University of Miami Law Review

Volume 69
Number 1 *Volume 69 Number 1 (Fall 2014)*

Article 8

10-1-2014

The "Biometric Revolution": An Erosion of the Fifth Amendment Privilege to Be Free from Self-Incrimination

Erin M. Sales

NOTES

The "Biometric Revolution": An Erosion of the Fifth Amendment Privilege to Be Free from Self-Incrimination

ERIN M. SALES*

I. INTRODUCTION

With iPhone 5s, getting into your phone is faster and easier with Touch ID—a new fingerprint identity sensor. Touch ID is a seamless way to use your fingerprint as a passcode. With just the touch of the Home button . . . the Touch ID sensor quickly reads your fingerprint

* Senior Writing Editor, *University of Miami Law Review*; J.D. Candidate 2015, University of Miami School of Law; M.A. 2008, University of Connecticut; B.S. 2006, University of Connecticut. I would like to thank my family for its unwavering support and encouragement. I would also like to thank Professor Scott Sundby and the *University of Miami Law Review* for their critical feedback regarding this article.

and *automatically* unlocks your phone.[1]

When Apple announced that its then-latest version of the iPhone would utilize a fingerprint scan instead of a traditional passcode to unlock the phone, the media, consumers, and competitors went crazy.[2] Of course, a fingerprint reader on your iPhone certainly seems exciting, simpler, and safer. But does eliminating the need to enter a memorized passcode to access the phone have any legal implications?

Consider the following hypothetical: A person is arrested. Officers locate the suspect's smartphone on him or her and want to search the phone for text messages and photos relating to the illegal activity for which the suspect was arrested. However, the suspect owns a smartphone that utilizes a fingerprint reader to unlock the phone, and unless the suspect puts his or her finger on the phone's fingerprint reader, the phone remains locked. The suspect either consents to the search while being interrogated and places his or her finger on the phone to unlock it, or the officers obtain a subpoena ordering the suspect to unlock the phone. On the phone, officers find incriminating text messages and photos that are used against the suspect at trial. Would this constitute "compelled authentication," violating the suspect's Fifth Amendment privilege to be free from self-incrimination?

The Fifth Amendment privilege is often overlooked and somewhat misunderstood. "No person . . . shall be compelled in any criminal case to be a witness against himself."[3] The privilege is a basic constitutional right that a person will likely never have to invoke or consider, until it is too late.[4] There are even differing opinions amongst legal professionals regarding when the privilege applies. For example, some argue that the privilege applies strictly to self-incrimination at trial, and not to investigations or interrogations.[5] While the foregone conclusion doctrine seems

1. *iPhone 5s: Using Touch ID*, APPLE, http://support.apple.com/kb/HT5883 (last modified May 6, 2014) [hereinafter *Using Touch ID*] (emphasis added).

2. *See, e.g.*, Jeff Garnet, *WSJ: New iPhone Really Will Have a Fingerprint Scanner*, MAC OBSERVER (Sept. 10, 2013, 10:52 AM), http://www.macobserver.com/tmo/article/wsj-new-iphone-really-will-have-a-fingerprint-scanner ("Rumors have been circulating that one of the new features will be a fingerprint sensor built into the Home button, and now the Wall Street Journal is chiming in with its own version of 'yep.'").

3. U.S. CONST. amend. V.

4. For example, an officer says to a suspect, "why don't you tell me what happened and we can hopefully clear up this whole thing." Caught up in the pressure from the situation, locked away in an investigation room, and not knowing what to do, the suspect starts talking and provides incriminating evidence. Later on, the suspect realizes that he did not need to say anything and could have simply invoked his Fifth Amendment right. *See id.* ("No person . . . shall be compelled in any criminal case to be a witness against himself . . . ."); *see also* Salinas v. Texas, 133 S. Ct. 2174, 2178 (2013) (explaining that the privilege against self-incrimination is not self-executing, so a witness must expressly invoke the privilege to claim its protection).

5. *See* Chavez v. Martinez, 538 U.S. 760, 766 (2003) (disagreeing with the respondent that

to clarify that when evidence is a "foregone conclusion" the privilege does not apply, ambiguity remains regarding how to determine whether evidence is in fact a "foregone conclusion."[6] Moreover, a circuit split currently exists regarding whether compelled production of a password or encrypted data violates the Fifth Amendment privilege.[7] What is clear, however, is that the privilege only applies to compelled information that is of a testimonial or communicative nature.[8] Thus, compelled production or displays of purely physical characteristics do not violate the Fifth Amendment's privilege. But what exactly is a display of purely physical characteristics?

Biometric authentication is the future of identification and security. Biometrics Research Group, Inc., has estimated that "over 90 million smartphones with biometric technology will be shipped in 2014."[9] Recent market research shows a compound annual growth rate of 19.8% for biometric technologies.[10] Biometric authentication is popping up everywhere; airports,[11] amusement parks,[12] and even school districts are jumping on board.[13] Not surprisingly, there is a multitude of scholarly publications available regarding biometric authentication and Fourth

police interrogation without actual charges being filed constituted a "criminal case"); *cf.* Thomas Y. Davies, *Farther and Farther from the Original Fifth Amendment: The Recharacterization of the Right Against Self-Incrimination as a "Trial Right" in* Chavez v. Martinez, 70 TENN. L. REV. 987 (2003) (discussing whether the Fifth Amendment is only a trial right).

6. *See* discussion *infra* Part II.B.

7. *See* discussion *infra* Part III.B.

8. *See* Doe v. United States, 487 U.S. 201, 219 (1988) (signing a consent form to release records was not compelled testimony); United States v. Wade, 388 U.S. 218, 222–23 (1967) (compelled speech merely to produce a voice sample did not violate the privilege); Gilbert v. California, 388 U.S. 263, 266–67 (1967) (a handwriting exemplar did not violate the privilege); Schmerber v. California, 384 U.S. 757, 761 (1966) (taking a blood sample for a blood analysis was not compulsion); Holt v. United States, 218 U.S. 245, 252–53 (1910) (compelled blouse modeling did not violate the privilege).

9. Rawlson King, *Mobile Commerce Will Drive Millions of Biometric Smartphone Shipments, Billions in Transactions*, BIOMETRICUPDATE.COM (Sept. 13, 2013), http://www.biometricupdate.com/201309/mobile-commerce-will-drive-millions-of-biometric-smartphone-shipments-billions-in-transactions.

10. *Biometrics: Technologies and Global Markets*, BCC RESEARCH (Jan. 2014), http://www.bccresearch.com/market-research/information-technology/biometrics-technologies-ift042d.html.

11. *About Global Entry*, U.S. CUSTOMS & BORDER PROTECTION, http://www.globalentry.gov/about.html (last visited Aug. 9, 2014) ("At airports, program participants . . . present their . . . passport or U.S. permanent resident card, place their fingertips on the scanner for fingerprint verification, and make a customs declaration.").

12. *See Finger Scanning at Theme Parks*, FOX 35 NEWS ORLANDO (May 9, 2012), http://www.myfoxorlando.com/story/18248551/finger-scanning-at-theme-parks (discussing the use of finger scanners to access parks at Walt Disney World, Universal Studios, and SeaWorld).

13. *See* Kathleen McGrory, *Lawmakers to Consider Banning Biometrics in Schools*, MIAMI HERALD (Feb. 2, 2014), http://www.miamiherald.com/2014/02/02/3909538/lawmakers-to-consider-banning.html (discussing how some Florida schools use fingerprint scanners or palm scanners in their cafeterias, which resulted in proposed laws banning the collection of biometric information by school districts); *see also* H.R. 195, 2014 Leg., Reg. Sess. (Fla. 2014) (House bill

Amendment privacy rights, such as tracking known or suspected criminals using facial recognition technology or deoxyribonucleic acid ("DNA") databanks.[14] Moreover, the Supreme Court of the United Sates recently considered DNA analysis and concluded that DNA identification is like fingerprinting and photographing for identification and does not violate the Fourth Amendment.[15]

Nonetheless, scholars have warned about the implications of biometrics on the Fourth Amendment: "While emerging biometric identification technology, such as iris scanning and fac[ial] recognition technology, may be a fast, cutting-edge way for law enforcement to keep track of convicted felons and suspected terrorists, the government should not be allowed to unreasonably intrude on individual privacy rights under the Fourth Amendment."[16] Likewise, the government should not be able to circumvent an individual's Fifth Amendment privilege to be free from self-incrimination through the use of biometric authentication. However, there has been considerably less conversation regarding biometric authentication's impact on the Fifth Amendment than there has been regarding its impact on the Fourth Amendment.[17]

This article analyzes whether biometric authentication implicates the Fifth Amendment privilege to be free from self-incrimination. First,

---

to regulate the use of biometrics in schools); S. 232, 2014 Leg., Reg. Sess. (Fla. 2014) (Senate bill to prohibit a school district from collecting students' biometric information).

14. *See, e.g.*, Rudy Ng, *Catching Up to Our Biometric Future: Fourth Amendment Privacy Rights and Biometric Identification Technology*, 28 HASTINGS COMM. & ENT. L.J. 425 (2006) (discussing biometric authentication and the Fourth Amendment).

15. Maryland v. King, 133 S. Ct. 1958, 1980 (2013).

16. Ng, *supra* note 14, at 442; *cf. King*, 133 S. Ct. at 1979 ("[S]cience can always progress further, and those progressions may have Fourth Amendment consequences . . . ."). In *King*, the Supreme Court acknowledged, "a significant government interest does not alone suffice to justify a search. The government interest must outweigh the degree to which the search invades an individual's legitimate exceptions of privacy." *Id.* at 1977–78. However, the "expectations of privacy of an individual taken into police custody 'necessarily [are] of a diminished scope.' " *Id.* at 1978 (alteration in original) (quoting Bell v. Wolfish, 441 U.S. 520, 557 (1979)).

17. Most discussion regarding the Fifth Amendment and compelled production involves traditional passcode authentication where the user needs to input a passcode committed to memory. *See, e.g.*, Erica Fruiterman, *Upgrading the Fifth Amendment: New Standards for Protecting Encryption Passwords*, 85 TEMP. L. REV. 655 (2013); John E. D. Larkin, *Compelled Production of Encrypted Data*, 14 VAND. J. ENT. & TECH. L. 253 (2012). Biometric authentication's impact on the Fifth Amendment is just now becoming a topic of conversation. *See* Marcia Hoffman, *Apple's Fingerprint ID May Mean You Can't 'Take the Fifth'*, WIRED (Sept. 12, 2013, 9:29 AM), http://www.wired.com/2013/09/the-unexpected-result-of-fingerprint-authentication-that-you-cant-take-the-fifth/ (discussing how the privilege to be free from self-incrimination "may not apply when it comes to biometric-based fingerprints (things that reflect who we are) as opposed to memory-based passwords and PINs (things we need to know and remember)"); Chet Kaufman, *Encrypting Data May Give Rise to a Limited Constitutional Defense*, 37 CHAMPION 36, 41 (2013) (biometrics involve physical acts that fall outside the Fifth Amendment's protection, so defendants cannot argue that a biometric act compels them to produce the contents of their minds). Nonetheless, this topic has been relatively unexplored.

Part II reviews the history of the Fifth Amendment privilege, including the foregone conclusion doctrine, and discusses the interplay between the search incident to arrest doctrine and the Fifth Amendment. Second, Part III provides an overview of encryption and the current circuit split regarding whether the Fifth Amendment prohibits compelled production of passwords and encrypted data. Third, Part IV presents an overview of biometric authentication and discusses how the "Biometric Revolution"[18] impacts our everyday lives. Finally, Part V analyzes biometric authentication's impact on the Fifth Amendment, suggesting that biometric authentication will not implicate the privilege to be free from self-incrimination, and discusses the consequences that this may have on an individual's constitutional rights.

II. THE FIFTH AMENDMENT

A. *The Privilege to Be Free from Self-Incrimination*

The Fifth Amendment to the United States Constitution provides the privilege to be free from self-incrimination, stating that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself."[19] The fundamental purpose of the Fifth Amendment is to preserve "an adversary system of criminal justice."[20] "That system is undermined when a government deliberately seeks to avoid the burdens of independent investigation by compelling self-incriminating disclosures."[21] Over time, however, the original meaning and purpose of this right has become somewhat unclear, often even referred to as "murky" or "confused."[22]

James Madison's proposed Bill of Rights contained a miscellaneous article—including his version of the self-incrimination clause—that appeared within the procedural rights the accused was to be afforded at trial.[23] However, Madison failed to explain how broadly he intended the self-incrimination clause to apply.[24] Nonetheless, the proposal appeared to apply to both civil and criminal cases and to any stage of legal investigation or inquiry.[25] Upon review, the House of Repre-

18. For purposes of this article, the growing prevalence of biometric authentication in consumer personal electronic devices, such as smartphones, tablets, and laptops, will be referred to as the "Biometric Revolution."

19. U.S. CONST. amend. V.

20. Garner v. United States, 424 U.S. 648, 655 (1976).

21. *Id.* at 655–56.

22. *See* Davies, *supra* note 5, at 998.

23. LEONARD W. LEVY, ORIGINS OF THE FIFTH AMENDMENT: THE RIGHT AGAINST SELF-INCRIMINATION 422–23 (Oxford Univ. Press 1968).

24. *See id.* at 423.

25. *See id.* In framing-era practice, defendants were viewed as interested witnesses and could not even testify as witnesses in their own trials under the rules of evidence in place at the time. *See*

sentatives amended the article, confining it to criminal cases, and unanimously adopted the amended article.[26] The Senate later accepted the self-incrimination clause, rephrased the double jeopardy clause, and added a clause on the grand jury, creating today's version of the Fifth Amendment.[27] The Senate then grouped together the accused's procedural rights afforded after indictment, creating the Sixth Amendment.[28]

> The location of the self-incrimination clause in the Fifth Amendment rather than the Sixth provides that the Senate, like the House, did not intend to restrict that clause to the criminal defendant only nor only to his trial. The Fifth Amendment, even with the self-incrimination clause restricted to criminal cases, still put its principle broadly enough to apply to witnesses and to *any phase of the proceedings*.[29]

An early consideration of this self-incrimination clause occurred in *Bram v. United States*, where the government offered a conversation between a detective and shipmate regarding a murder aboard the vessel into evidence as a confession.[30] Notably, the Supreme Court explained that a mere confession made to a police officer while the accused was under arrest is not enough to render the confession involuntary; instead, the facts and circumstances surrounding the confession must be considered to determine whether the confession was in fact "compelled" under the Fifth Amendment.[31] Over time, the premise became clear—the accused cannot be compelled to incriminate himself.[32] This privilege is fulfilled "only when the person is guaranteed the right 'to remain silent unless he chooses to speak in the unfettered exercise of his own will.'"[33] In the landmark custodial interrogation case, *Miranda v. Arizona*, the Supreme Court stated,

> [w]e are satisfied that all the principles embodied in the privilege apply to informal compulsion exerted by law enforcement officers

Davies, *supra* note 5, at 999 (citing JOHN H. LANGBEIN, THE ORIGINS OF ADVERSARY CRIMINAL TRIAL 38 (2003)).

26. *See* LEVY, *supra* note 23, at 424–25. However, the Fifth Amendment's self-incrimination privilege can still be asserted in non-criminal cases where the answers might incriminate the speaker in future criminal proceedings. Chavez v. Martinez, 538 U.S. 760, 770 (2003) (citations omitted). Nonetheless, "a violation of the constitutional right against self-incrimination occurs only if one has been compelled to be a witness against himself in a criminal case." *Id.*

27. *See* LEVY, *supra* note 23, at 426–27.

28. *See id.* at 427.

