University of Florida Journal of Law & Public Policy

Volume 31 | Issue 2 Article 5

2021

Place Your Finger on the Home Button: The Legality of Compelling Biometrics

Casey Coffey

PLACE YOUR FINGER ON THE HOME BUTTON: THE LEGALITY OF COMPELLING BIOMETRICS

Casey Coffey[*]

INTRODUCTION

Imagine you are presented with a search warrant. The warrant authorizes law enforcement officials to search your home and seize various items, including electronic devices. The search is conducted and among the seized items is an iPhone. Instead of confiscating the phone and ending the search, the officers direct you to place your thumb on the Touch ID sensor or Home button. You hesitate, questioning whether this is legal.

---

* Casey Coffey graduated University of Florida Levin College of Law in 2020. She was a member of the Journal of Law and Public Policy and wrote this Note during her second year of law school. This Note was picked from the student submissions for publication. Her topic was inspired by Judge Dave Lee Brannon, who Casey interned for during the summer of 2018. She would like to give a special thank you to Judge Brannon for his mentorship and support.

Requests to authorize law enforcement to compel an individual to produce biometrics began appearing in warrant requests in 2016. Since then, courts have wrestled with the legality of these requests and ultimately split on whether compelling biometrics violates constitutional rights. This Note analyzes whether law enforcement officials or the government can compel an individual to produce their fingerprints and other biometrics for the purpose of unlocking a lawfully seized electronic device.

Biometrics or biometric recognition is defined as the automated recognition of an individual based on their unique physical characteristics, such as fingerprints.[1] Biometrics covers a broad range of technologies including facial recognition, fingerprint recognition and voice identification.[2] The widespread use of biometric recognition in cell phones coupled with the vast storage capabilities of these devices makes this issue one of great significance. If the government can force an individual to unlock his or her device, then it can gain access to all of the data that is stored on the device. In theory, this would allow law enforcement to filter through text messages, photographs, and more. Not only does this raise privacy concerns, but it also raises the question of whether this infringes upon an individual's privilege against self-incrimination.

This Note will first explain the rise of biometric recognition technology in cell phones and the role that modern cell phones play in everyday life. Second, this Note will analyze the Fourth and Fifth Amendment concerns raised by these warrant requests, focusing on the Fifth Amendment because courts have turned on the characterization of biometrics as testimonial or nontestimonial. Third, this Note will consider the decisions of the courts that have addressed this issue and will highlight where the courts are diverging. Last, this Note will set forth a potential solution as to whether the government can compel an individual to produce their biometrics in order to unlock a lawfully seized device.

I. THE INCREASED USE OF BIOMETRICS IN CELL PHONES

From the release of the first smartphone in the 1990s, a clunky mobile device with a battery life of an hour, manufacturers have continuously worked to improve cellular devices, often by incorporating the latest

1. *Biometrics*, HOMELAND SEC., https://www.dhs.gov/biometrics [https://perma.cc/HQ8T-VB8X] (May 9, 2019); *What is Biometrics?*, BIOMETRICS INST., https://www.biometricsinstitute.org/what-is-biometrics/ [https://perma.cc/4HEV-74PL] [hereinafter *What is Biometrics?*].

2. *Types of Biometrics*, BIOMETRICS INST., https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/ [https://perma.cc/Q6WY-HXJB]; *What is Biometrics?*, *supra* note 1.

technology.[3] In 2013, Apple introduced the first major smartphone to utilize biometrics, the iPhone 5s.[4] The iPhone 5s features a fingerprint sensor named Touch ID.[5] Touch ID allows users to register a fingerprint that they can then use to unlock the device.[6] In most circumstances, this allows users to secure their cell phones without requiring a passcode. With Touch ID, you are able to unlock your device with just a touch. Other cell phone manufacturers, such as Samsung, followed suit and incorporated biometric recognition into their products.[7]

