical evidence and towards a more flexible approach. A suspect compelled to unlock a device with his fingerprint could very well receive constitutional protection, because the act could "provide a prosecutor with a lead to incriminating evidence or a link in the chain of evidence needed to prosecute."[94] The act has then become testimonial because it is implicitly communicating information to the government.

It is important to keep in mind that the privilege protects against compulsory incrimination through one's own testimonial communication, but does not protect private information *per se*. In this way, "the Fifth Amendment privilege against self-incrimination does not necessarily bar compelling the disclosure of evidence that a criminal defendant created voluntarily in the past, even if the evidence betrays incriminating assertions of fact or belief."[95]

The Supreme Court has made it clear that the contents of the compelled documents themselves are not entitled to constitutional protection.[96] If the government were in pursuit of contacts, emails, or other incriminating data, there is no question that such information could be used to incriminate a suspect, if obtained lawfully.[97] But the issue here is the testimonial quality of the production of documents, not the creation of the documents themselves.[98] Like in *Fisher*, where the documents were voluntarily created,[99] it is assumed that data on a phone was voluntarily placed on the device for later use. Presumably, the cell phone owner consciously creates and stores information by choice, whether for convenience, reference, or for some other purpose. Instead of focusing on the creator's action, the focus of this discussion is on how the government would obtain the aforementioned data. The crux of the argument is whether the act of producing the evidence would have communicative aspects of its own; for example, as an admission of ownership or knowledge of the location or contents of the cellular phone data.

A suspect accessing an iPhone with a fingerprint accedes ownership of the phone and its contents, and could provide the government with information that it would not have been able to obtain without cooperation; this essentially forces the defendant to act as a

94 *Id.* at 42 (internal quotations omitted).

95 Coltoff et al., *supra* note 18.

96 *See* Fisher v. United States, 425 U.S. 391 (1976).

97 Such a request is not unheard of. For example, the government will subpoena social media websites for basic subscriber information or the content of communications provided, even if it is relevant to its investigation. *See* Twitter, Inc., *Guidelines for Law Enforcement*, TWITTER.COM, http://support.twitter.com/groups/33-report-a-violation/topics/148-policy-information/articles/41949-guidelines-for-law-enforcement#6 (last visited Sept. 2, 2014).

98 *See* Fisher, 425 U.S. 391.

99 *Id.*

witness against himself, even if he is not communicating in the traditional sense. In the not-so-distant past, before biometric technology was in use, a fingerprint indicated nothing more than the identity of a suspect; the communication of information was not even a consideration. A change in the function of a fingerprint similarly requires an adaptation in legal doctrine to accommodate for potential self-incrimination through the use of a fingerprint, a possibility that was, until recently, unheard of.

A. *Applicable Recent Case Law*

A recent case in the federal circuit that is helpful to this analysis is *In re:* Grand Jury Subpoena Duces Tecum Dated March 25, 2011.[100] This case involved a similar situation in which the use of modern technology complicated the traditional notion of what constitutes a communication. The plaintiff, referred to as John Doe, was served with a subpoena calling him to appear before a grand jury and produce the unencrypted files stored on his laptop, as well as five external hard drives.[101] Doe was under investigation for the possession of child pornography.[102] He was suspected of sharing explicit material with underage girls via a YouTube account. By obtaining IP addresses that he used to access the Internet, law enforcement officials were able to trace the activity back to Doe.[103] They lawfully seized seven digital media devices, including two laptops and five external hard drives. However, forensic examiners were unable to access some portions of the drives.[104]

Doe was subsequently issued a subpoena compelling him to produce the unencrypted contents of the digital media.[105] Because Doe intended to invoke his Fifth Amendment rights and the government considered the acquisition of the files necessary to its investigations, the Attorney General authorized the U.S. Attorney for the Northern District of Florida to apply to the court for an order granting Doe immunity and requiring him to testify.[106] Immunity would allow Doe to testify without

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

101 *Id.* at 1339.

102 *Id.* at 1338.

103 *Id.* at 1339.

104 *Id.*

105 *Id.*

106 The authority to grant an individual immunity comes from 18 U.S.C.A. § 6003 (2010):

> In the case of any individual who has been or may be called to testify or provide other information at any proceeding before or ancillary to a court of the United States or a grand jury of the United States, the United States district court for the judicial district in which the proceeding is or may be held shall issue, in accordance with subsection (b) of this section, upon the request of the United States attorney for such district, an

fear that the information obtained from his testimony would be used against him.[107] However, Doe's immunity extended only to his production of the unencrypted files, and the government's derivative use of the files could be used against him.[108]

The district court held that because the contents of the files themselves were created voluntarily and therefore not testimonial, then the government's use of them was not a violation of the privilege against self-incrimination.[109] This was the view adopted by the Court in *Hubbell* in order to permit the compelled production of evidence. The Court of Appeals reversed the decision of the lower court, determining that it had not implemented the correct analysis. Rather, the question was whether the production of the files "explicitly or implicitly convey[ed] some statement of fact."[110]

To receive Fifth Amendment protection, an individual must meet three criteria: (1) compulsion, (2) a testimonial act, and (3) incrimination.[111] Here, the first and third prongs of the test were met. Doe was being compelled to decrypt and produce the files of his personal hard drives, and the information obtained from this compulsion

order requiring such individual to give testimony or provide other information which he refuses to give or provide on the basis of his privilege against self-incrimination, such order to become effective as provided in section 6002 of this title.