29. *Id.* (emphasis added); *see also* R. H. HELMHOLZ ET AL., THE PRIVILEGE AGAINST SELF-INCRIMINATION: ITS ORIGINS AND DEVELOPMENT 2 (Univ. of Chicago Press 1997) ("The privilege . . . may be invoked . . . also by those who might be tried at some time in the future. . . . [T]he privilege extends beyond the courtroom and the interrogation room of the police station.").

30. 168 U.S. 532, 534–40 (1897).

31. *Id.* at 558, 561 (citations omitted).

32. *See* Malloy v. Hogan, 378 U.S. 1, 7 (1964).

33. Miranda v. Arizona, 384 U.S. 436, 460 (1966) (quoting *Malloy*, 378 U.S. at 8).

> during in-custody questioning. An individual swept from familiar surroundings into police custody, surrounded by antagonistic forces, and subjected to the techniques of persuasion . . . cannot be otherwise than under compulsion to speak. As a practical matter, the compulsion to speak in the isolated setting of the police station may well be greater than in courts or other official investigations, where there are often impartial observers to guard against intimidation or trickery.[34]

Although the privilege was historically accorded a liberal construction,[35] once defendants attempted to expand the privilege's reach, the Supreme Court had to carve out a line of distinction. Specifically, the Supreme Court eventually clarified that "the privilege is a bar against compelling 'communications' or 'testimony,' but . . . compulsion which makes a suspect or accused the source of 'real or physical evidence' does not violate it."[36]

For example, in *Holt v. United States*, the Supreme Court rejected an argument that compelling an accused to put on and model a blouse violated the privilege.[37] Later, in *Schmerber v. California*, the Supreme Court held, "the privilege protects an accused only from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature," and determined that a blood sample taken from the petitioner was not "compulsion" in that sense.[38] The Supreme Court noted that "[t]he 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."[39] Thus, even though the petitioner was required to submit to a blood test that revealed an incriminating piece of evidence, the evidence was not "testimony [ ]or evidence relating to some communicative act or writing by the petitioner . . . ."[40]

However, Justice Black starkly dissented from the majority's viewpoint in *Schmerber*:

> In the first place it seems to me that the compulsory extraction of

34. *Id.* at 461 (explaining why the privilege against self-incrimination is fully applicable during a period of custodial interrogation).

35. *See id.* ("In this Court, the privilege has consistently been accorded a liberal construction.").

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

37. 218 U.S. 245, 252–53 (1910).

38. 384 U.S. at 761. A police officer directed a physician to withdraw a blood sample from the petitioner's body while the petitioner was at the hospital receiving treatment for injuries suffered in an automobile accident. *Id.* at 758. An analysis of the blood sample later revealed that the petitioner was intoxicated at the time of the accident. *Id.* at 759.

39. *Id.* at 763 (quoting *Holt*, 218 U.S. at 252–53).

40. *Id.* at 765.

> petitioner's blood for analysis so that the person who analyzed it could give evidence to convict him had both a "testimonial" and a "communicative nature." 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. And the purpose of the project was certainly "communicative" in that the analysis of the blood was to supply information to enable a witness to communicate to the court and jury that petitioner was more or less drunk. I think it unfortunate that the Court rests so heavily for its very restrictive reading of the Fifth Amendment's privilege against self-incrimination on the words "testimonial" and "communicative." These words are not models of clarity and precision as the Court's rather labored explication shows. Nor can the Court, so far as I know, find precedent in the former opinions of this Court for using these particular words to limit the scope of the Fifth Amendment's protection.[41]

Nonetheless, the majority agreed that the privilege generally "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."[42] However, the majority did admit that a test that obtains physical evidence could still be "testimonial" if the test reveals physiological responses, such as a lie detector test that measures changes in body function during interrogation.[43]

A year after *Schmerber*, the Supreme Court further restricted the meaning of "testimonial" in *United States v. Wade*.[44] In *Wade*, the Supreme Court considered a situation in which the government compelled the petitioner to stand in a lineup wearing strips of tape similar to those worn by a bank robber and to speak the words uttered by the bank robber.[45] Explaining that this was "compulsion of the accused to exhibit his physical characteristics, not compulsion to disclose any knowledge he might have," the Supreme Court rejected the petitioner's argument that his privilege against self-incrimination had been violated.[46] *Wade* further clarified that even compelled speech is not "testimonial" in nature if the speech is to be used solely as an identifying physical characteristic and not to admit guilt.[47] Likewise, the taking of a handwriting

41. *Id.* at 774 (Black, J., dissenting).

42. *Id.* at 764.

43. *Id.*

44. 388 U.S. 218 (1967).

45. *Id.* at 220.

46. *Id.* at 222. However, the Supreme Court emphasized that the case at hand did not present the question of admissibility in evidence of anything the petitioner did or said at the lineup. *Id.* at 223.

47. *Id.* at 222–23 ("[C]ompelling Wade to speak within hearing distance of the witnesses,

exemplar does not violate the privilege against self-incrimination when used solely as an identifying physical characteristic and not as evidence of the content of what is written.[48]

Similarly, a consent directive signed by an accused does not violate the privilege, provided the directive is nontestimonial in nature.[49] In *Doe v. United States*, the United States District Court for the Southern District of Texas denied a motion to compel the defendant to sign forms consenting to a disclosure of bank records, reasoning that "by signing the consent forms [the accused] would necessarily be admitting the existence of the accounts," and that if the banks then produced the records, it would equate to an admission that the accused exercised authority over the accounts and their potentially incriminating documents.[50] On certiorari, the Supreme Court acknowledged that the execution of the form would be compelled and that its execution might have an incriminating effect, but emphasized that the question was "whether the act of executing the form [wa]s a 'testimonial communication.'"[51] Ultimately, the Supreme Court determined that the consent directive did not have testimonial significance because executing the form was not an assertion of fact; the only fact that would be revealed if the banks produced the records would be that the bank believed the accounts belonged to the accused.[52] Notably, Justice Stevens dissented, arguing that if the accused could "be compelled to use his mind to assist the Government in developing its case . . . he w[ould] be forced 'to be a witness against himself,'" in violation of the Fifth Amendment privilege to be free from

even to utter words purportedly uttered by the robber, was not compulsion to utter statements of a 'testimonial' nature; he was required to use his voice as an identifying physical characteristic, not to speak his guilt.").

48. Gilbert v. California, 388 U.S. 263, 266–67 (1967). Some states' criminal procedure discovery rules explicitly outline similar permissible nontestimonial identification methods. *E.g.*, FLA. STAT. ANN. § 3.220(c)(1) (West 2013); MD. CODE ANN., CRIM. PROC. § 4-262(f) (West 2013). See also *Maryland v. King*, upholding the taking and analysis of DNA after a defendant's arrest, but before conviction, as a reasonable search under the Fourth Amendment because DNA analysis is an identification method and part of the routine booking procedure. 133 S. Ct. 1958, 1980 (2013).

49. Doe v. United States, 487 U.S. 201, 219 (1988). The "consent directive" in *Doe* was a form prepared by the Government that effectively rendered consent from the petitioner to have twelve foreign banks release records related to certain account numbers that the Government knew or suspected the petitioner had control over. *Id.* at 203.

50. *Id.* at 203–04. The district court noted that the petitioner's "signing of the forms might provide the Government with the incriminating link necessary to obtain an indictment, the kind of 'fishing expedition' that the Fifth Amendment was designed to prevent." *Id.* at 204. The United States Court of Appeals for the Fifth Circuit reversed, holding that the form did not have testimonial significance so the petitioner could not assert his Fifth Amendment privilege. *Id.* at 205.

51. *Id.* at 207.

52. *Id.* at 215–18.

self-incrimination.[53] Nevertheless, the majority had spoken, and the privilege's limits seemed clear: to violate the privilege, the compelled information had to be a factual assertion that was testimonial in nature.[54]

While the privilege's contours finally seemed clear, in 2003, the murkiness resurfaced with the Supreme Court's decision in *Chavez v. Martinez*.[55] Interestingly, the respondent in *Chavez* asserted—in a civil rights claim—that his Fifth Amendment privilege against self-incrimination had been violated during previous police questioning, even though he was never charged with a crime or had his statements used against him in a criminal case.[56] Accordingly, the Supreme Court held that the respondent's Fifth Amendment privilege had not been violated because he was never prosecuted for a crime, nor were his statements admitted against him in a criminal case.[57] The Supreme Court disagreed with the respondent's assertion that police interrogations alone constituted a "criminal case" and explained that "a 'criminal case' at the very least requires the initiation of legal proceedings."[58] While the *Chavez* decision seems relatively clear in that eliciting statements during police questioning does not violate the privilege if the statements are never used against the speaker in a criminal proceeding,[59] subsequent legal analysis by some scholars suggests that the *Chavez* opinion restricts the privilege strictly to self-incrimination at trial.[60]

B. *The Foregone Conclusion Doctrine's Limiting Effect*

The foregone conclusion doctrine[61] removes the Fifth Amend-

53. *Id.* at 220 (Stevens, J., dissenting).

54. *See id.* at 215 ("We agree with the Court of Appeals that it would not [have testimonial significance], because neither the form, nor its execution, communicates any factual assertions, implicit or explicit, or conveys any information to the Government.").

55. 538 U.S. 760 (2003).

56. *Id.* at 764–65. During questioning the respondent had admitted to taking a gun from a police officer and pointing it at the officer and to regularly using heroin. *Id.* at 764.

57. *Id.* at 766–67.

58. *Id.* at 766.

59. *Id.* at 767 ("Here [the respondent] was never made to be a 'witness' against himself in violation of the Fifth Amendment's Self-Incrimination Clause because his statements were never admitted as testimony against him in a criminal case.").

60. *See, e.g.*, Davies, *supra* note 5, at 988 ("According to the positions taken by six Justices in Chavez, the core right protected by the Fifth Amendment Self-Incrimination Clause consists merely of prohibiting the introduction of compelled statements or of derivative 'fruits' of such statements at a person's criminal trial . . . ."). The Supreme Court also recently re-visited the privilege in *Salinas v. Texas*, where it clarified that an accused must expressly invoke the privilege; the accused cannot merely stand silent and later claim that the government violated his privilege. 133 S. Ct. 2174, 2178 (2013).

61. Lower courts and commentators have coined the term "foregone conclusion doctrine." *See, e.g.*, *In re* Grand Jury Subpoena Duces Tecum, 670 F.3d 1335, 1343 (11th Cir. 2012) (discussing the Supreme Court's explanation that the documents were a foregone conclusion in

ment's protection from the act of producing the requested information or evidence if the government knows about the existence and location of the evidence.[62] Although producing information generally has a testimonial aspect, if the government can show that it had "prior knowledge of the existence, possession, and authenticity" of the information, the testimonial information becomes a "foregone conclusion."[63] Once the information is a foregone conclusion, compelled production no longer violates the Fifth Amendment.[64]

This doctrine first appeared in *Fisher v. United States*, where the Supreme Court held that a taxpayer's production of an accountant's documents would not constitute incriminating testimony,[65] because the existence and location of the papers were a "foregone conclusion," and the taxpayer would not add anything to the government's case by merely admitting to having the papers.[66] The Fifth Amendment is limited to situations in which a person is compelled to be a witness against himself in a criminal case by extorting information from that person.[67] In *Fisher*, however, the government was not extorting anything from the accused.[68] "A party is privileged from producing evidence but not from its production," and, in *Fisher*, the accused taxpayer was not compelled to testify against himself, or even to produce the papers.[69] Further, even if the taxpayer had been subpoenaed to produce the documents, production would not violate the privilege against self-incrimination because the taxpayer did not prepare the documents, and the documents did not contain testimonial declarations by the taxpayer.[70] Ultimately, *Fisher* clarified that the privilege only applies to testimonial assertions by the accused, and the accused can nevertheless be compelled to produce incriminating evidence that is not testimonial in nature.[71]

Fisher v. United States, 425 U.S. 391, 411 (1976), noting that "[t]his explanation became known as the 'foregone conclusion' doctrine").

62. *See, e.g.*, Bret E. Rasner, *International Travelers Beware: No Reasonable Suspicion Needed to Search Your Electronic Storage Devices at the Border*, 3 PHOENIX L. REV. 669, 695 (2010) ("The foregone conclusion doctrine can remove the Fifth Amendment protection from the act of production if the government already knows of the item and its whereabouts and obtaining it does not add to its case.").

63. Fruiterman, *supra* note 17, at 658.

64. Kenneth J. Melilli, *Act-of-Production Immunity*, 52 OHIO ST. L.J. 223, 236 (citing *Fisher*, 425 U.S. at 411) ("According to the Fisher Court, where the relevant testimonial component—existence, possession, or authentication—is a 'foregone conclusion,' then the testimonial aspect of the act of production is not protected by the fifth amendment.").

65. 425 U.S. at 414.

66. *See id.* at 411 (citation omitted).

67. *See id.* at 398.

68. *Id.*

69. *Id.* at 398–99 (quoting Johnson v. United States, 228 U.S. 457, 458 (1913)).

70. *Id.* at 409–11.

71. *Id.* at 410–11.

Later, *United States v. Hubbell* limited the doctrine, although no specific contours were defined.[72] In *Hubbell*, the respondent invoked his Fifth Amendment privilege and refused to comply with a subpoena ordering him to produce documents.[73] The Supreme Court explained that the act of producing the documents might have a compelled testimonial aspect because production would assert that the accused had control over the documents, and the accused could then be compelled to testify that all documents requested by the subpoena had been produced.[74] Moreover, because the privilege against self-incrimination also includes compelled statements that lead to incriminating evidence, even though the statements themselves were not incriminating,[75] the breadth of the documents requested was "tantamount to answering a series of interrogatories" that could lead to incriminating evidence.[76] *Hubbell* was unlike *Fisher*'s foregone conclusion because the government did not show that it had any specific knowledge of the papers or their location;[77] instead, the respondent would have had to use the contents of his own mind to identify all the documents the subpoena requested.[78] Although clarifying that the scope of the foregone conclusion doctrine did not extend to overbroad foregone conclusions—like a businessman possessing general business records to justify compelled production of a broad range of business documents—*Hubbell* failed to resolve the standard by which a "foregone conclusion" should be measured.[79]

C. *The Search Incident to Arrest Doctrine's Effect on the Fifth Amendment*

As will be discussed in Part V.B, the search incident to arrest doctrine may affect the Fifth Amendment based on the ability of law enforcement to retrieve incriminating evidence from the search of an arrestee's cell phone or computer. Evolving from *Chimel v. California*[80]

72. 530 U.S. 27 (2000).

73. *Id.* at 31.

74. *See id.* at 36–37.

75. *See id.* at 38 (citing Doe v. United States, 487 U.S. 201, 208 n.6 (1988)); *see also* Hoffman v. United States, 341 U.S. 479, 486 (1951) ("The privilege afforded not only extends to answers that would in themselves support a conviction under a federal criminal statute but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant for a federal crime.").

76. *Hubbell*, 530 U.S. at 41–42.

77. *See id.* at 44–45.

78. *See id.* at 43. The Supreme Court compared the assembly of the documents requested by the subpoena to verbally revealing the combination to a safe instead of "being forced to surrender the key to a strongbox." *Id.* (citing *Doe*, 487 U.S. at 210 n.9).

79. *See* Kaufman, *supra* note 17, at 37–38.