Less than four years after the release of Touch ID, Apple revealed the iPhone X. The iPhone X contained the latest of biometric technology, Face ID.[8] Face ID involves the use of facial recognition software.[9] Face ID's advanced technology maps the geometry of an individual's face and then allows the individual to unlock the device with a glance at the front camera.[10] Face ID is able to register when a user wants to unlock their device and adapts to changes in appearance.[11]

Apple claims that Touch ID and Face ID utilize "some of [Apple's] most sophisticated technologies" to ensure that customers' devices are protected from the security risks that accompany this technology, such as false matches and fraud.[12] One protective measure for users utilizing Touch ID or Face ID is that the phone is set up with a passcode.[13] The passcode must be entered in order to unlock the device under certain circumstances such as when the device hasn't been unlocked for more than 48 hours or when the device restarts.[14] It is also required when there

3. Doug Aamoth, *First Smartphone Turns 20: Fun Facts About Simon*, TIME (Aug. 18, 2014), http://time.com/3137005/first-smartphone-ibm-simon/ [https://perma.cc/ZGJ2-LQVC] ("A tip of the hat to Simon, long referenced as the first smartphone. It went on sale to the public on August 16, 1994.").

4. Fionna Agomuoh, *Password-free smartphones are no longer the stuff of science fiction — they're everywhere*, BUS. INSIDER (Dec. 27, 2017, 3:28 PM), https://www.businessinsider.com/smartphone-biometrics-are-no-longer-the-stuff-of-science-fiction-2017-12 [https://perma.cc/7YJE-B8RG].

5. *Id.*

6. *Use Touch ID on iPhone and iPad*, APPLE (Apr. 24, 2019), https://support.apple.com/en-us/HT201371 [https://perma.cc/6GKJ-MGKR].

7. Agomuoh, *supra* note 4.

8. Brian Roemmele, *How Does Apple's New Face ID Technology Work?*, FORBES (Sept. 13, 2017, 12:47 PM), https://www.forbes.com/sites/quora/2017/09/13/how-does-apples-new-face-id-technology-work/#1c4e636f2b7f [https://perma.cc/8PWN-MMQG].

9. *Id.*

10. *Face ID Security Guide*, APPLE, 2 (Nov. 2017), https://www.apple.com/tr/business/docs/site/FaceID_Security_Guide.pdf [https://perma.cc/V86R-4N3F] [hereinafter *Face ID Security Guide*].

11. *Id.*

12. *About Touch ID Advanced Security Technology*, APPLE (Sept. 11, 2017), https://support.apple.com/en-us/HT204587 [https://perma.cc/GGQ3-WUP2].

13. *Face ID Security Guide*, *supra* note 10.

14. *Id.*

are multiple failed attempts to unlock the device with the fingerprint or facial recognition software.[15]

II. CELL PHONE USAGE & CELL PHONE STORAGE

Cell phones have become an integral part of daily life. According to a Pew Research Center study, 97% of Americans own a cell phone of some kind, with 85% owning a smartphone.[16] This is a dramatic increase from a 2011 study that found only 35% of U.S. adults owned a smartphone.[17] Further studies reported 83% of Americans use their mobile device to go online.[18] Along with cell phone ownership, cell phone storage increased dramatically. Now, "[t]he sum of an individual's private life" can be reconstructed through the contents of a cell phone.[19]

In the 2014 landmark decision of *Riley v. California*,[20] the Supreme Court addressed the unique issues that cell phones pose.[21] *Riley* involved the consolidation of two appeals where each defendant was advocating that the warrantless search of their cell phone, which was seized incident to arrest, was unconstitutional.[22] The Court noted that "[t]hese cases require us to decide how the search incident to arrest doctrine applies to modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important part of human anatomy."[23]

After noting the pervasive presence of cell phones, the Court identified that the immense storage capacity of modern cell phones raises much larger privacy concerns than those that are raised in the search of a wallet or a purse.[24] Unlike a wallet or a purse, a cell phone can contain a record of almost every aspect of an individual's life in pictures, text messages, mobile applications, and other stored data.[25] To determine "whether to exempt a given type of search from the warrant requirement," the court weighed "the degree to which [the search] intrudes upon an

15. *Id.*

16. *Mobile Phone Ownership Over Time*, PEW RESEARCH. CTR. (last updated Apr. 7, 2021), http://www.pewinternet.org/fact-sheet/mobile/ [https://perma.cc/X5UF-BK69].