A United States attorney may, with the approval of the Attorney General, the Deputy Attorney General, the Associate Attorney General, or any designated Assistant Attorney General or Deputy Assistant Attorney General, request an order under subsection (a) of this section when in his judgment--

(1) the testimony or other information from such individual may be necessary to the public interest; and

(2) such individual has refused or is likely to refuse to testify or provide other information on the basis of his privilege against self-incrimination.

107 *See* 18 U.S.C.A. § 6002 (2010):

Whenever a witness refuses, on the basis of his privilege against self-incrimination, to testify or provide other information in a proceeding before or ancillary to--

(1) a court or grand jury of the United States,

(2) an agency of the United States, or

(3) either House of Congress, a joint committee of the two Houses, or a committee or a subcommittee of either House,

and the person presiding over the proceeding communicates to the witness an order issued under this title, the witness may not refuse to comply with the order on the basis of his privilege against self-incrimination; but no testimony or other information compelled under the order (or any information directly or indirectly derived from such testimony or other information) may be used against the witness in any criminal case, except a prosecution for perjury, giving a false statement, or otherwise failing to comply with the order.

108 In re Gand Jury Subpoena, 670 F.3d at 1338.

109 *Id.* at 1342 (citing United States v. Hubbell, 530 U.S. 27 (2000)) (holding that the compelled production of incriminating evidence is not protected by the Fifth Amendment because the creation of the files themselves was voluntary, and not compelled within the meaning of the privilege).

110 *Id.*

111 *Id.* at 1341 (citing United States v. Ghidoni, 732 F.2d 814, 816 (11th Cir. 1984)).

would be used to incriminate him for the possession of child pornography. Thus, the crux of the issue became whether the act of production was a testimonial act.[112]

Accordingly, the court in *In re:* Grand Jury Subpoena Duces Tecum structured its analysis around the question of whether Doe's compelled production was testimonial and subject to Fifth Amendment protection. Doe argued that by decrypting the contents of the hard drives "he would be testifying that he, as opposed to some other person, placed the contents on the hard drive, encrypted the contents, and could retrieve and examine them whenever he wished."[113] Although he was not explicitly communicating the contents of his mind to the government, his act nevertheless had a testimonial quality. Similarly, the use of a fingerprint to unlock a phone would create a factually analogous situation by demonstrating a defendant's ability to access the restricted content of the cell phone whenever he chose.

The Court of Appeals used two seminal cases, discussed in Part II of this Note, to guide its analysis: *Fisher* and *Hubbell*. In *Fisher*, the court held that the act of producing documents could maintain a testimonial quality, making it possible for a physical act to receive constitutional protection. But in that case the government had in no way been relying on the truth telling of the taxpayer, making the information a foregone conclusion and thus ineligible for the privilege.[114] *Hubbell* was distinguished from *Fisher* because the court could not indict the defendant without the subpoenaed documents, and the facts resulting from the production were not a foregone conclusion.[115] Therefore *Hubbell* was more pertinent to the situation at hand, because the government did not know with relative certainty what the hard drives contained.[116]

In *In re:* Grand Jury Subpoena Duces Tecum, the Court of Appeals ultimately held that compelling the suspect to use an encryption password was analogous to using the contents of his mind, subsequently making the production of the unencrypted contents of the hard drives testimonial.[117] The court determined that "the decryption and production would be tantamount to testimony by Doe of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives;

112 *Id.* at 1342.

113 *Id.* at 1339–40.

114 *Id.* at 1344.

115 *Id.* at 1344–45 (citing U.S. v. Hubbell, 530 U.S. 27, 44-45 (2000))("Whatever the scope of this "foregone conclusion" rationale, the facts of this case plainly fall outside of it.").

116 *Id.*

117 *Id.* at 1346.

and of his capability to decrypt the files."[118]

The same conclusion should be reached if a court were asked to decide on the compulsion of a biometric password. The Court of Appeals in *John Doe* reached its holding by determining that: (1) Doe's decryption and production of the files would be testimonial and not just a mere physical act, and (2) that the explicit and implicit information obtained in association with the production was not a foregone conclusion.[119] Accordingly, using a fingerprint to unlock a phone would be more testimonial than a physical act because it accedes ownership and knowledge of the cellular device's contents. To corroborate the second part of the holding in *John Doe*, the specific circumstances related to the use of a cell phone must be more closely examined, as previously discussed in Part III of this Note.

B. *The Fingerprint as a Password Replacement*

From this point forward, the legality of the government compulsion of a suspect's fingerprint must be considered within the context of its use. This Note proposes that a court, when eventually faced with the question of whether or not law enforcement officials can compel a suspect to unlock a phone or similar device with his fingerprint, must look at what action the fingerprint serves to replace. This type of "substitution test" would allow for different treatment of fingerprints used for identification purposes and fingerprints used for security purposes. Such a test could be extended to other forms of biometric passwords as well, including uses of the ear, voice, DNA, or eye.[120] Many personal characteristics that were once purely physical have recently acquired an additional purpose, and may eventually need to be addressed by the judicial system.