80. 395 U.S. 752 (1969).

and *United States v. Robinson*,[81] the doctrine later expanded to cover cell phones[82] but was recently restricted by the Supreme Court's decision in *Riley v. California*.[83]

In *Chimel*, the Supreme Court held that police officers may search an arrestee's person and the area within his immediate control for weapons and evidence that could easily be destroyed or concealed following the arrest.[84] Several years later, in *Robinson*, the Supreme Court expanded the doctrine to allow searches of closed containers found on the arrestee's person during the search incident to arrest, even without suspicion of illegal contents in the containers.[85] Then in 2007, in *United States v. Finley*, the United States Court of Appeals for the Fifth Circuit upheld the warrantless search of cell phones incident to arrest, noting that police can look for evidence on the arrestee's person,[86] and that the search extends to containers found on the arrestee's person.[87]

The cell phone issue finally reached the Supreme Court in *Riley*, where the Supreme Court acknowledged that the search incident to arrest doctrine "has been recognized for a century," but noted that "its scope has been debated for nearly as long."[88] Putting an end to that debate, the Supreme Court held that, generally, police may not search an arrestee's cell phone incident to a lawful arrest without first obtaining a search warrant.[89] Noting how "modern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy," the Supreme Court explained that today's cell phones "are based on technology nearly inconceivable just a few decades ago when *Chimel* and *Robinson* were decided."[90] The Supreme Court analyzed the two concerns addressed in *Chimel*—harm to officers and destruction of evidence—and determined that cell phones do not present the same concerns as the area within an arrestee's immediate control.[91] Further, due

81. 414 U.S. 218 (1973).

82. United States v. Finley, 477 F.3d 250 (5th Cir. 2007).

83. No. 13-132, slip op. at 6 (U.S. June 25, 2014).

84. 395 U.S. at 763.

85. 414 U.S. at 235–36.

86. 477 F.3d at 259–60 (citing *Robinson*, 414 U.S. at 233–34).

87. *See id.* at 260 (citing United States v. Johnson, 846 F.2d 279, 282 (5th Cir. 1988)). Like *Finley*, many other courts that confronted the issue also found a warrantless search of a cell phone found on the arrestee's person to be lawful under the search incident to arrest doctrine. *See, e.g.*, United States v. Grooms, No. 2:10-CR-87, 2011 U.S. Dist. LEXIS 10824, at *3–5 (E.D. Tenn. Jan. 3, 2011), United States v. Santillian, 571 F. Supp. 2d 1093, 1102–03 (D. Ariz. 2008).

88. No. 13-132, slip op. at 6.

89. *See id.* at 28.

90. *Id.* at 9.

91. *See id.* ("On the government interest side, *Robinson* concluded that the two risks identified in *Chimel*—harm to officers and destruction of evidence—are present in all custodial

to the vast quantity of personal information modern cell phones hold, the Supreme Court explained that cell phones are different from other physical objects that can be kept on an arrestee's person.[92] Nonetheless, the Supreme Court noted that officers can still search a cell phone incident to an arrest after obtaining a search warrant, and that exigent circumstances "may still justify a warrantless search . . . ."[93]

In addition to exigent circumstances that may justify a warrantless search, police can still obtain consent to search the arrestee's phone without a warrant.[94] Regardless of whether the arrestee consents to a warrantless search or police obtain a warrant, having a passcode on the phone further complicates the situation and has the potential to "shift the legal issues into more complicated Fourth and Fifth Amendment territory."[95]

If an arrestee has a passcode on the phone, police will have to ask for the passcode to unlock the phone, arguably constituting interrogation.[96] The hallmark interrogation case, *Miranda v. Arizona*, specified

arrests. There are no comparable risks when the search is of digital data."). First, digital data is not a weapon that can be used to harm a police officer or used to help the arrestee escape. *Id.* at 10. Second, "once law enforcement officers have secured a cell phone, there is no longer any risk that the arrestee himself will be able to delete incriminating data from the phone." *Id.* at 12. While the government expressed concerns about remote data wiping and phones being protected by unbreakable encryption once the phone locks, the Supreme Court declined to consider those concerns significant or prevalent enough to permit a warrantless search. *See id.* at 13. The Supreme Court also explained that officers likely have little time to search a cell phone at the scene of the crime anyway, so third parties would still have significant time to remotely wipe data. *Id.* at 14. Meanwhile, officers can just disconnect the phone from the network to prevent the possibility of data being wiped from the phone. *Id.* Additionally, the phone would likely lock anyway before an officer could search the phone. *Id.*

92. *Id.* at 17–19 ("First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone or even earlier. . . . Finally, there is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day.").

93. *Id.* at 25–26 ("Such exigencies could include the need to prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, and to assist persons who are seriously injured or are threatened with imminent injury.").

94. *See, e.g.*, Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973) ("[O]ne of the specifically established exceptions to the [Fourth Amendment's] requirements of both a warrant and probable cause is a search that is conducted pursuant to consent.").

95. Adam M. Gershowitz, *Password Protected? Can a Password Save Your Cell Phone from a Search Incident to Arrest?*, 96 IOWA L. REV. 1125, 1144 (2011).

96. *See id.* at 1166. Consider the case of *People v. Rangel*, where officers searched a suspect's house pursuant to a valid search warrant authorizing the seizure of items that constitute "gang indicia," and found a smartphone that had been next to the suspect when they entered his room.

that procedural safeguards must be provided prior to custodial interrogation that secure the privilege against self-incrimination.[97] The Supreme Court defined custodial interrogation as "questioning initiated by law enforcement officers after a person has been taken into custody or otherwise deprived of his freedom of action in any significant way."[98] However, the Supreme Court has also held that a violation of the *Miranda* rule does not require suppression of physical evidence obtained as a result of the violation.[99] Thus, as Professor Adam Gershowitz suggests, "[i]f police obtain an arrestee's password in violation of *Miranda*, an officer's statement conceding knowledge of the password will be inadmissible, but any valuable resulting evidence—for instance incriminating text messages . . . found on the phone—will be admissible."[100] Additionally, police and prosecutors may rely on a subpoena to either compel production of the password or to compel production of encrypted data.[101] The subpoena has typically been the preferred means of compulsion because it is less intrusive than a search, involves no entry, and avoids most Fourth Amendment concerns.[102]

206 Cal. App. 4th 1310, 1313 (Cal. Ct. App. 2012). Police read the suspect his *Miranda* rights and the suspect agreed to speak with a detective. *Id.* When the detective asked the suspect for his girlfriend's name and phone number, the suspect replied that it was in his phone, and he (the suspect) would have to look it up. *Id.* at 1313–14. The detective then asked, "[d]o you give me permission to look in your phone so I can get her phone number," to which the suspect responded, "[t]here's personal stuff in there. If you want I can call her and tell her." *Id.* at 1314. Not surprisingly the detective responded, "[i]t helps more if I can do it. You know what I mean? Then it makes it look, you know, a little more forthcoming." *Id.* The detective then asked again if he could look in the suspect's phone, and the suspect said yes but did not tell the detective that he could only look in the contact or directory section of the phone. *Id.* After the interview, the detective retrieved the suspect's smartphone and read the file of text messages between the suspect and his girlfriend, some of which appeared to link the suspect to the alleged crime. *Id.* The court later denied a motion to suppress the text messages because they had been retrieved with a valid search warrant for "gang indicia," and a smartphone is an item that could logically contain "gang indicia" in the form of text messages and directories. *Id.* at 1316–17. Although *Rangel* concerns the Fourth Amendment, it is an example of the interrogation setting in which a suspect waives his *Miranda* rights, begins talking, and is ultimately persuaded into allowing the detective to search his smartphone for incriminating evidence that is later used against him at trial.

97. 384 U.S. 436, 444 (1966).

98. *Id.*

99. *See* United States v. Patane, 542 U.S. 630, 636–37 (2004) (declining to extend the fruit of the poisonous tree doctrine to the *Miranda* rule, holding that the self-incrimination clause "is not implicated by the admission into evidence of the physical fruit of a voluntary statement").

100. Gershowitz, *supra* note 95, at 1168. Professor Gershowitz suggests that even if police demand a passcode, instead of merely requesting it, police likely still have not "compelled an arrestee to incriminate himself with a testimonial response in violation of the Fifth Amendment's protection against self-incrimination." *Id.*

101. *See* Larkin, *supra* note 17, at 263, 278.

102. *See, e.g.*, *id.* at 263 (citing *In re* Establishment Inspection of Skil Corp., 846 F.2d 1127, 1133 (7th Cir. 1988)). Some forensic software even allows an agent to view the contents of a hard drive without first determining whether a password is necessary to access the computer. *See* United States v. Andrus, 483 F.3d 711, 713–14 (10th Cir. 2007).

Further, if police obtain a search warrant, they can also try to crack the passcode or hack into the phone.[103] And, of course, police may also have to simply give up on the cell phone search if they fail to obtain consent to search and are unable to access the phone after procuring a search warrant.[104] Nonetheless, while there remain ways for police to search an arrestee's cell phone incident to a lawful arrest, a passcode provides the user with some level of protection in cell phone data by at least requiring police to figure out a way to obtain or bypass the passcode.

III. ENCRYPTED DATA VS. THE FIFTH AMENDMENT: THE CIRCUIT SPLIT

A. *Encryption 101*

Encryption is the process by which information is converted into an unreadable form through the use of mathematical algorithms.[105] The use of these algorithms allows "an individual to 'encrypt' a message by transforming its original form . . . into an unreadable form . . . . Anyone who later obtains possession of the message will be unable to read it without first 'decrypting' the message—by using a 'key' or by breaking the code."[106] The text essentially becomes unreadable, appearing as random letters, numbers, and symbols, unless the correct password is entered to unscramble the text.[107]

Encryption has become so standard that computer and software manufacturers consider it a basic security measure; even if the data is lost or stolen, it could not be accessed without the owner's password to decrypt it.[108] Moreover, encryption also provides "critical protection for data stored on individuals' personal computers. People keep vast amounts of information on their digital devices, ranging from personal correspondence to Internet browsing histories to sensitive medical details."[109] As such, encryption is especially useful—and necessary—on devices that can easily be lost or stolen, such as cell phones, tablets, and laptops.[110]

103. *See* Gershowitz, *supra* note 95, at 1164.

104. *See id.* at 1154; *see also* Riley v. California, No. 13-132, slip op. at 12–13 (U.S. June 25, 2014) (explaining how when a phone locks with encryption security features the phone becomes "all but 'unbreakable' unless police know the password").

105. *See* Kenneth P. Weinberg, *Cryptography: "Key Recovery" Shaping Cyberspace (Pragmatism and Theory)*, 5 J. INTELL. PROP. L. 667, 673–74 (1998).

106. *Id.* at 674. For example, the algorithm "?3?" transforms the word "code" to "frgh" by changing each letter to the letter three letters later in the alphabet. *See id.* at 673.

107. *See id.* at 673–74.

108. *See* Fruiterman, *supra* note 17, at 659.

109. *Id.* at 660.

110. *See* Kaufman, *supra* note 17, at 36; *see also* Guy McDowell, *How to Encrypt Data on*

Most new computers have built-in encryption security as a basic feature.[111] Apple's iOS platform on iPads, iPhones, and iPods also uses encryption and data protection that protects the user's data by either preventing access or wiping the operating system clean if lost or stolen.[112] However, most Android phones do not currently have built-in data encryption.[113] And neither iOS nor Android automatically encrypts text messages where the user is required to enter a passcode to decrypt the data before viewing the actual message. Regardless, using a passcode on the phone in general can protect text messages by requiring the user to enter the correct passcode before he or she can read the message. Third-party smartphone applications are also available, which will encrypt text messages and emails.[114] Further, text message encryption applications are available for the iPhone, which require the recipient of a text message to enter a passcode to view the message.[115] Finally, text messages between iPhone users on the iMessage platform are encrypted

Your Smartphone, MAKEUSEOF (Aug. 14, 2014), http://www.makeuseof.com/tag/how-to-encrypt-data-on-your-smartphone/ ("To really secure your information, you need to use some sort of encryption. By encrypting the data on your phone, even if someone gets past your lock screen, whatever else is on the phone is pretty much useless to them."). Statistics show that eighty-six percent of Internet users have used strategies to avoid being observed online, including fourteen percent who have encrypted their communications. *See* Lee Rainie, Sara Kiesler, Ruogu Kang & Mary Madden, *Anonymity, Privacy, and Security Online*, PEW RES. INTERNET PROJECT (Sept. 5, 2013), http://www.pewinternet.org/Reports/2013/Anonymity-online/Summary-of-Findings/Key-findings.aspx.

111. For example, one recent Apple Mac operating system, OS X Mavericks, includes FileVault 2, which encrypts the entire Mac drive and all of its data, and also includes the ability to encrypt any removable drive. *See Apple—OS X Mavericks*, APPLE, http://apple.com/osx/what-is/security.html (last visited Aug. 15, 2014).

112. *See iOS Security*, APPLE, http://images.apple.com/iphone/business/docs/iOS_Security_Feb14.pdf (last visited Aug. 9, 2014). Apple also provides additional protection with the ability to wipe clean all the data on a phone after ten failed password attempts. *See* APPLE, IPHONE USER GUIDE FOR IOS 7 (Oct. 2013), *available at* http://manuals.info.apple.com/MANUALS/1000/MA1565/en_US/iphone_user_guide.pdf.

113. *See* Alex Wawro, *How to Encrypt Your Smartphone*, TECHHIVE (Oct. 28, 2011, 6:00 PM), http://www.techhive.com/article/242650/how_to_encrypt_your_smartphone.html. Android is a mobile operating system developed by Google. *See Discover Android*, ANDROID, http://www.android.com/about/ (last visited Aug. 15, 2014).

114. *See* Wawro, *supra* note 113. For example, Android users have options such as AnDisk Encryption to encrypt specific files or folders on their phones, as well as options like TextSecure to encrypt text messages. *Id.* "TextSecure uses an advanced end to end encryption protocol that provides privacy for every message every time." *TextSecure Private Messenger*, GOOGLE PLAY, http://play.google.com/store/apps/details?id=org.thoughtcrime.securesms&hl=en (last visited Aug. 9, 2014).

115. *See* Casey Chan, *Sending Secret Encrypted Text Messages on Your iPhone Just Got Easier*, GIZMODO (Jan. 29, 2013, 10:00 PM), http://gizmodo.com/5980083/sending-secret-encrypted-text-messages-on-your-iphone-just-got-easier; *Encrypt SMS*, APPLE, http://itunes.apple.com/us/app/encrypt-sms/id432891578?mt=8 (last visited Aug. 15, 2014); *Encrypt SMS—Send Secret Text Messages*, APPLE, http://itunes.apple.com/us/app/encrypt-sms-send-secret-text/id349861478 (last visited Aug. 15, 2014).

via "end-to-end encryption" and are only stored by Apple "in encrypted form for a limited period of time."[116] This "end-to-end encryption" has made it impossible for law enforcement to intercept iMessages.[117]

Undoubtedly, with the growing use of encryption to protect personal data, the government's attempts to compel production of passwords or encrypted data will also grow.[118] Whether such compulsion violates an individual's Fifth Amendment privilege to be free from self-incrimination poses interesting and unresolved questions.

B. *The Circuit Split: Compelled Self-Incrimination or Not?*

Several decisions to date demonstrate the disparate views regarding the Fifth Amendment privilege to be free from self-incrimination and compelled disclosure of passwords or production of encrypted data.[119] Some courts have prohibited compelled disclosure of a password or production of encrypted data due to the privilege against self-incrimination, while others have determined that it does not violate the privilege.[120]

---

116. Zack Whittaker, *U.S. Government Can't Intercept iMessage, but It Can Still Serve Apple a Search Warrant*, ZDNET (Apr. 4, 2013), http://www.zdnet.com/u-s-government-cant-intercept-imessage-but-it-can-still-serve-apple-a-search-warrant-7000013533/ [hereinafter Whittaker *iMessage*] (citing *Apple Inc. Software License Agreement for OS X Mountain Lion*, APPLE, *available at* http://images.apple.com/legal/sla/docs/OSX108.pdf (last visited Sept. 1, 2014)).