17. Andrew Perrin, *10 Facts About Smartphones as the iPhone Turns 10*, PEW RESEARCH CTR. (June 28, 2017), https://www.pewresearch.org/fact-tank/2017/06/28/10-facts-about-smartphones/ [https://perma.cc/UH5G-24W6].

18. Andrew Perrin & Jingjing Jiang, *About a Quarter of U.S. Adults Say That They Are 'Almost Constantly' Online*, PEW RESEARCH CTR. (Mar. 14, 2018), http://www.pewresearch.org/fact-tank/2018/03/14/about-a-quarter-of-americans-report-going-online-almost-constantly/ [https://perma.cc/L346-M5YE].

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

20. 573 U.S. 373 (2014).

21. *Id.* at 385.

22. *Id.* at 379–81 (citing United States v. Wurie, 612 F. Supp. 2d 104 (D. Mass. 2009)).

23. *Id.* at 385.

24. *Id.* at 393–95.

25. *Id.* at 393.

individual's privacy and . . . the degree to which [the search] is needed for the promotion of legitimate governmental interests."[26] The Court acknowledged that requiring a warrant prior to a search may delay law enforcement's ability to combat crime, but ultimately found that the privacy costs outweighed the competing governmental interest.[27]

Privacy supporters applauded the Court's decision in *Riley* as a step in the right direction.[28] "[The Justices] get that digital technologies are different from anything our culture has seen before. . . . and they get that, in at least some contexts, the Old Rules need to change."[29] *Riley* is an important case because it suggests that lower courts should consider the unique issues surrounding cell phones, including the heightened privacy concerns when applying the law.[30] *Riley* also provides a glimpse into how the Court may analyze the issue of biometric recognition.

III. THE FOURTH AND FIFTH AMENDMENT IMPLICATIONS

The request to compel the production of biometrics implicates the Fourth and Fifth Amendments. To begin, the Fourth Amendment is explicitly implicated because the government is requesting authorization to engage in this behavior through a warrant. The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[31]

Rule 41 of the Federal Rules of Criminal Procedure sets forth the general principles governing the use and obtainment of warrants.[32] In regard to electronic devices, Rule 41 states that a warrant may authorize the seizure of electronically stored media and information.[33] As discussed above, *Riley* requires that the government obtain a warrant prior to searching the data on a cellphone.[34]

---

26. *Riley*, 573 U.S. at 385 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).
27. *Id.* at 401.
28. Richard M. Re, *Symposium: Inaugurating the Digital Fourth Amendment*, SCOTUS BLOG (June 26, 2014, 12:37 PM), https://www.scotusblog.com/2014/06/symposium-inaugurating-the-digital-fourth-amendment/ [https://perma.cc/CHP5-6Q3Z].
29. *Id.*
30. *Id.*
31. U.S. CONST. amend. IV.
32. *See* FED. R. CRIM. P. 41.
33. FED. R. CRIM. P. 41(e)(2)(B).
34. Riley v. California, 573 U.S. 373, 386 (2014).