Arguably, the volitional movement required to place a finger on a scanner does not require the suspect to divulge the "contents of the mind." This is exactly why fingerprints have never received constitutional protection in the past.[121] Instead, a fingerprint, because of the creation of new technologies, must be viewed in terms of the act it replaces. If an individual cannot be compelled to use a password to

118 *Id.*

119 *Id.*

120 *See* Types of Biometrics, BIOMETRICS INSTITUTE, http://www.biometricsinstitute.org/pages/types-of-biometrics.html (last visited Sept. 1, 2014), for a list of biometric technology currently in use. Although most items on this list are not currently in mainstream use, it seems plausible that the use of biometrics as a security measure will only continue to become more widespread.

121 Schmerber v. California, 384 U.S. 757 (1966) ("[B]oth federal and state courts have usually held that it offers no protection against compulsion to submit to fingerprinting, photographing, or measurements, to write or speak for identification, to appear in court, to stand, to assume a stance, to walk, or to make a particular gesture.")

unlock guarded information, this privilege should naturally extend to a physical act that is designed to achieve the same purpose. To deny the protection afforded by the privilege against self-incrimination in this context would be merely to punish a defendant for taking advantage of developments in modern technology. The Constitution, after all, is a living document that must adapt to circumstances that could not have been predicted over two hundred years ago.[122]

Even though the Constitution was drafted long before biometric passwords were even contemplated, the policy underlying the Fifth Amendment and the privilege against self-incrimination favors the treatment of a fingerprint as testimonial evidence. The Fifth Amendment aims to protect the rights of the innocent and the privacy of the individual.[123] There is nothing more deserving of protection from government intrusion than an individual's most private and personal information, which is often the information that is guarded with a password.

CONCLUSION

Over the years the Supreme Court has developed useful tools with which to guide its interpretation of the Fifth Amendment privilege against self-incrimination.[124] The guidelines the Court has developed to determine whether evidence produced by compulsion should be suppressed under the Fifth Amendment privilege ultimately have proven more useful to the analysis of the issue at hand than any bright line rule, statute or regulation. Applying the law to issues of first impression involving modern technology requires flexibility and reinterpretation of precedential case law. Seminal Fifth Amendment case law, including *Doe* and *Hubbell,* are illustrative of the Court's struggle to account for the testimonial qualities of compelled physical actions. However, under the proper circumstances, it is evident that a physical compulsion, such as a signature or even a fingerprint, could

122 *See* Missouri v. Holland, 252 U.S. 416, 433 (1920) ("[W]hen we are dealing with words that also are a constituent act, like the Constitution of the United States, we must realize that they have called into life a being the development of which could not have been foreseen completely by the most gifted of its begetters.").

123 *See* RICH, *supra* note 2.

124 *See* In re: Grand Jury Subpoena Duces Tecum, 670 F.3d at 1345–46:

> [T]he Court has marked out two ways in which an act of production is *not testimonial.* First, the Fifth Amendment privilege is not triggered where the Government merely compels some physical act, i.e. where the individual is not called upon to make use of the contents of his or her mind…Second, under the "foregone conclusion" doctrine, an act of production is not testimonial—even if the act conveys a fact regarding the existence or location, possession, or authenticity of the subpoenaed materials—if the Government can show with "reasonable particularity" that, at the time it sought to compel the act of production, it already knew of the materials, thereby making any testimonial aspect a "foregone conclusion."

maintain the requisite level of testimonial quality deserving of Fifth Amendment protection.

It is likely that the Supreme Court will one day be required to interpret how the Fifth Amendment should treat the compelled production of electronic data through the use of a suspect's fingerprint. Biometric passwords, specifically the fingerprint scanner now featured on the iPhone, are gaining mainstream popularity as the demand for new technology continues to grow.[125] Barring the application of the immunity exception and foregone conclusion doctrine, a compelled fingerprint, when used as a password, should receive the same treatment as any other physical act with a testimonial quality.

The Supreme Court has admitted that each situation must be examined on a case-by-case basis. The compulsion of a fingerprint requires such a case-by-case analysis, because it is now capable of serving a function as both a method of identification and as a security measure. The facts surrounding biometric passwords are unique, and as of yet, have not been examined by a federal court. However, the analysis and doctrine developed by the judicial system in order to interpret the privilege against self-incrimination can seamlessly be applied to the compulsion of a potentially incriminating fingerprint.

*Kara Goldman**

125 *See* Apple Inc., Press Release, supra note 11.

*Articles Editor, CARDOZO ARTS & ENT. L.J. Vol. 33; J.D. Candidate, Benjamin N. Cardozo School of Law (2015); B.A., Political Science, University of Florida (2012). Thank you to my faculty advisor, Professor Felix Wu, and the AELJ Editorial Board for their help and guidance.