117. *See id.* Title III of the Omnibus Crime Control and Safe Streets Act, commonly referred to as the "Electronic Communications Privacy Act" or the "Federal Wiretap Act," regulates wiretapping and electronic surveillance. 68 AM. JUR. 2D *Searches and Seizures* § 339 (2013). Pursuant to this Act, federal law authorizes interception of wire, oral, or electronic communications by court order when such interception may provide evidence of certain crimes. 18 U.S.C. § 2516. The judge may approve the order if there is probable cause to believe the individual is committing or about to commit one of the offenses in section 2516. § 2518(3).

118. *See* Fruiterman, *supra* note 17, at 660.

119. *See* discussion *infra* Part III.B.

120. *Compare In re* Grand Jury Subpoena Duces Tecum, 670 F.3d 1335, 1349 (11th Cir. 2012) (the government could not show that the contents of a hard drive were a foregone conclusion, so decryption and production would be testimonial and would implicate the Fifth Amendment), *and* United States v. Kirschner, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) (compelled production of a password violated the defendant's Fifth Amendment privilege), *with* Order Granting *Ex Parte* Request for Reconsideration of the United States's Application Under the All Writs Act at 3, *In re* Decryption of a Seized Data Storage System, No. 13-M-449 (E.D. Wis. May 21, 2013) [hereinafter Order Granting *Ex Parte* Request for Reconsideration] (holding on reconsideration that it was a foregone conclusion that the defendant had access to and control over the encrypted files, so Fifth Amendment protection was no longer available), United States v. Fricosu, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012) (the Fifth Amendment was not implicated because the government knew of the existence and location of the documents based on a recorded phone conversation), *and In re* Boucher, No. 2:06-mj-91, 2009 U.S. Dist. LEXIS 13006, at *10 (D. Vt. Feb. 19, 2009) (the defendant had no act of production privilege because he admitted to possession of the computer and had previously provided the government with access). The Supreme Court has yet to address the issue.

1. The Fifth Amendment Prohibits Compelled Disclosure or Decryption

Most recently, the United States Court of Appeals for the Eleventh Circuit considered self-incrimination in relation to encrypted documents, applying *Hubbell*'s narrower view of the foregone conclusion doctrine.[121] The Eleventh Circuit held that the appellant's decryption and production of hard drive contents would be testimonial in nature and that, because the government could not show that the contents were a "foregone conclusion," the Fifth Amendment applied.[122] The government had subpoenaed the appellant to produce the decrypted contents of his hard drives, but the appellant refused, invoking the Fifth Amendment.[123] On appeal, the court noted that the files themselves were not testimonial in nature.[124] However, under *Fisher* and *Hubbell*, production was testimonial because the decryption password required the appellant to use "the contents of the mind" to produce information that could be incriminating.[125]

Similarly, the United States District Court for the Eastern District of Michigan refused to compel production of a computer password because production would communicate a factual assertion to the government, which could reveal knowledge that might lead to incriminating evidence.[126] Thus, it appears that in cases in which the government cannot show with "reasonable particularity" that it knew files existed on the hard drives or that the accused could even access the encrypted hard drives, compelled "testimony" in the form of a password would violate the privilege to be free from self-incrimination.[127]

2. Compelled Disclosure or Decryption Does Not Violate the Fifth Amendment

Several decisions from lower courts have taken the alternative

121. *See In re Grand Jury Subpoena Duces Tecum*, 670 F.3d at 1352.

122. *See id.* at 1349.

123. *See id.* at 1337–39.

124. *Id.* at 1342.

125. *Id.* at 1345–46 (citing United States v. Hubbell, 530 U.S. 27, 43 (2000)).

126. *See* United States v. Kirschner, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010).

127. *See In re Grand Jury Subpoena Duces Tecum*, 670 F.3d at 1346. Also see *United States v. Pearson*, where, although the government knew the defendant's laptop contained incriminating encrypted files, some of the encrypted files had allegedly been prepared by the defendant's father—who was also his attorney—and were attorney-client privileged material. No. 1:04-CR-340, 2006 U.S. Dist. LEXIS 32982, at *60–62 (N.D.N.Y. May 24, 2006). The United States District Court for the Northern District of New York noted that production of the password would authenticate the encrypted files that the defendant had prepared, but because the defendant's father had prepared some of the files, production of the password would not authenticate all the files. *Id.* at 62. Thus, the government would have to show that it could authenticate the files by means other than a compelled password. *Id.*

view: compelled disclosure of passwords or production of encrypted data does not violate the privilege to be free from self-incrimination.[128] For example, the United States District Court for the District of Colorado held that requiring production of encrypted contents of a laptop did not implicate the Fifth Amendment because the government knew the files existed and knew where they were located based on a recorded phone conversation between the defendant and her husband.[129] Relying on the limited precedent dealing with compelled password production, the court noted that while the contents of a document may not be privileged, the act of producing the document might nonetheless be privileged because the act of production acknowledges the document's existence.[130]

Similarly, the United States District Court for the Eastern District of Wisconsin reversed a previous denial to compel a defendant to decrypt electronic data upon the government's discovery of new information that rendered the contents of a hard drive a "foregone conclusion."[131] The court had initially denied the government's motion to compel production because the government had not established that the defendant "actually had access to and control over the encrypted storage devices and, therefore, the files contained therein."[132] However, agents were eventually able to access part of one of the hard drives, which contained the incriminating evidence along with the defendant's personal financial records and photographs of the defendant.[133] Consequently, under *Fisher*, the act of producing the decrypted data would not use the contents of the defendant's mind against him because the government was no longer relying on the defendant's truth-telling to prove

128. Additionally, some legal scholars argue that courts should interpret the Fifth Amendment so as to permit compelled production of passwords or decrypted content to balance the state's interest and the individual's interest. *See generally* Dan Terzian, *The Fifth Amendment, Encryption, and the Forgotten State Interest*, 61 UCLA L. REV. DISCOURSE 298 (2014) (emphasizing the importance of the state's interest).

129. *See* United States v. Fricosu, 841 F. Supp. 2d 1232, 1235, 1237 (D. Colo. 2012). The defendant and her husband discussed something being on the laptop and discussed refusing to provide the password. *Id.* at 1235. Although the government did not know the specific contents of the documents located on the encrypted laptop, that lack of knowledge did not prohibit production. *See id.* at 1237 (citation omitted).

130. *See id.* at 1236 (citing United States v. Doe, 465 U.S. 605, 612 (1984); *Hubbell*, 530 U.S. at 36).

131. *See* Order Granting *Ex Parte* Request for Reconsideration, *supra* note 120, at 3.

132. *Id.* at 2 (quoting Order Denying Application to Compel Decryption at 8, *In re* Decryption of a Seized Data Storage System, No. 13-M-449 (E.D. Wis. Apr. 19, 2013)). The storage devices in question were found in the defendant's home where he lived alone, but the computer only had the username "Jeff" on the login screen, and the defendant had not admitted to access and control over the encrypted devices. *Id.* (citing Order Denying Application to Compel Decryption, *supra* note 132, at 8–9).

133. *Id.* at 2–3.

that the data existed or that he had access to the data.[134]

Likewise, in *In re Boucher*, the United States District Court for the District of Vermont also relied on the foregone conclusion doctrine in determining that compelled production of a decrypted version of a laptop hard drive did not violate the privilege.[135] In *In re Boucher*, the defendant initially provided access to the incriminating files, but later refused to provide the password.[136] However, because the defendant already provided access to the drive once, providing access again would add "little or nothing to the sum total of the Government's information . . . ."[137] Further, the defendant did not have an act of production privilege because he already admitted to possession of the computer, so his act of producing a decrypted version was not necessary to authenticate the data.[138]

These cases seem to denote that the foregone conclusion doctrine, in many cases, will avoid a Fifth Amendment violation. However, the lack of clarity regarding the proper standard to apply to the foregone conclusion doctrine remains a problem.[139] Without the Supreme Court addressing the confusion, it remains to be seen as to whether compelled disclosure of passwords or production of encrypted data is a testimonial act that would implicate the privilege to be free from self-incrimination.

IV. THE "BIOMETRIC REVOLUTION"

Biometrics are "measurable biological (anatomical and physiological) and behavioral characteristic[s] that can be used for automated recognition."[140] Biometric authentication is the method of identifying a person by his or her unique physical characteristics.[141] At the most basic level, "an individual's physical traits are scanned by a machine and then a comparison is made to a database containing previously stored information about that individual."[142] Biometric authentication can be used to either verify that the person is who he or she claims to be, or to identify

134. *See id.* at 1–3 ("[T]he government has now persuaded me that it is a 'foregone conclusion' that [the defendant] has access to and control over the subject encrypted storage devices.").

135. No. 2:06-mj-91, 2009 U.S. Dist. LEXIS 13006, at *10 (D. Vt. Feb. 19, 2009).

136. *See id.* at *4–5.

137. *Id.* at *9 (quoting Fisher v. United States, 425 U.S. 391, 411 (1976)).

138. *See id.* at *9–10.

139. *See supra* note 79 and accompanying text.

140. NAT'L SCI. & TECH. COUNCIL SUBCOMM. ON BIOMETRICS & IDENTITY MGMT., BIOMETRICS GLOSSARY 4 (2006), *available at* http://biometrics.gov/Documents/Glossary.pdf [hereinafter NSTCS BIOMETRICS GLOSSARY].

141. *See* Ng, *supra* note 14, at 428.

142. *Id.*

an unknown person.[143] For example, when someone shows up at a security checkpoint claiming to be "John Doe," that person's biometrics are checked against the system which contains the biometrics of "John Doe," and the system verifies that the person is in fact that particular "John Doe."[144] Alternatively, an unknown person's biometrics can be checked against a database to determine who that person is, such as matching a fingerprint found at a crime scene to the FBI's database.[145]

The use of biometrics by the government and governmental agencies is nothing new.[146] In 2008, President George W. Bush signed the "Directive on Biometrics for Identification and Screening To Enhance National Security,"

> establish[ing] a framework to ensure that Federal executive departments and agencies . . . use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under United States law.[147]

The use of biometrics has also been prevalent in commerce and commercial security due to the recent proliferation of "electronic identities" and the need to ensure proper identification.[148] Innovative companies have tapped into this niche market by developing biometric

143. *See* NSTCS BIOMETRICS GLOSSARY, *supra* note 140 (defining "identification"). Using biometrics to verify that someone is whom he or she claims to be is known as "closed-set identification," or "one-to-one matching." *See id.* (defining "closed-set identification"); Robin Feldman, *Considerations on the Emerging Implementation of Biometric Technology*, 25 HASTINGS COMM. & ENT. L.J. 653, 655–56 (2003) (explaining "one-to-one matching").

144. *See* Feldman, *supra* note 143, at 655–56.

145. *See id.* at 656. Comparing an unknown person's biometrics against a database is referred to as "open-set identification," or "one-to-many matching." *See* NSTCS BIOMETRICS GLOSSARY, *supra* note 140 (defining "open-set identification"); Feldman, *supra* note 143, at 656 (explaining "one-to-many matching").

146. *See, e.g.*, *Standards for Biometric Technologies: Hearing Before the Subcomm. on Gov't Operations of the H. Comm. on Oversight & Gov't Reform*, 113th Cong. 2 (2013) (testimony of Charles H. Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology, United States Department of Commerce) [hereinafter *Standards*], *available at* http://docs.house.gov/meetings/GO/GO24/20130619/101010/HHRG-113-GO24-Wstate-RomineC-20130619.pdf ("For decades, biometric technologies were used primarily in law enforcement applications, and they are still a key component of these important applications.").

147. Directive on Biometrics for Identification and Screening To Enhance National Security, 1 PUB. PAPERS 757 (June 5, 2008), *available at* http://www.gpo.gov/fdsys/pkg/PPP-2008-book1/pdf/PPP-2008-book1-doc-pg757.pdf. The directive acknowledged that many agencies were already collecting biometric information in their identification and screening processes, and that the harmonization of their collecting, storing, and sharing procedures would help identify "individuals who may do harm to Americans and the Nation . . . ." *Id.*

148. *See Government Biometrics Activity*, BIOMETRIC CONSORTIUM, http://biometrics.org/government.php (last visited Aug. 9, 2014); *see also Standards*, *supra* note 146, at 2 ("Over the past several years, the marketplace for biometrics solutions has widened significantly and today includes public and private sector applications worldwide.").

authentication products solely for commerce.[149]

A. *An Array of Biometric Authentication Methods*

Various biometric authentication methods currently exist. Some of the more prevalent ones include fingerprint analysis, facial recognition, iris scanning, voice recognition, and DNA analysis. However, fingerprint identification has been the most commonly used and accepted form of biometric authentication.[150]

Fingerprint identification has been used in the criminal context by law enforcement since the early twentieth century.[151] Due to the high degree of confidence in fingerprint identification and the ease in which fingerprint sensors can be embedded in devices, "fingerprint-based authentication is becoming more and more popular in a number of civilian and commercial applications such as, welfare disbursement, cellular phone access and laptop computer log-in."[152] All fingertips have unique ridge formation patterns.[153] Fingerprint identification involves comparing these unique ridge formations with stored formations.[154] Fingerprint authentication provides benefits over other forms of biometric authentication because fingerprints do not change throughout the course of an individual's lifetime,[155] no two people have the same ridge formation, and it is a quick and noninvasive means of identification.[156] However, because dirt, oils, or cuts on the finger can result in identification errors,[157] and because fingerprints can easily be lifted from surfaces with tape, fingerprint authentication also has disadvantages.[158]

149. *See, e.g.*, *Biometrics in E-commerce*, BIOENABLE, http://www.biometricsintegrated.com/biometrics-in-e-commerce (last visited Aug. 9, 2014) (offering e-commerce biometric products and software).

150. *See* Ng, *supra* note 14, at 429.

151. *See id.* The Federal Bureau of Investigation's fingerprint database contains fingerprints and corresponding criminal history of more than 47 million people. *See id.*

152. A. Jameer Basha et al., *Efficient Multimodal Biometric Authentication Using Fast Fingerprint Verification and Enhanced Iris Features*, 7 J. COMPUTER SCI. 698, 698 (2011).

153. *See* Ng, *supra* note 14, at 429.

154. *See id.*

155. However, Apple warns that "[c]ertain activities can . . . temporarily affect fingerprint recognition, including exercising, showering, swimming, cooking, or other conditions or changes that affect your fingerprint." *Using Touch ID*, *supra* note 1.

156. *See* Ng, *supra* note 14, at 429–30.

157. *See Using Touch ID*, *supra* note 1.

158. *See* Jose Pagliery, *iPhone Fingerprint Scanner Will Start Security Revolution*, CNNMONEY (Sept. 11, 2013, 3:04 PM), http://money.cnn.com/2013/09/11/technology/security/iphone-fingerprint-scanner/index.html. Indeed, fingerprint misidentifications do occur. *See, e.g.*, Mayfield v. United States, 599 F.3d 964, 966 (9th Cir. 2010) (discussing the false positive fingerprint identification of Brandon Mayfield following the 2004 terrorist bombing on commuter trains in Madrid, Spain); Simon A. Cole, *More than Zero: Accounting for Error in Latent Fingerprint Identification*, 95 J. CRIM. L. & CRIMINOLOGY 985 (2005) (reviewing known fingerprint misidentification cases and explaining the potential identification error rate).