Moreover, the Fourth Amendment is implicated because of an individual's right to privacy. Case law has established that the basic purpose behind the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."[35] Like the Court recognized in *Riley*, privacy concerns are at an all-time high when cell phones are involved since an individual's entire private life can be reconstructed through the stored information.[36] The Court reaffirmed the interest in safeguarding privacy rights of individuals in *Carpenter v. United States*.[37] There, the Court restated that even in the face of advancing technology, "this Court has sought to 'assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"[38]

In *Carpenter*, the Court applied the Fourth Amendment "to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals."[39] While the holding in *Carpenter* was stressed to be a narrow one, the Court nevertheless recognized an individual's reasonable privacy expectation "in the whole of their physical movements" and found that the government did not acquire the required warrant before seizing the defendant's cell-site records.[40]

Despite the fact that there are various Fourth Amendment concerns raised by these warrant requests, the courts that have addressed this issue have dedicated little space to the Fourth Amendment analysis and focused on the constitutionality of these requests under the Fifth Amendment. While the courts' decisions seem to turn on whether or not the compelled production of a physical characteristic is testimonial or nontestimonial under the Fifth Amendment, the Fourth Amendment is likely to play a much larger role in the outcome of this issue as it works its way up the courts. This is supported by the Court's recent analyses in *Carpenter* and *Riley*, where the Court stressed the heightened privacy concerns due to the advancement of technology.

IV. THE RIGHT AGAINST SELF-INCRIMINATION AND THE REQUEST TO COMPEL BIOMETRICS

The Fifth Amendment provides in relevant part: "No person . . . shall be compelled in any criminal case to be a witness against himself . . . ."[41] It is well established that the right against self-incrimination is not

35. Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (quoting Camara v. Mun. Ct. of City and Cnty. of S.F., 387 U.S. 523, 528 (1967)).

36. *See Riley*, 573 U.S. at 386.

37. *Carpenter*, 138 S. Ct. at 2214.

38. *Id.* (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

39. *Id.* at 2216.

40. *Id.* at 2217, 2220.

41. U.S. CONST. amend. V.

absolute.[42] The privilege only applies to communications that are testimonial, compelled, and incriminating.[43] It is a relatively simple task to determine whether a communication is compelled or is incriminating, but the line becomes blurry when deciding what constitutes a testimonial versus a nontestimonial communication. To this end, the Court has stated that "[t]he difficult question whether a compelled communication is testimonial for purposes of applying the Fifth Amendment often depends on the facts and circumstances of the particular case."[44]

A testimonial communication is a communication that "explicitly or implicitly, relate[s] a factual assertion or disclose[s] information."[45] The Court has consistently held that the compulsion of certain acts falls outside the protections of the Fifth Amendment despite the fact that the compelled act may lead to incriminating information.[46] For example, in *Schmerber v. California*,[47] the Court held that the forced taking of a blood sample did not violate the individual's right against self-incrimination.[48] The Court recognized that in compelling the blood sample the accused was forced "to submit to an attempt to discover evidence that might be used to prosecute him for a criminal offense," but this was not enough to bring the compelled act within the meaning of the privilege.[49] "Not even a shadow of testimonial compulsion upon or enforced communication by the accused was involved either in the extraction or in the chemical analysis."[50] Similarly, the compulsion of voice exemplars, handwriting exemplars, and fingerprints all fall outside the Fifth Amendment privilege.[51] Through this line of cases, the Court generally established

42. United States v. Hubbell, 530 U.S. 27, 34 (2000) ("The term 'privilege against self-incrimination' is not an entirely accurate description of a person's constitutional protection against being 'compelled in any criminal case to be a witness against himself.' The word 'witness' in the constitutional text limits the relevant category of compelled incriminating communications to those that are 'testimonial' in character.").

43. *Id.*

44. Doe v. United States, 487 U.S. 201, 214–15 (1988) (citing *Fisher v. United States*, 425 U.S. 391, 410 (1976)).

45. *Id.* at 210.

46. *Id.*

47. 384 U.S. 757 (1966).

48. *Id.* at 772.

49. *Id.* at 761.

50. *Id.* at 765.