Facial recognition technology is an increasingly discussed method of biometric authentication.[159] "Facial recognition . . . involves taking a picture of a subject's face or capturing [his or her] image from video surveillance. The system then processes the image and converts it into a digital template based on the geometry of the individual's face."[160] One of facial recognition technology's benefits is its unobtrusive nature due to the ability to capture images without the suspect's knowledge or cooperation.[161] Additionally, changes in hairstyle, color, and facial expressions do not impede the technology's ability to identify subjects.[162] However, facial recognition technology is not as accurate as other methods of biometric authentication due to poor lighting, shadows, and glare.[163]

Iris scanning is another emerging means of biometric authentication. Iris scanning involves scanning the colored part of the eye surrounding the pupil and comparing it to stored images in a database.[164] The iris structure is unique to each individual based on "the [cornea], pits, filaments, crypts, striation, radial furrows, and other structures."[165] Iris scanning is non-invasive, can be done from up to three feet away, and results are available in seconds.[166] However, iris scanning has its disadvantages because the subject needs to cooperate to obtain a usable iris image and sunglasses prevent the scans.[167]

Voice recognition is another form of biometric authentication, which identifies an individual based on his or her voice.[168] The voice recognition system "analyzes the frequency content of the speech and compares characteristics such as the quality, duration, intensity, dynamics, and pitch of the signal."[169] The system then compares the voice of

159. *See, e.g.*, Yana Welinder, *Facing Real-Time Identification in Mobile Apps & Wearable Computers*, 30 SANTA CLARA COMPUTER & HIGH TECH. L.J. 89 (2004) (discussing real-time facial recognition applications in mobile devices). Facial recognition first generated public discussion after the 2001 Super Bowl when it was used as a trial to compare surveillance images of attendees to a mug shot database. *See* NAT'L SCI. & TECH. COUNCIL SUBCOMM. ON BIOMETRICS & IDENTITY MGMT., FACE RECOGNITION 1 (2006), *available at* http://biometrics.gov/Documents/FaceRec.pdf [hereinafter NSTCS FACE RECOGNITION].

160. Ng, *supra* note 14, at 432.

161. *See id.*

162. *See id.*

163. *See id.* at 433.

164. *See id.* at 431. An infrared scan reveals the patterns in the iris structure. *See* Feldman, *supra* note 143, at 661.

165. Ng, *supra* note 14, at 431 n.55 (citation omitted).

166. *See id.* at 431.

167. *See id.* at 432.

168. *See* NAT'L SCI. & TECH. COUNCIL SUBCOMM. ON BIOMETRICS & IDENTITY MGMT., SPEAKER RECOGNITION 1 (2006), *available at* http://biometrics.gov/Documents/SpeakerRec.pdf [hereinafter NSTCS SPEAKER RECOGNITION].

169. *Id.*

the subject saying a fixed password to the voice that is programmed into the system for that password.[170] While voice recognition is a relatively simple authentication method, it also poses significant concerns because background noise can affect the authentication and because voices can change.[171]

Another widely accepted means of biometric authentication is DNA analysis.[172] DNA has been called "the instruction manual for every living organism."[173] DNA is found in blood, semen, saliva, vaginal secretions, skin, hair roots, urine, feces, bones, teeth, nasal secretion, vomitus, and cells from any tissues or organs.[174] The FBI has the ability to compare suspects' DNA through its Combined DNA Index System ("CODIS").[175] Unlike the noninvasive nature of fingerprint analysis, a disadvantage of DNA analysis is that it generally involves invasive techniques, such as taking a blood sample or mouth swab.[176] Nonetheless, because a tiny amount of DNA found at a crime scene can be amplified and reliably compared to the FBI's database, DNA analysis is the preferred method of identification for law enforcement.[177]

B. *Biometric Authentication's Growing Prevalence in Consumer Devices*

In 2011, approximately seventy-five percent of households reported having a computer.[178] Moreover, in 2013, ninety-one percent of American adults reported owning a cell phone, and the percentage of American adults who own a smartphone instead of a basic cell phone continues to grow.[179] In late 2013, Apple unveiled its then-latest version of the

170. *See id.*

171. *See* John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns—Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 107 (1997).

172. *See* Ng, *supra* note 14, at 431.

173. CECILIA HAGEMAN ET AL., DNA HANDBOOK 3 (2002).

174. *See id.* at 22–23. A person's DNA profile resembles a bar code; each line represents the size of the specific piece of DNA, known as short tandem repeats ("STR"). *See id.* at 1. "Due to the significant variability in the sizes of STR DNA possible . . . an individual's genetic profile is extremely unlikely to be found elsewhere in the world, except in the case of identical siblings." *Id.*

175. *See* Maryland v. King, 133 S. Ct. 1958, 1968 (2013).

176. *See* Ng, *supra* note 14, at 431.

177. *See id.* at 430–31. The Supreme Court has also acknowledged that "the utility of DNA identification in the criminal justice system is already undisputed. . . . [L]aw enforcement, the defense bar, and the courts have acknowledged DNA testing's 'unparalleled ability both to exonerate the wrongly convicted and to identify the guilty.'" *King*, 133 S. Ct. at 1966 (citation omitted).

178. *See* U.S. CENSUS BUREAU, COMPUTER AND INTERNET USE IN THE UNITED STATES 1 (2013), *available at* http://www.census.gov/prod/2013pubs/p20-569.pdf.

179. *See* Aaron Smith, *Smartphone Ownership 2013*, PEW RES. INTERNET PROJECT (June 5, 2013), http://pewinternet.org/Reports/2013/Smartphone-Ownership-2013/Findings.aspx. For example, in May 2013, fifty-six percent of U.S. adults indicated that they owned a smartphone, up

smartphone, the iPhone 5s, which included a fingerprint reader called Touch ID.[180] In response to Apple's release, HTC debuted its version of a fingerprint sensor in the HTC One Max, a competing Android smartphone.[181] Critics suggest, "Apple's combination of ease-of-use and more robust security is why Touch ID will help popularize fingerprint and other biometric scanners on consumer gadgets . . . ."[182] Additionally, "security experts largely see Touch ID as a positive step that could take society a step closer to eliminating much more hack-prone PINs and passwords . . . ."[183]

One overwhelming benefit of biometric authentication on personal devices is always having the means of identification with you.[184] With biometric authentication, the days of straining to remember complex passwords could cease to exist. Fingerprint readers are also available on laptops.[185] Fingerprint authentication specifically "has increasingly seen an uptick in consumer devices, notably laptops. With a swipe of a finger, a device can unlock or decrypt documents without the need for remembering passwords."[186] Some smartphones even offer "Face Unlock," which uses the phone's camera and facial recognition technology to

from forty-six percent in February 2012 and thirty-five percent in May 2011, according to the Pew Research Center. *Id.* A smartphone is "a cellular phone 'that has the ability to store data, photographs, and videos.'" People v. Rangel, 206 Cal. App. 4th 1310, 1313 (Cal. Ct. App. 2012). A smartphone is "akin to a personal computer because it has the capacity to store people's names, telephone numbers and other contact information, as well as music, photographs, artwork, and communications in the form of e-mails and messages . . . ." *Id.* at 1316.

180. *See Using Touch ID*, *supra* note 1 and accompanying text. "To set up Touch ID, you must first set a passcode. Touch ID is designed to minimize the input of your passcode, but you need a passcode for additional security validation, such as enrolling new fingerprints." *Using Touch ID*, *supra* note 1. "If Touch ID doesn't recognize your finger, you'll be asked to try again. After three attempts, you'll be given the option of entering your passcode. After two more tries, you will need to enter your passcode." *Id.* Additionally, the user must enter the passcode in three instances: (1) after restarting the iPhone; (2) when more than forty-eight hours elapsed since the iPhone was last unlocked; and (3) to enter the Touch ID and Passcode setting screen. *See id.*

181. *See* David Quinn, *HTC One 2 (M8) to Use Sapphire for Its Fingerprint Scanner?*, ANDROIDORIGIN (Jan. 1, 2014), http://www.androidorigin.com/htc-one-2-sapphire-fingerprint-scanner/.

182. Pagliery, *supra* note 158.

183. *Id.*

184. *E.g.*, *iPhone 5s: About Touch Security*, APPLE, http://support.apple.com/kb/HT5949 (last modified Mar. 8, 2014) ("Your fingerprint is one of the best passcodes in the world. It's always with you, and no two are exactly alike.").

185. *See, e.g.*, *Using HP SimplePass Fingerprint Reader (Windows 8)*, HEWLETT-PACKARD, http://h10025.www1.hp.com/ewfrf/wc/document?cc=us&lc=en&dlc=en&docname=c03653209 (last visited Aug. 9, 2014) (explaining fingerprint readers included on some HP notebook computers).

186. Zack Whittaker, *iPhone 5S Fingerprint Reader: Doubling Down on Identity, a Death Knell to Passwords?*, ZDNET (Sept. 11, 2013), http://www.zdnet.com/iphone-5s-fingerprint-reader-doubling-down-on-identity-a-death-knell-to-passwords-7000020547/ [hereinafter Whittaker *iPhone*].

unlock the phone with a scan of the user's face.[187] Undoubtedly, the smartphone mass market will continue to drive the growth of biometric authentication in other consumer devices.[188] Moreover, because biometric authentication provides a more secure method of identification, an increased prevalence of biometric authentication in personal devices has the ability to boost mobile commerce.[189] As companies' revenues increase due to a boost in mobile commerce from biometric authentication, funding for biometric development will likely increase.[190] As research and development increases, the prevalence in consumer devices will also likely increase, continuing to fuel the "Biometric Revolution."[191]

V. THE "BIOMETRIC REVOLUTION" MEETS THE FIFTH AMENDMENT

With the growing prevalence of biometric authentication in our everyday lives,[192] it is important to consider how it may impact our basic constitutional rights. Although biometric authentication is nothing new for the government or organizations using the latest in security measures,[193] biometric authentication is a relatively new concept for the general public with its arrival in the form of portable consumer devices. The iPhone 5s has introduced biometric authentication everywhere people go—homes, schools, malls, workplaces, restaurants, gyms, and libraries. Given the prevalence of the iPhone and Apple's industry-leading position, some have noted that we can expect the use of biometric

187. *See Introducing Android 4.0*, ANDROID, http://www.android.com/about/ice-cream-sandwich/ (last visited Aug. 9, 2014) (noting that the user still has the option to use a backup PIN or pattern to unlock the phone).

188. *See* King, *supra* note 9.

189. *See id.*

190. *See, e.g.*, Ben McClure, *R&D Spending and Profitability: What's the Link?*, INVESTOPEDIA (Sept. 30, 2010), http://www.investopedia.com/articles/fundamental-analysis/10/research-development-rorc.asp ("At the end of the day, the productivity of R&D [("Research and Development")] is what drives technology company profits, and ultimately their share prices."); Raul O. Chao et al., *Revenue Driven Resource Allocation: Funding Authority, Incentives, and New Product Development Portfolio Management*, 55 MGMT. SCI. 1451, 1558 (2009) (discussing how improving products and developing new products sustains or enhances revenue).

191. For example, in its 2013 Annual Report, Apple Inc. stated,

> [t]he Company continues to believe that focused investments in R&D are critical to its future growth and competitive position in the marketplace and are directly related to timely development of new and enhanced products that are central to the Company's core business strategy. As such, the Company expects to make further investments in R&D to remain competitive.

APPLE INC., ANNUAL REPORT (FORM 10-K) 33 (Oct. 30, 2013), *available at* http://investor.apple.com/secfiling.cfm?filingID=1193125-13-416534&CIK=320193.

192. *See* discussion *supra* Part IV.B.

193. *See id.*

authentication in other personal media devices to increase.[194]

A. *Biometric Authentication Is Not a Foregone Conclusion*

At the outset, some may question the need to even consider the implications of biometric authentication on the Fifth Amendment due to the foregone conclusion doctrine. It could be argued that the foregone conclusion doctrine removes Fifth Amendment protection from text messages and emails because the government knows that text messages and emails exist on a phone.[195] Arguably, under *Fisher*, production of the data theoretically might not constitute incriminating testimony because most people are aware that data is located on a smartphone, so a person admitting to having that data would not add anything to the government's case.[196]

In *Fisher*, however, even though the documents might have contained incriminating writing, the government was not compelling the accused himself to produce incriminating testimony because producing the accountant's documents in compliance with the subpoena "would express nothing more than the taxpayer's belief that the papers are those described in the subpoena."[197] Alternatively, in the case of biometric authentication, the question would be whether or not the government compelled the accused himself to produce incriminating testimony via the authentication.

Additionally, *Hubbell* later made clear that the foregone conclusion doctrine did not apply to overbroad foregone conclusions like "business documents."[198] One could argue that "text messages and emails" possessed by all smartphone users are akin to "business documents" possessed by a businessman.[199] If this argument were successful, text messages and emails would not be considered a "foregone conclusion," unless the government could show that it had specific knowledge of the contents of certain text messages, emails, or documents located on the

194. *See* Hoffman, *supra* note 17 ("Given Apple's industry-leading position, it's probably not a far stretch to expect this kind of authentication to take off."); *see also* King, *supra* note 9 (Biometrics Research Group, Inc., "predicts that Apple will initially lead in the deployment of such devices, due to the fact that the firm is the first consumer electronics provider to introduce biometric technology to the global smartphone mass market.").

195. *See* discussion *supra* Part II.B (discussing the foregone conclusion doctrine).

196. *See* Fisher v. United States, 425 U.S. 391, 411, 414 (1976).

197. *Id.* at 412–13.

198. *See* United States v. Hubbell, 530 U.S. 27, 45 (2000) ("The Government cannot cure [its lack of prior knowledge of the existence or whereabouts of the documents] through the overbroad argument that a businessman such as respondent will always possess general business and tax records that fall within the broad categories described in this subpoena.").

199. *See* Riley v. California, No. 13-132, slip op. at 18 (U.S. June 25, 2014) ("Even the most basic phones . . . might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on.").

device in question.[200] Professor Gershowitz suggests that, based on *Hubbell*'s specificity requirement, the foregone conclusion argument "should fail in the vast majority of cases, because without knowing the specific contents of the phone, police are not in a position to say before the search what evidence will be found once the arrestee enters his password."[201]

However, because there continues to be relatively little guidance as to how specific the government's independent knowledge must be for the evidence to be a "foregone conclusion," we cannot confidently say that the contents of a phone are protected from the foregone conclusion doctrine's limiting effect on the privilege against self-incrimination.[202] Moreover, the government's ability to lawfully intercept electronic communications further complicates this issue.[203] iPhone users sending secure text messages via the iMessage platform may be protected from the government's ability to gain independent knowledge of incriminating evidence based on iMessage's "end-to-end encryption."[204] However, an iPhone user sending a text message to a non-iPhone user, as well as text messages between non-iPhone users, would likely be more susceptible to the government's ability to intercept those messages and gain independent knowledge of the incriminating evidence.[205]

Consequently, the foregone conclusion doctrine does not dismiss the need to consider the implications of biometric authentication on the privilege against self-incrimination. If the data located on a personal

200. *See Hubbell*, 530 U.S. at 44–45. Thus, while one could argue that possession and ownership of the phone and the phone numbers linked to potentially incriminating phone calls, text messages, emails, and photos, could be independently verified by phone bills, the actual information contained within the phone would probably not be a foregone conclusion without specific knowledge of their contents.

201. Gershowitz, *supra* note 95, at 1173. "In light of the specificity required by *Hubbell*, prosecutors will likely be unsuccessful in making vague assertions that the contents of text messages on a cell phone are a foregone conclusion." *Id.*

202. *See* Kaufman, *supra* note 17, at 37 ("The standard by which a foregone conclusion is analyzed is not settled, and the Supreme Court has provided little guidance."); *see also* discussion *supra* Part II.B.

203. *See supra* note 117 (discussing the Omnibus Crime Control and Safe Streets Act).

204. *See* Whittaker *iMessage*, *supra* note 116 (discussing how the iMessage platform makes it impossible for the government to intercept messages between users).

205. *See* Andy Greenberg, *Ten Million More Android Users' Text Messages Will Soon Be Encrypted by Default*, FORBES (Dec. 9, 2013, 4:16 PM), http://www.forbes.com/sites/andygreenberg/2013/12/09/ten-million-more-android-users-text-messages-will-soon-be-encrypted-by-default/ (explaining how Android users that have replaced the Android operating system with the CyanogenMod operating system will have TextSecure as the phone's default text messaging platform, and discussing how TextSecure's end-to-end encryption prevents text messages from being intercepted); *see also supra* notes 113–14 and accompanying text; *cf.* Dan Goodin, *Think Your Skype Messages Get End-to-End Encryption? Think Again*, ARS TECHNICA (May 20, 2013, 12:17 PM), http://arstechnica.com/security/2013/05/think-your-skype-messages-get-end-to-end-encryption-think-again/ (discussing how Skype messages can be intercepted).

device was not a "foregone conclusion," and law enforcement needed the accused to authenticate the device, one could argue that the authentication would provide the government with a " 'lead to incriminating evidence,' or 'a link in the chain of evidence needed to prosecute.' "[206] The analysis would then turn to whether the act of production—biometric authentication—would be considered "testimonial in nature," such that it required the accused to use the contents of his mind, or if it was merely an analysis of physical traits.[207]

B. *Biometric Authentication: An Analysis of Physical Traits*

1. Compelled Biometric Authentication Is Not Self-Incriminating

Although the science behind biometric authentication itself may be extremely technical and complex, an initial consideration of its impact on the Fifth Amendment suggests a much simpler legal analysis. While the privilege against self-incrimination bars compelling communications or testimony, compulsion that makes the suspect the source of physical evidence does not.[208] Given that biometric authentication is merely a scan of physical traits that are compared to previously stored information,[209] one can argue that compelled biometric authentication is not barred by the self-incrimination privilege. Indeed, the Supreme Court has repeatedly held that compelling an accused to demonstrate physical characteristics for identification purposes does not qualify as compelled self-incrimination because it is not testimonial in nature.[210] Likewise, if an accused was compelled to place his finger on his laptop's fingerprint reader, or have his face scanned with his phone's facial recognition software, the physical characteristics would have been used for identification purposes and would likely not be considered "testimonial in nature" such that the scan would violate the self-incrimination privilege.[211]

206. United States v. Hubbell, 530 U.S. 27, 42 (2000).

207. *Cf. id.* at 41–42 (the accused's act of production required him to use the contents of his mind in locating 13,120 pages of materials, akin to answering interrogatories).

208. *See* Schmerber v. California, 384 U.S. 757, 761 (1966).

209. *See* Ng, *supra* note 14, at 428; *see also* discussion *supra* Part IV.A.

210. *See* Gilbert v. California, 388 U.S. 263, 266–67 (1967); United States v. Wade, 388 U.S. 218, 222 (1967); *Schmerber*, 384 U.S. at 761; Holt v. United States, 218 U.S. 245, 252–53 (1910); *see also In re* Grand Jury Subpoena, 176 F. App'x 72, 74 (11th Cir. 2006), *cert. denied*, 549 U.S. 818 (2006) ("the Supreme Court has held that a handwriting exemplar is an identifying physical characteristic that falls outside the protection of the Fifth Amendment").

211. *See* Kaufman, *supra* note 17, at 40 (suggesting that compelling a person to place a finger on a fingerprint reader is not a "testimonial act within the meaning of the privilege"); Hoffman, *supra* note 17 (noting that because biometrics are not something people remember, it is less likely that the self-incrimination privilege would apply). *But see* Susan W. Brenner, *Intellectual*

Moreover, biometric authentication does not reveal the contents of the accused's mind. Unlike instances where defendants are compelled to reveal their passwords that they committed to memory, biometric authentication does not reveal anything committed to memory.[212] Compelling the accused to stand still for an iris scan or to place his fingerprint on a fingerprint reader does not convey where he was last night, whether he committed a crime, or if he has any information regarding an investigation. In short, it reveals nothing other than whether he is or is not the person whose physical traits are associated with the device in question.[213] While it may be argued that biometric authentication is analogous to an accused saying, "this smartphone is mine," and thus impliedly asserting that any incriminating text messages, emails, or photos discovered within the device were his, this argument would likely fail.[214] Because biometric authentication is an analysis of physical traits, the Supreme Court would likely treat it just like other compelled exhibitions of physical characteristics used for identification purposes. Thus, just like fingerprint analyses, handwriting exemplars, voice exemplars, and blood analyses, which do not violate the privilege against self-incrimination,[215] using fingerprint recognition, iris scanning, facial recognition, voice recognition, and DNA analysis as a means of identification also would not implicate the privilege against compelled self-incrimination. Surely, just like discovering incriminating evidence after

Property Law Symposium: Encryption, Smart Phones, and the Fifth Amendment, 33 WHITTIER L. REV. 525, 538 (2012) (suggesting that the Supreme Court could rule either way). Additionally, while compelling an accused to place his finger on his phone's fingerprint reader or have his face scanned with his phone's facial recognition software might only be used for identification purposes, it could constitute an impermissible seizure under the Fourth Amendment if police were only detaining the suspect, did not have an arrest warrant, and lacked probable cause to arrest. *See* Hayes v. Florida, 470 U.S. 811, 814–15 (1985) (fingerprinting the detained suspect at the police station without an arrest warrant or probable cause to arrest was an impermissible seizure under the Fourth Amendment); Davis v. Mississippi, 394 U.S. 721, 727–28 (1969) (petitioner's Fourth Amendment rights were violated when he was detained, fingerprinted, and interrogated without an arrest warrant or probable cause to arrest).

212. *See* Kaufman, *supra* note 17, at 41 ("It would be a stretch for defendants or witnesses to argue that such acts compel one to produce the contents of the mind.").

213. *See supra* notes 140–45 and accompanying text.

214. The United States Court of Appeals for the District of Columbia considered this analogy in *United States v. Hubbell*, 167 F.3d 552, 573–74 (D.C. Cir. 1999), *aff'd*, 530 U.S. 27 (2000). The majority explained that when a suspect is compelled to submit to fingerprint analysis, while the suspect "can be said to be communicating that this is my hand and it contains five fingerprints unique to my person . . . the individual has merely been compelled to make himself available as a source of real or physical evidence." *Id.* at 574 (quoting *Schmerber*, 384 U.S. at 764) (internal quotation marks omitted).

215. *See Gilbert*, 388 U.S. at 266–67 (handwriting exemplar does not violate the privilege); *Wade*, 388 U.S. at 222–23 (voice exemplar does not violate the privilege); *Schmerber*, 384 U.S. at 761 (taking a blood sample was not compelled testimony in violation of the privilege, nor would compulsion to submit to fingerprinting be a violation).

an arrestee provides a password or permission to search a device, police may discover incriminating evidence after an arrestee unlocks a device via biometric authentication.[216]

Consider the hypothetical posed at the outset of this article. Whether the government compels the accused to unlock his phone via subpoena, the suspect voluntarily provides the passcode after police obtain a warrant, or the suspect consents to the search during interrogation and provides the passcode, the government could obtain text messages and emails relating to illegal activity that the user sent. Thus, like *Hubbell*, where producing the subpoenaed documents was not itself incriminating but might lead to incriminating evidence,[217] the act of biometric authentication itself might not be incriminating, but it may provide the link necessary to obtain the incriminating evidence inside the phone.[218] Nevertheless, under *Hubbell*, if the government could show that the information contained within the phone was a "foregone conclusion," the fact that biometric authentication provided that link to the evidence would be irrelevant.[219]

Interestingly, yet problematically, biometric authentication might even resolve the difficulties law enforcement has traditionally encountered in accessing locked devices or encrypted data. While Professor Gershowitz suggests that "cell-phone users could password protect their phones and shift the legal issues into more complicated Fourth and Fifth Amendment territory,"[220] biometric authentication may render users with even fewer options in protecting their phones and other personal devices.[221] Ironically, the convenience and protection generally associated with biometric authentication may actually make a user's life more problematic by having less legal protection.

Recall the discussion of cell phone searches incident to arrest in Part II.C. Regardless of whether police obtained consent to search the

216. *Compare* People v. Rangel, 206 Cal. App. 4th 1310, 1313–14 (Cal. Ct. App. 2012) (where the suspect only gave the detective permission to search the phone to look up the suspect's girlfriend's number, but the detective also read the suspect's text messages and found incriminating evidence that was later used against the suspect), *with* United States v. Hubbell, 530 U.S. 27, 41–42 (2000) (where producing a breadth of subpoenaed documents was akin to answering interrogatories, which could lead to incriminating evidence that would later be used against the respondent).

217. *See Hubbell*, 530 U.S. at 42.

218. *See, e.g.*, Hoffman v. United States, 341 U.S. 479, 486 (1951) (explaining that the privilege against self-incrimination does not only apply to answers that would themselves alone support a conviction, but also applies to answers that provide the government with a link in the chain of evidence necessary to prosecute the accused).

219. *See Hubbell*, 530 U.S. at 43–45 (discussing how the foregone conclusion doctrine negates self-incrimination claims).

220. Gershowitz, *supra* note 95, at 1144.

221. *See* discussion *infra* Part V.B.1.

phone or obtained a warrant permitting the search, police would no longer need to then also procure the passcode by consent, nor would interrogation occur, under which *Miranda* would provide some form of protection.[222] Considering biometric authentication is merely a measure of physical characteristics, law enforcement would no longer need the accused to reveal the contents of his mind—in the form of the passcode—via consent.[223] As to voice recognition, if the suspect first declines to cooperate for authentication by refusing to speak for the recognition software, and police initiated questioning in an attempt to elicit a response that would hopefully authenticate the device, such questioning would arguably constitute interrogation and the suspect would be afforded *Miranda*'s protections.[224] However, in such a case, even if a *Miranda* violation occurred, any physical evidence obtained as a result likely would still be admissible at trial because the Supreme Court has declined to extend the fruit of the poisonous tree doctrine to the *Miranda* rule.[225] Additionally, because biometric authentication can be done almost instantaneously without saying anything,[226] it is difficult to imagine how most methods of biometric authentication would even constitute "interrogation" to require *Miranda*'s safeguards.

Consider, for example, a hypothetical in which police obtain a search warrant for the home of a person who is suspected of having been involved in an armed robbery, and the warrant also permits the officers to search the suspect's cell phone. After searching the suspect's home, the police determine that they have probable cause to arrest the suspect. Immediately after police handcuff the suspect and prior to giving the suspect his or her *Miranda* rights, police locate the suspect's smartphone on his or her person. The smartphone has facial recognition enabled and, without asking the suspect any questions, police scan the suspect's face with the phone, and the phone automatically unlocks. Pursuant to the search warrant, police look through the suspect's text messages and find a text message conversation between the suspect and an individual already in custody, who confessed to being involved, making plans to

222. *See supra* notes 96–97 and accompanying text.

223. *See* Kaufman, *supra* note 17, at 41 (suggesting that the government would argue that compelling a defendant to put his finger on a fingerprint reader is not "a testimonial act within the meaning of the privilege," and noting that, "[i]t would be a stretch for defendants . . . to argue that such acts compel one to produce the contents of the mind"). Nevertheless, although police might not need the suspect to consent and voluntarily provide the passcode, they would still need the suspect to physically cooperate to authenticate the device.

224. *See* Miranda v. Arizona, 384 U.S. 436, 444 (1966) (holding that the privilege against self-incrimination requires procedural safeguards prior to custodial interrogation).

225. *See supra* note 95 and accompanying text.

226. *See* Ng, supra note 14, at 431 (iris scanning is done in seconds); *Using Touch ID*, *supra* note 1 (Touch ID quickly reads fingerprints and automatically unlocks the phone).

meet one hour prior to the robbery on the night the robbery occurred. Upon seeing the police reading the text messages, the suspect also makes an incriminating statement, still having yet to receive his or her *Miranda* warnings. At trial, the defendant alleges a violation of the privilege against self-incrimination. However, the court would probably determine that custodial interrogation had not occurred because the police never initiated questioning prior to the incriminating statement.[227] Thus, not only would the incriminating text messages be admissible, the incriminating statement would be admissible as well.

Additionally, police would no longer have to procure a subpoena to compel the suspect to provide the passcode because biometric authentication would allow simple, immediate access through a mere physical trait analysis. Police and prosecutors would no longer need to "compel production" of passcodes or encrypted data therein to obtain the evidence they need to prosecute, and the ability to "invoke the Fifth" would disappear.

Similarly, police would never have to try to crack the passcode with biometric authentication.[228] Biometric authentication would essentially ensure that police could get into the smartphone upon a quick authentication via the suspect's physical trait. And, quite obviously, police would never have to give up on the cell phone search anymore because biometric authentication would provide access if the police wanted access.

Moreover, the government's ability to grant immunity for the act of producing a memorized passcode weakens a claim that biometric authentication implicates the Fifth Amendment. Under the act of production doctrine, self-incrimination may result merely from the act of producing evidence in response to a subpoena when the evidence has "a compelled testimonial aspect."[229] However, provided the government can show that the evidence used to obtain the indictment and offered at trial "was derived from legitimate sources 'wholly independent' of the testimonial aspect of [the accused's] immunized conduct," the accused can be compelled to produce a passcode after receiving a grant of immu-

227. *See Miranda*, 384 U.S. at 444 (defining custodial interrogation as "questioning initiated by law enforcement officers after a person has been taken into custody or otherwise deprived of his freedom of action in any significant way").

228. *See* Gershowitz, *supra* note 95, at 1164 (noting that cracking the passcode is one way for police to gain access to the data in an arrestee's cell phone).

229. *See* United States v. Hubbell, 530 U.S. 27, 36 (2000). The act of production doctrine "provides that persons compelled to turn over incriminating papers or other physical evidence pursuant to a subpoena *duces tecum* or a summons may invoke the Fifth Amendment privilege against self-incrimination as a bar to production only where the act of producing the evidence would contain 'testimonial' features." *Id.* at 49 (Thomas, J., concurring).

nity under 18 U.S.C. § 6003.[230] Thus, even if biometric authentication was determined to be an assertion of fact that became a link in the chain of evidence necessary for prosecution, much like granting immunity for the act of producing a memorized passcode, the government could grant immunity for the act of authentication if the evidence was a foregone conclusion.[231]

In short, although a passcode on a cell phone provides an additional layer of protection from unwanted governmental searches, biometric authentication seems to entirely remove this protection, which inadvertently affects Fifth Amendment rights. While some are quick to note that biometric authentication provides better protection from hackers than passcodes because biometrics are more unique than passcodes, they fail to consider the protection from unwanted governmental intrusion.[232]

2. The Slim Chance that the Self-Incrimination Privilege Will Apply

While the analysis regarding biometric authentication's impact on the Fifth Amendment seems relatively simple, there are two specific factors that complicate the issue. First, in many personal media devices, although biometric authentication minimizes the times the user needs to enter the passcode, the passcode is nonetheless still running in the background. For example, with the iPhone 5s, biometric authentication cannot be set up without first creating a passcode.[233] Therefore, while the actual authentication occurs via mere physical traits, authentication is still linked to the passcode. It would not be surprising to hear the argument that, because the authentication is linked to a passcode, a fingerprint scan is akin to the defendant entering that passcode to unlock the

230. *See id.* at 38–46 (explaining the constitutionality of an order to compel production under 18 U.S.C. § 6002 after receiving a grant of immunity under § 6003). 18 U.S.C. § 6002 provides,

> [w]henever a witness refuses, on the basis of his privilege against self-incrimination, to testify or provide other information in a proceeding . . . 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.

231. *See* Brenner, *supra* note 211, at 537 (discussing how the ability to grant immunity for the act of producing a passcode can overcome an invocation of the Fifth Amendment).