51. *See* United States v. Dionisio, 410 U.S. 1, 5–7 (1973) (compelling voice exemplars does not violate the Fifth Amendment); Gilbert v. California, 388 U.S. 263, 265–67 (1967) (compelling handwriting exemplars does not violate the Fifth Amendment); Holt v. United States, 218 U.S. 245, 252–53 (1910) (compelling a suspect to put on particular clothing does not violate the Fifth Amendment); *Schmerber*, 384 U.S. at 764 (compelling a suspect to submit to fingerprinting does not violate the Fifth Amendment).

that there is no testimonial communication in the "compelled display of identifiable physical characteristics." [52]

The compelled production of specific documents also raises Fifth Amendment concerns.[53] In *Fisher v. United States*,[54] the compelled production of documents was held non-testimonial because the papers were voluntarily prepared prior to the summons.[55] Based on this, the individual could not avoid complying with the summons on the grounds that the documents contained incriminating information.[56] However, in *United States v. Hubbell*,[57] the respondent was similarly subpoenaed to produce specific documents, but the Court held this to be a testimonial communication.[58] In analyzing the compelled act the Court stated:

> We have held that "the act of production" itself may implicitly communicate "statements of fact." By "producing documents in compliance with a subpoena, the witness would admit that the papers existed, were in his possession or control, and were authentic." . . . Whether the constitutional privilege protects . . . the act of production itself, is a question that is distinct from the question whether the unprotected contents of the documents themselves are incriminating.[59]

Here, the Court found that the respondent would "make extensive use of 'the contents of his own mind'" in identifying and assembling the compelled documents.[60] This made the production more analogous to "telling an inquisitor the combination to a wall safe" rather than "being forced to surrender the key to a strongbox."[61] Because the defendant would implicitly communicate statements of fact through the production of documents, the defendant was justified in refusing to comply with the subpoena.

Biometrics are, by definition, physical characteristics. In warrant requests to compel biometrics, law enforcement seeks to use these physical traits to unlock a seized electronic device. Law enforcement officials would likely argue that there is no Fifth Amendment issue when they request authorization to compel the production of biometrics

---

52. *See Dionisio*, 410 U.S. at 5–7 (citing *Gilbert*, 388 U.S. at 266–67; *Holt*, 218 U.S. at 252).

53. *See* United States v. Hubbell, 530 U.S. 27, 35–36.

54. 425 U.S. 391 (1976).

55. *Id.* at 414.

56. *Hubbell*, 530 U.S. at 36 (citing *Fisher*, 425 U.S. at 409–10).

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

58. *Id.* at 43.

59. *Id.* at 36–37.

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

61. *Id.* (citing Doe v. United States, 487 U.S. 201, 210 n.9 (1988)).

because there is nothing communicative in the act of production. "The government chooses the finger to apply to the sensor, and thus obtains the physical characteristic—all without need for the person to put any thought at all into the seizure."[62] An individual could even be asleep or unconscious during the seizure.[63] But, unlike the cases involving the compulsion of a blood sample or voice exemplar, here the compulsion of the physical trait is being used to unlock a cell phone, a device that stores vast amounts of information. If the compelled physical characteristic unlocks the seized cell phone, the individual implicitly communicates that they had a least some control over the device and its contents.

V. THE SPLIT AMONG LOWER COURTS

The issue of compelling biometrics is beginning to arise in front of judges more and more. So far, most of the litigation has taken place in the lower district courts.[64]

A. *In re Application for a Search Warrant*

The U.S. District Court for the Northern District of Illinois was one of the first federal courts to issue an opinion on whether law enforcement officials can compel biometrics.[65] In 2017, the magistrate judge was presented with a warrant request where the government identified items to be seized at a specified location and requested the authority to take the electronics in order to conduct forensic analysis pursuant to Fed. R. Crim. P. 41(e)(2)(B).[66] These standard requests raised no issues with the court.[67]

> "[I]n its warrant application, the government also seeks the authority to compel any individual who is present at the subject premises at the time of the search to provide his fingerprints and/or thumbprints onto the Touch ID sensor of any Apple iPhone, iPad, or other Apple brand device in order to gain access to the content of any such device."[68]

---

62. *In re* Search Warrant Application for [Redacted Text], 279 F. Supp. 3d 800, 804 (N.D. Ill. 2017).