232. *See* Pagliery, *supra* note 158. *But see* Charlie Osborne, *Apple iPhone Fingerprint Scanner Raises Security Worries*, ZDNet (Sept. 17, 2013), http://www.zdnet.com/apple-iphone-fingerprint-scanner-raises-security-worries-7000020767/ (if hackers are able to gain access, they gain access to permanent data that cannot be changed like a passcode).

233. *See supra* note 180 (discussing how to set up Touch ID).

phone. While the accused was technically compelled to exhibit a physical characteristic, the accused was arguably compelled to indirectly disclose knowledge of the passcode because the fingerprint is connected to the passcode. Thus, unlike the cases where the Supreme Court has held that compelling the suspect to be the source of physical evidence did not violate the self-incrimination privilege,[234] a court may consider biometric authentication differently. In those cases, the physical evidence was not linked to any knowledge. The blood analysis in *Schmerber*,[235] the blouse modeling in *Holt*,[236] the speech in *Wade*,[237] and the handwriting exemplar in *Gilbert*,[238] all occurred without the defendant creating a passcode committed to his and only his memory. Alternatively, an iris scan or a fingerprint scan on a smartphone or laptop cannot occur without the defendant creating a passcode committed to his and only his memory. Further, in the aforementioned cases, the Supreme Court did not base its decisions on whether the incriminating information was a "foregone conclusion."[239]

Additionally, unlike the consent directive in *Doe* that did not communicate any implicit or explicit factual assertions to constitute a testimonial communication,[240] biometric authentication may communicate an implicit factual assertion that the accused owns the smartphone or laptop and the data therein.[241] Should law enforcement then find incriminating evidence within the smartphone or laptop, one could contend that its submission at trial would violate the Fifth Amendment because the purpose of authenticating the device was to obtain testimony from someone to prove that there was incriminating evidence—meeting the testimonial prong—and to communicate to the court that the defendant was linked to the evidence—meeting the communicative prong.[242] However,

234. *See* discussion *supra* Part II.A.

235. 384 U.S. 757 (1966).

236. 218 U.S. 245 (1910).

237. 388 U.S. 218 (1967).

238. 388 U.S. 263 (1967).

239. *See* United States v. Hubbell, 167 F.3d 552, 598 (D.C. Cir. 1999) (Williams, J., dissenting) (noting how *Schmerber*, 384 U.S. 757, *Holt*, 218 U.S. 245, *Wade*, 388 U.S. 218, and *Gilbert*, 388 U.S. 263, "do not rely on anything like the 'foregone conclusion' rationale; instead, they find that such facts are not testimonial because they fit into the category of compulsion which makes a suspect or accused the source of real or physical evidence"), *aff'd*, 530 U.S. 27 (2000).

240. 487 U.S. 201, 215 (1988).

241. *Contra id.* at 218 (the only factual assertion that would be made if the banks produced records in response to consent forms the petitioner signed would be the bank's implicit assertion that it believes the accounts to be the petitioner's).

242. *See Schmerber*, 384 U.S. at 774 (Black, J., dissenting) (explaining how extracting blood from the petitioner to determine if he was drunk had both a testimonial and a communicative aspect even though it was merely an analysis of physical evidence). Justice Black opined that the majority used a "very restrictive reading of the Fifth Amendment's privilege against self-incrimination [particularly] on the words 'testimonial' and 'communicative.'" *Id.* Justice Black

this argument still faces an uphill battle. While the compelled act (authentication) may implicitly assert that the smartphone is the accused's by unlocking the phone or laptop—just like it would by entering the correct passcode retrieved from memory—the compelled act (authentication) makes the accused the source of physical evidence instead of making the accused reveal the contents of his mind.[243] Although the user is asserting the fact, "this is mine," by being the source of physical evidence, this argument has explicitly been rejected.[244]

Second, some biometric authentication methods might actually be able to reveal the contents of one's mind. For example, consider speech recognition. People are generally conscious of whether they speak slowly or quickly, at what tone, and how they pronounce certain words.[245] Dissenting Judge Williams set forth a similar position in *Hubbell*, stating:

> [I]n giving a voice sample, one also admits that one's voice has various characteristic idiosyncrasies—a non-obvious and incriminating fact that the law allows the prosecutor to secure by compulsion. . . . One can, of course, discern a communicative element in the

pointed out the Court's "rather labored explication" of these words, suggesting that "[t]hese words are not models of clarity and precision," and noted the Court's inability to "find precedent in the former opinions of this Court for using these particular words to limit the scope of the Fifth Amendment's protection." *Id.* With the problems that biometric authentication may create regarding the Fifth Amendment that will be discussed in Part V.C, the Supreme Court could end up reconsidering Justice Black's viewpoint.

243. *See id.* at 764 ("[T]he privilege is a bar against compelling 'communications' or 'testimony,' but . . . compulsion which makes a suspect or accused the source of 'real or physical evidence' does not violate it."). *Compare id.* at 764–65 (a blood test was not a violation of the privilege because it only made the accused the source of physical evidence), *with In re* Grand Jury Subpoena Duces Tecum, 670 F.3d 1335, 1346 (11th Cir. 2012) (decrypting and producing hard drive contents would violate the privilege because it would require a memorized decryption password).

244. See *Hubbell*, 167 F.3d at 573–74, where the United States Court of Appeals for the District of Colombia acknowledged and dismissed this argument:

> While it can be argued that the accused implicitly testified . . . that this is my blood containing my unique DNA, that this is my face with all of its characteristic idiosyncra[s]ies, that this is my body with a particular shape and size which fits into this blouse—that testimony was irrelevant to the Fifth Amendment inquiry because it required no act of will on his part as to what he would communicate. The same reasoning applies to a compelled submission to fingerprint analysis. The suspect can be said to be communicating that this is my hand and it contains five fingerprints unique to my person, but in reality the individual has merely been compelled to make himself available as a "source of 'real or physical evidence.'" . . . For purposes of Fifth Amendment analysis, it is dispositive that the government has no need to rely upon the witness's truthtelling to secure the evidence it seeks.

245. *See generally* TOASTMASTERS INT'L, YOUR SPEAKING VOICE (2011), *available at* http://www.toastmasters.org/199-YourSpeakingVoice (discussing how to change the way one speaks with pitch, rate, and volume alterations).

> giving of a voice sample: a person commanded to speak implicitly says, "This is the way I sound when I speak."[246]

If an accused had a phone that used voice recognition for authentication, it would analyze these factors to identify the user.[247] Thus, the accused could easily change the rate, tone, pitch, and pronunciation while attempting to authenticate the device to consciously prevent authentication.[248] Alternatively, consciously speaking in the same manner in which one normally does might be analogous to revealing the contents of one's mind.[249] It would then follow that compelling voice recognition would be analogous to compelling a suspect to reveal something testimonial in nature, which some courts have held to violate the privilege against self-incrimination.[250] However, *Wade* suggests that this argument would probably fail.[251] One could assume that the accused in *Wade* was also conscious of his speech pattern when being compelled to speak for identification, and since the Supreme Court still considered his speech not "testimonial in nature," a court would probably also consider speech for voice recognition not "testimonial in nature."

Additionally, the *Chavez* decision poses yet another hurdle for biometric authentication to overcome before it could be considered a violation of the self-incrimination privilege.[252] Post-*Chavez*, some scholars have suggested that it is difficult for a defendant to demonstrate that requests for passwords by police even have a compulsion element because police "lack legal authority to compel the individual to say anything."[253] The argument would follow that because biometric authentication provides easy access to a phone or laptop without police having to "compel" the suspect to provide the password, the compulsion element

246. 167 F.3d at 598 (Williams, J., dissenting).

247. *See* NSTCS SPEAKER RECOGNITION, *supra* note 168.

248. *See generally* Donald B. Fiedler, *Acting Effectively in Court: Using Dramatic Techniques*, 25 CHAMPION 18, 20–22 (2001) (discussing how attorneys can change the way they speak in the courtroom); TOASTMASTERS INT'L, *supra* note 245 (suggesting how one can change the way he or she speaks).

249. *Cf.* Schmerber v. California, 384 U.S. 757, 764 (1966) (a test that measures changes in body functioning could be testimonial in nature).

250. *See In re* Grand Jury Subpoena Duces Tecum, 670 F.3d 1335, 1346 (11th Cir. 2012) (decryption would require the appellant to use the contents of his mind); United States v. Kirschner, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) (the defendant would have to use his mental processes to reveal his password).

251. 388 U.S. 218, 222–23 (1967) (compelled speech is not testimonial in nature if the speech was to be used solely as an identifying characteristic and not to admit guilt).

252. *See* 538 U.S. 760, 766–67 (2003) (rejecting the assertion that the phrase "criminal case" in the self-incrimination clause includes police interrogations without the initiation of legal proceedings).

253. Gershowitz, *supra* note 95, at 1168. *But see* Miranda v. Arizona, 384 U.S. 436, 461 (1966) (noting that compulsion to speak during police questioning may be greater than in courts where there are impartial observers).

in password requests would disappear.[254] Then, because authentication would occur without having to compel production of the password via a subpoena, one could contend that biometric authentication could not implicate the privilege because the compulsion aspect would never be present. However, this argument ignores the fact that in *Chavez* the government never filed criminal charges.[255] In a case where an accused had criminal charges filed against him, the accused could at least try to argue that biometric authentication during interrogation violated the Fifth Amendment.[256]

Further, a consideration of the self-incrimination clause's history indicates that the privilege is not merely a "trial right."[257] First, the clause is in the wrong amendment to only be considered a post-indictment trial right.[258] Second, historical cases considered confessions and statements made to police while in custody prior to trial.[259] And, third, the Supreme Court has explicitly stated that "all the principles embodied in the privilege apply to informal compulsion exerted by law-enforcement officers during in-custody questioning."[260] Therefore, while the characterization of the self-incrimination privilege as a "trial right" poses yet another hurdle to jump in order to successfully advance a claim that biometric authentication implicates the privilege, the possibility does remain open.

In sum, while one could argue that biometric authentication is "testimonial in nature" and may implicate the privilege against self-incrimination, the arguments are a stretch. Although passcode case law remains somewhat unclear, biometric authentication appears to pose a simpler analysis, suggesting that a user joining the "Biometric Revolution" has less ability to "invoke the Fifth" than a traditional passcode user.

C. *Eroding the Fifth Amendment*

Biometric authentication is exciting, more convenient, and arguably

254. *See* discussion *supra* Part II.C (discussing how police have to get the suspect to voluntarily provide the passcode or subpoena the passcode if the suspect does not voluntarily provide it).

255. 538 U.S. at 764.

256. *See id.* at 766 ("[A] 'criminal case' at the very least requires the initiation of legal proceedings."). Indeed, the Supreme Court stated, "[t]he text of the Self-Incrimination Clause simply cannot support the . . . view that the mere use of compulsive questioning, without more, violates the Constitution." *Id.* at 767.

257. *See* Davies, *supra* note 5, at 1018 (characterizing the claim that the privilege against self-incrimination is a trial right, as "acontextual, ahistorical, and essentially arbitrary").

258. *See supra* notes 23–29 and accompanying text (discussing how post-indictment procedural rights are contained within the Sixth Amendment).

259. *See* Miranda v. Arizona, 384 U.S. 436 (1966); Bram v. United States, 168 U.S. 532 (1897).

260. *Miranda*, 384 U.S. at 461.

safer than the traditional passcode authentication that most people are probably familiar with. However, biometric authentication may limit the opportunities in which an individual may invoke the privilege against self-incrimination. While the National Science and Technology Subcommittee on Biometric and Identity Management noted the importance of using the technology "to support national needs while being considerate of the public's social and privacy concerns,"[261] few seem to have considered its legal implications. Unfortunately, biometric authentication may erode the constitutional protection that traditional passcodes have provided and also create concerns for future technologies.

First, biometric authentication ultimately creates two general categories of laptop, tablet, and cell phone users: those who are protected and those who are not. Users who retain an older device or decide to forgo biometric authentication retain the ability to refuse to provide a passcode based on the privilege against self-incrimination. Alternatively, those who purchase the latest smartphone or laptop and utilize biometric authentication no longer have this ability because biometric authentication likely does not implicate the privilege. As previously discussed, because biometric authentication removes the need to ever compel an arrestee to produce a passcode,[262] law enforcement will always have the ability to access devices once they obtain a search warrant. Upon finding incriminating evidence, a defendant would have little success in claiming that the government violated his or her privilege against self-incrimination. Meanwhile, traditional passcode users could argue that any incriminating evidence found as a result of compelled passcode production violates their privilege against self-incrimination. Logically, two groups of people emerge: those who reject biometric authentication and retain the ability to invoke the Fifth Amendment, and those who relinquish that ability by signing on the dotted line for the latest mobile consumer device and choosing to utilize biometric authentication.[263]

261. *See* NSTCS FACE RECOGNITION, *supra* note 159 (regarding the use of facial recognition technology at the 2001 Super Bowl).

262. *See* discussion *supra* Part V.B.1. *But cf.* Brief in Opposition to Petition for Writ of Certiorari to the United States Court of Appeals for the First Circuit at 12, Riley v. California, No. 13-132 (U.S. June 25, 2014) (where in *United States v. Wurie*, No. 13-212, which was consolidated in the *Riley v. California* decision, the respondent noted that "[t]he newest models [of cell phones] use biometrics and other methods to control access. Whether an individual could be required to provide access to officers who have seized his/her phone is yet another issue not yet raised or addressed in the decisions to date.").

263. Interestingly, in *Riley*, Justice Alito explained a similar problem regarding the Fourth Amendment that may arise from the Court's decision. *See* No. 13-132, slip op. at 4–5 (Alito, J., concurring in part and concurring in the judgment) (discussing how the Court's holding "favors information in digital form over information in hard-copy form"). Justice Alito posed a hypothetical in which two suspects are arrested, one with a hard-copy form of a cell phone bill on his person and one with a cell phone, and pointed out that, under the Court's holding prohibiting

Creating a distinction between the ability to compel individuals to disclose passwords in the form of fingerprints versus alphanumeric form erodes the basic premise that everyone is afforded Fifth Amendment protection—the distinction actually affords less protection to those who embrace the new technology.[264] Considering that the Fifth Amendment's fundamental purpose was to preserve "an adversary system of criminal justice,"[265] to imply that the government can skirt its burdens with those who accept technological advancements is patently unjust. Moreover, these two groups will likely exist longer than one may expect. While some may find themselves eager to embrace biometric authentication for the excitement, convenience, and purported security, the ability to imitate biometric factors because they are not secrets committed to memory may make others more reluctant.[266] Some security experts caution that the convenience of biometric authentication on smartphones and other personal devices "could become a hacking treasure trove, granting [hackers] access to permanent data which cannot be deleted or changed."[267] Because the physical elements cannot be changed like a traditional passcode, there is concern about putting such permanent data on a phone that can easily be stolen, lost, or hacked into.[268] Thus, while some view biometric authentication on personal devices as a reliable convenience, others may be wary of relying on biometrics, or may simply just abandon the technology if it proves to be too unreliable.[269] Consequently, this disparate protection will probably

warrantless cell phone searches incident to arrest, police could seize and examine the phone bill for incriminating evidence without a warrant but not the cell phone. *Id.* at 5. Thus, the suspect with the cell phone would have greater Fourth Amendment protection than the suspect with the hard-copy phone bill. *See id.* The fact that at least one Justice considered this idea of disparate protection but did not see a "workable alternative," supports the proposition that, as technology advances, Constitutional protection will vary from person to person. *See id.* (acknowledging that "the Court's approach leads to anomalies").

264. *See* Larkin, *supra* note 17, at 270 ("Compelling some defendants to surrender their 'passwords' in the form of a fingerprint, but allowing others to keep an alphanumeric password secret, creates an arbitrary distinction in a way that ignores the purpose of the Fifth Amendment's important protections."). This problem compounds when considering the vast amount of personal information modern cell phones hold. *See supra* note 92 and accompanying text (discussing how much information modern cell phones hold).

265. Garner v. United States, 424 U.S. 648, 655 (1976).

266. *See* Paul Rubens, *Biometric Authentication: How It Works*, eSECURITY PLANET (Aug. 17, 2012), http://www.esecurityplanet.com/trends/biometric-authentication-how-it-works.html. For example, a hacker could present a photograph to fool a facial recognition system or play a recording of a voice to a voice recognition system. *See id.*

267. Osborne, *supra* note 232 (quoting an interview by Der Spiegel with John Caspar, Hamburg Comm'r for Data Prot. & Freedom of Info.).

268. *See id.*

269. Biometric authentication's accuracy is measured "by two statistics: False Non Match Rate (FNMR) and False Match Rate (FMR)." Rubens, *supra* note 266. FNMR refers to "how often a biometric is not matched to the template when it should be," resulting in prohibited authentication

be an issue that will not quickly cure itself. In short, the disparate protection is a significant concern that will likely exist long enough to force courts or legislatures to address the issue.[270]

Second, the ability to encrypt data via biometric authentication means that users who do so probably have no Fifth Amendment protection regarding that data. If a person can be compelled to unlock a phone via biometric authentication because it does not reveal the contents of his mind, a person can be compelled to produce encrypted data because it also does not reveal the contents of his mind. Undoubtedly, the news that the National Security Agency ("NSA") has been collecting phone records generated much conversation regarding privacy concerns.[271] Now, in addition to the traditional hackers and identity thieves, people may worry about the government gaining access to their personal data. Some suggest that encrypting data on smartphones is one way to prevent this,[272] and, because biometric authentication allows the user to decrypt documents without having to remember a password, users may be more likely to adopt this method.

While it is unclear as to whether compelled production of a passcode or encrypted data violates the privilege against self-incrimination, at least a traditional passcode user has some hope that the government cannot compel production.[273] Biometric authentication removes that hope and creates unequal protection amongst encryption users. The current circuit-split on the issue of compelled production of a password or encrypted data suggests that where the information is a foregone conclusion, compelled production does not violate the Fifth Amendment.[274] Thus, in situations where the information is not a foregone conclusion, compelled production would violate the Fifth Amendment. Consequently, in cases where the information within a laptop or cell phone is not a foregone conclusion, a person using an older laptop or cell phone

by the correct person, while FMR refers to "how often a false biometric is matched (and authentication is allowed) when it shouldn't be," resulting in authentication by the wrong person. *Id.*

270. *See* Riley v. California, No. 13-132, slip op. at 6 (U.S. June 25, 2014) (Alito, J., concurring in part and concurring in the judgment) (explaining how modern cell phones "implicate[ ] very sensitive privacy interests that this Court is poorly positioned to understand and evaluate," and that "[l]egislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future").

271. *See, e.g.*, Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN, June 5, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

272. *See* McDowell, *supra* note 110.

273. *See generally* Gershowitz, *supra* note 95 (discussing the benefits of password protecting cell phones); *see also supra* notes 95–104 and accompanying text.

274. *See* discussion *supra* Part III.B.

without biometric authentication capabilities could keep his information private, while the person with a brand new laptop or smartphone could be forced to reveal his information. Effectively, those who choose to lag behind and resist technological advances may be afforded stronger constitutional protection. Although this presents the same disparate protection concerns as previously discussed, biometric authentication will impact not only traditional every-day passcode issues, but also more complex encryption issues.

Third, the privilege to be free from self-incrimination will actually provide less protection, if any, to situations where biometric authentication provides the government with more reliable proof that the accused has knowledge, possession, and control over the incriminating evidence. As previously discussed, while compelled biometric authentication may assert that the device and the files contained within it are the accused's, the compelled act (authentication) merely makes the accused the source of physical evidence, and is therefore not compelled testimony like producing a passcode committed to memory.[275] If the government cannot show its independent knowledge of the accused's knowledge and control over the incriminating evidence—without compelled testimony—the evidence is not a "foregone conclusion," and the self-incrimination privilege applies; thus, the accused is protected from being compelled to be a witness against himself by revealing the contents of his mind.[276] If biometric authentication merely makes the accused the source of physical evidence and is not considered "compelled testimony," the self-incrimination privilege would not apply,[277] and the government would never have to show that the evidence is a "foregone conclusion."[278] Compelling an accused to reveal a passcode, however, could be considered "compelled testimony" because it forces the accused to reveal the contents of his mind; unless the government can show that the evidence is a "foregone conclusion," the self-incrimination privilege likely applies.[279] Problematically, though, compelling an accused to enter a memorized passcode may actually be less reliable proof that the person has knowledge of and control over any incriminating evidence found within that device because passcodes can easily be shared with others,

275. *See* discussion *supra* Part V.B.

276. *E.g.*, United States v. Hubbell, 530 U.S. 27, 43–45 (2000).

277. *See* Schmerber v. California, 384 U.S. 757, 765 (1966) (compelling the accused to be the source of physical evidence is not "compelled testimony" to violate the privilege).

278. *See Hubbell*, 530 U.S. at 43–45 (when the government relies on the accused to confirm the existence and authenticity of the evidence through compelled testimony, the evidence is not a "foregone conclusion," and the self-incrimination privilege applies).

279. *See id.*; *In re* Grand Jury Subpoena Duces Tecum, 670 F.3d 1335, 1345–46, 1349 (11th Cir. 2012).

whereas biometrics cannot.[280] For example, John could tell Jane the password to certain encrypted files located on a computer; if Jane were to then decrypt the particular data by producing the password, it would not necessarily prove that Jane had knowledge of or control over that data. On the other hand, John could not share his fingerprint or iris with Jane, so if John were to decrypt the data with his fingerprint or iris, it would almost certainly prove that John had knowledge of and control over that data. If the government could not show that the incriminating evidence was a "foregone conclusion," the privilege would provide protection in the password situation, where it would actually be less reliable that the person had knowledge of and control over the incriminating evidence.[281]

Alternatively, with biometric authentication, where one can practically be certain that the authenticator has knowledge of and control over the data therein because the authenticating factor cannot be shared, duplicated, or hacked,[282] the privilege would not afford any protection because the accused would merely be the source of physical evidence.[283] Consequently, the self-incrimination privilege would afford more protection when it is less certain that the compelled individual has knowledge of and control over the incriminating evidence. If the self-incrimination privilege protects an accused from being compelled to be a witness against himself by producing incriminating testimony,[284] it is troubling that an accused may actually have less constitutional protection where the compelled act of production more reliably confirms that the person has knowledge of and control over the incriminating evidence.

Fourth, the conclusion that biometric authentication does not implicate the privilege to be free from self-incrimination poses serious concerns for future technologies. Assuming this conclusion is correct, what will happen if and when innovation creates a device that can read a

280. *See* Rubens, *supra* note 266 ("The main benefit of using a biometric authentication factor instead of a physical token is that biometrics can't easily be lost, stolen, hacked, duplicated, or shared. They are also resistant to social engineering attacks . . . ."). Thus, it may be less reliable to assume a person owns data after he enters a passcode than it would be if the person uses biometrics to unlock the data. Even the Supreme Court has noted the value of DNA analysis regarding identification. *See* Maryland v. King, 133 S. Ct. 1958, 1971 (2013) ("An individual's identity is more than just his name or Social Security number, and the government's interest in identification goes beyond ensuring that the proper name is typed on the indictment.").

281. *See supra* notes 277–78 and accompanying text.

282. *See* Rubens, *supra* note 266 (discussing the benefits of biometric authentication compared to passwords).

283. *See* Schmerber v. California, 384 U.S. 757, 764–65 (1966) (the privilege does not afford protection to situations where the accused is merely compelled to be the source of physical evidence).

284. U.S. CONST. amend. V; Fisher v. United States, 425 U.S. 391, 408 (1976).

person's mind?[285] By analogy, if the device were to scan brain activity, would this be analogous to the individual revealing the contents of his mind, thereby implicating the self-incrimination privilege?[286] Or would this merely be akin to a display of physical characteristics, therefore not implicating the self-incrimination privilege?[287] Based on the previously discussed precedent, it seems likely that the Supreme Court would simply consider this an analysis of physical characteristics.[288] If so, then the Fifth Amendment privilege to be free from self-incrimination would essentially disappear because the government would never have to compel any knowledge or testimony. Nonetheless, it is clear that this technology has the ability to impact our constitutional rights.

So, what should users do? Should users take a chance and jump into the "Biometric Revolution"? Or should they lag behind, resisting technological change, while becoming more and more wary of what the government might lawfully be able to do? Some have suggested that due to the murky interplay of biometric authentication and the privilege to be free from self-incrimination, it may be better to continue relying on numeric passcodes until the law becomes clearer.[289] However, this may be impracticable, or even impossible, as the demand to stay current with the ever-changing technology remains a strong societal force. Because there is no easy answer, arguably the best option is to use both biomet-

285. *See* Alan S. Cowen et al., *Neural Portraits of Perception: Reconstructing Face Images from Evoked Brain Activity*, 94 NEUROIMAGE 12, 12–13 (2014) (reporting how recent neuroimaging advances have allowed researchers to reconstruct face images from brain activity); *see also* Karen Weintraub, *Scientists Explore Possibilities of Mind Reading*, USA TODAY (Apr. 22, 2014, 9:26 AM), http://www.usatoday.com/story/tech/2014/04/22/mind-reading-brain-scans/7747831/ (discussing how some researchers believe thoughts may be readable someday).

286. *See* United States v. Hubbell, 530 U.S. 27, 43 (2000) (The privilege applied because the respondent was compelled to "make extensive use of 'the contents of his own mind' in identifying the hundreds of documents responsive to the request in the subpoena. . . . The assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox.").

287. *See Schmerber*, 384 U.S. at 764–65 ("compulsion which makes a suspect or accused the source of 'real or physical evidence' does not violate" the privilege).

288. *See* cases cited *supra* note 8. However, in *Schmerber*, the Supreme Court noted,

> [s]ome tests seemingly directed to obtain "physical evidence," for example, lie detector tests measuring changes in body function during interrogation, may actually be directed to eliciting responses which are essentially testimonial. To compel a person to submit to testing in which an effort will be made to determine his guilt or innocence on the basis of physiological responses, whether willed or not, is to evoke the spirit and history of the Fifth Amendment. Such situations call to mind the principle that the protection of the privilege "is as broad as the mischief against which it seeks to guard."

384 U.S. at 764 (quoting Counselman v. Hitchcock, 142 U.S. 547, 562 (1892)).

289. *See* Kaufman, *supra* note 17, at 41 ("[I]t may be safer to rely, at least in part, on memorized encryption keys unless and until more favorable law or technology evolves.").

rics and a passcode on personal devices if possible.[290] That way, the user not only has legal protection with the passcode, but also security protection with the biometrics. But how feasible is this? Not very, considering one major advantage of biometric authentication is that it avoids having to remember yet another passcode. Further, most biometric authentication technologies only offer the biometric method up front; it is not until the biometric method fails that in some devices the passcode method then becomes available.[291] Should the biometrics match in the first place, the device would be unlocked and the user would not even have the option to enter the passcode. While ideal in theory, using both biometrics and a passcode is likely an unrealistic option.

One option is fairly obvious, yet complex: legislative action. For example, lobbying the Federal Communications Committee ("FCC"), or the United States Department of Commerce, may be successful in creating laws requiring smartphone manufacturers and operating system developers to at least provide the option to utilize both biometrics and passcodes before a device can be "unlocked."[292] That way, users can choose to authenticate with both methods, one or the other, or none at all. Unfortunately, because of the benefits biometric authentication provides, it is unlikely that manufacturers would provide this without some kind of regulation.[293]

A second, more obvious, and more immediate option is relatively simple: users will have to choose what they value more—convenient authentication and better hacker protection, or traditional memorization and more assured legal protection. Unfortunately, due to the lack of any specific biometric authentication precedent and the lack of specific precedent from the Supreme Court on compelled production of encrypted data, this might be the only option a user has. Ultimately, it appears to come down to a "value and risk" balancing game: what does a user value more and how big of a risk-taker is that user?

290. *See* Hoffman, *supra* note 17 ("Here's an easy fix: give users the option to unlock their phones with a fingerprint plus something the user knows."); Rubens, *supra* note 266 ("A better method is to adopt a two-factor authentication system.").

291. *See, e.g.*, *supra* note 180 (discussing Touch ID).

292. The FCC is the United States governmental agency responsible for federal communications law and regulation. *See What We Do*, FED. COMM. COMMISSION, http://www.fcc.gov/what-we-do (last visited Aug. 9, 2014). Another option is the National Institute of Standards and Technology, which is the U.S. Department of Commerce agency that provides research services on standards, technical regulations, and conformity assessment procedures for non-agricultural products. *See National Center for Standards and Certification Information*, NIST, http://www.nist.gov/director/sco/ncsci/index.cfm (last updated May 15, 2014).

293. *See generally* Pagliery, *supra* note 158 (discussing how fingerprint scanning is safer than typing in a password and more convenient because the user no longer has to memorize numerous username and password combinations).

VI. CONCLUSION

The current state of the Fifth Amendment privilege to be free from self-incrimination is unclear enough as it is. On one hand, precedent suggests that biometric authentication would not implicate the privilege to be free from self-incrimination because it is an analysis of physical characteristics. On the other hand, the circuit split regarding compelled disclosure of passwords and production of encrypted data complicates the issue, especially if consumers begin encrypting data on their smartphones and laptops via biometrics and as technology improves and reveals more about the user than pure physical characteristics. Undoubtedly, the state of the Fifth Amendment privilege to be free from self-incrimination will only get cloudier with the "Biometric Revolution." While biometric authentication provides users with stronger hacker and identity theft protection,[294] it likely removes constitutional protection.[295]

To continue technological progress, improve security, and make authentication and identification more convenient for the user, biometric authentication certainly must be embraced. Nonetheless, it is important to keep in mind how technological advancements may impact constitutional rights and to do everything possible to uphold those rights. While many users may opt to take the legal risk and jump into the "Biometric Revolution," it should be their choice to potentially relinquish their constitutional right by doing so. Ultimately, the ability to utilize both biometrics and memorized passcodes to access personal devices is arguably the best option.[296] In the age of increased security concerns combined with the lust for the latest technological invention, this option would provide users with the heightened security they desire, the latest-and-greatest technology, and a protected Fifth Amendment privilege.

Now reconsider the hypothetical posed at the outset. Would compelled authentication via a fingerprint reader on a suspect's smartphone violate the suspect's Fifth Amendment privilege to be free from self-incrimination? Likely not. In that case, the suspect would undoubtedly wish he or she was a member of the group that rejected biometric authentication and, instead, continued to shoulder the burden of memorizing a passcode. But what will happen when that group no longer has

294. *See id.* (discussing how fingerprint scanning provides better protection against hackers); Whittaker *iPhone*, *supra* note 186 (explaining how fingerprint scanning helps prevent identity theft).

295. In considering DNA in regards to searches, while ultimately determining a DNA analysis was a reasonable search under the Fourth Amendment, the Supreme Court noted, "science can always progress further, and those progressions may have Fourth Amendment consequences . . . ." Maryland v. King, 133 S. Ct. 1958, 1979 (2013). Indeed, biometric authentication may be a good example of science's progressions having Fifth Amendment consequences.

296. *See supra* note 290.

the option to carry this burden? Precedent indicates that people will simply have less constitutional protection in testimonial evidence that may be contained in their mobile consumer devices. Until then, the two groups—those who embrace the "Biometric Revolution" and those who do not—will have disparate constitutional protection. Either way, biometric authentication poses significant Fifth Amendment concerns.