63. *Id.*

64. *But see In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1352 (11th Cir. 2012) (finding the act of decrypting hard drives to be sufficiently testimonial so the defendant was justified in refusing to comply with the subpoena duces tecum).

65. *See In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1074 (N.D. Ill. 2017) (concluding that the government had not "established a proper basis to force any individual at the subject premises to provide a fingerprint").

66. *Id.* at 1067.

67. *Id.*

68. *Id.* (internal quotation marks omitted).

This abnormal request raised a number of concerns and was ultimately denied.[69]

First, the judge found that the warrant did not meet the probable cause requirements of the Fourth Amendment to "compel any person who happens to be at the subject premises at the time of the search to give his fingerprint to unlock an unspecified Apple electronic device."[70] The government argued that the Fourth Amendment is not implicated in the taking of a fingerprint, but the court rejected this view.[71] The judge stressed that it is not the fingerprint itself but rather "the method of obtaining the print that is at issue."[72] Here, the factual deficiencies of the warrant such as the failure to specify the persons and specific devices likely to be found at the premises violated the requirements of the Fourth Amendment.[73]

Then, the judge turned to the Fifth Amendment concerns.[74] The Court cited *Hubbell* and argued that a fingerprint is akin to a key that opens a strongbox which involves no testimonial communication and therefore falls outside Fifth Amendment protections.[75] The judge noted that generally the production of physical characteristics does not raise Fifth Amendment concerns,[76] but Fifth Amendment concerns are raised "where the production of information is compelled, and the production itself is deemed incriminating."[77]

Applying previous Supreme Court decisions, the judge reasoned that the compelled act does "explicitly or implicitly relate a factual assertion or disclose information" because "[t]he connection between the fingerprint and Apple's biometric security system, shows a connection with the suspected contraband."[78]

> By using a finger to unlock a phone's contents, a suspect is *producing* the contents on the phone. With a touch of a finger, a suspect is testifying that he or she has accessed the phone before, at a minimum, to set up the fingerprint password capabilities, and that he or she currently has some

---

69. *Id.*

70. *Id.* at 1068.

71. *In re* Application for a Search Warrant, 236 F. Supp. 3d at 1068, 1069 (citing *United States v. Sechrist*, 640 F.2d 81, 86 (7th Cir. 1981)).

72. *Id.* at 1070.

73. *Id.*

74. *Id.*

75. *Id.* (citing Commonwealth v. Baust, 89 Va. Cir. 267, 270 (Va. Cir. Ct. 2014)).

76. *Id.* at 1070–71 (citing United States v. Dionisio, 410 U.S. 1, 5–7 (1973); Gilbert v. California, 388 U.S. 263, 265–67 (1967); United States v. Wade, 388 U.S. 218 (1967); Schmerber v. California, 384 U.S. 263, 267 (1966)).

77. *In re* Application for a Search Warrant, 236 F. Supp. 3d at 1071 (citing Fisher v. United States, 425 U.S. 391, 410 (1976)).

78. *Id.* at 1073 (citing United States v. Doe, 670 F.3d 1335, 1342 (11th Cir. 2012)).

> level of control over or relatively significant connection to the phone and its contents.[79]

To the government's argument that the "Fifth Amendment privilege . . . offers no protection against compulsion to submit to fingerprinting," the judge pointed out that the case law that the government relies on was decided before the existence of cell phones and only dealt with the use of fingerprinting for identification purposes.[80] The judge then turned to the Supreme Court's reasoning in *Riley* for support in rejecting the proposition that fingerprinting for identification purposes and fingerprinting to unlock an electronic device are the same.[81] But, the judge ended the opinion by stating that not all of these requests would raise problems with the Fourth and Fifth Amendments, leaving the door open to future requests.[82]

B. *In the Matter of the Search Warrant Application For [Redacted Text]*

Appearing to be one of the more active courts on this issue, the U.S. District Court for the Northern District of Illinois addressed the legality of compelling biometrics again a few months after *In re Application for a Search Warrant*.[83] In the case of *In the Matter of the Search Warrant Application for [Redacted Text]*,[84] the court reviewed the order of a magistrate judge who had similarly denied the request to compel the use of fingerprints.[85] Reviewing the decision as a matter of first impression, the district court disagreed that "the Fifth Amendment prohibits the forced unlocking of a device by finger touch."[86] The district court instead held that the Fifth Amendment did not bar a warrant requesting authorization to compel home residents to produce their fingerprints to unlock electronic devices.[87]

In this case, the government requested "authorization to seize, in effect, the four residents in order to apply their fingers (including thumbs)

---

79. *Id.*

80. *Id.* (criticizing the government's reliance on United States v. Wade, 388 U.S. 218, 223 (1967)).

81. *Id.* at 1073–74 (citing Riley v. California, 573 U.S. 373, 393 (2014)).

82. *Id.* at 1074.

83. *See In re* Search Warrant Application for [Redacted Text], 279 F. Supp. 3d 800, 801 (N.D. Ill. 2017).

84. 279 F. Supp. 3d 800 (N.D. Ill. 2017).

85. *Id.*

86. *In re* Search of Single-Family Home & Attached Garage Located at [redacted], 2017 WL 4563870, at *7 (N.D. Ill. Feb. 21, 2017), *rev'd*, 279 F. Supp. 3d 800.

87. *In re* Search Warrant Application for [Redacted Text], 279 F. Supp. 3d at 807 ("For the reasons discussed, the government's application to require the fingerprint seizure of the four residents does not violate the privilege against self-incrimination set forth in the Fifth Amendment.").

to Apple-made devices (here, most likely iPhones and iPads) found at the home."[88] The affidavit in support of the warrant application stated that the devices were likely encrypted, requiring a passcode or Touch ID.[89] The government stressed that the ability to unlock a device with Touch ID is time sensitive, "[s]o to take advantage of this potential way of unlocking an iPhone or iPad, the government asks that the four residents of the home—if they are present during the search—be required to press fingers, chosen by the [G]overnment, to the [t]ouch ID sensor."[90]

The magistrate judge denied the warrant because such a compelled production would violate an individual's Fifth Amendment privilege, but the district court reversed in part, finding that the warrant did not violate an individual's right against self–incrimination.[91] The district court stated that the fingerprint seizure sought in the warrant application did not engage the thought process of any of the individuals.[92] "The application of the fingerprint to the sensor is simply the seizure of a physical characteristic, and the fingerprint by *itself* does not communicate anything."[93] The district court distinguished this act from the line of cases that involve the production of documents by relying on the fact that the compelled individual did not have to put any thought into the seizure.[94]

In addition, the district court rejected the magistrate judge's characterization of "the fingerprint seizure as containing an implicit communication when the fingerprint *is applied* to the Touch ID sensor: if the device unlocks, then the incriminating inference is that the person had possession or control of the device."[95] The court said the fact that the compelled physical trait yields incriminating information does not immediately make the compulsion unconstitutional.[96] "If a compelled act is not testimonial, then the privilege against self-incrimination does not apply—even if the act is incriminating."[97] So, if the act does not inherently contain a communication then the compulsion is constitutional.

The court found the surrender of a person's fingerprint to be analogous to the surrender of a key to a safe whose contents are otherwise unavailable.[98] Based on this reasoning, the warrant application did not

88. *Id. at* 802.
89. *Id.*
90. *Id.*
91. *Id.* at 801.
92. *Id.* at 804.
93. *In re* Search Warrant Application for [Redacted Text], 279 F. Supp. 3d at 807
94. *In re* Search Warrant Application for [Redacted Text], 279 F. Supp. 3d at 804.
95. *Id.* at 805 (emphasis in original).
96. *Id.*
97. *Id.* (citing Doe v. United States, 487 U.S. 201, 210 (1988)).
98. *Id.* at 806.

violate an individual's Fifth Amendment right.[99] However, the court did limit its holding by suggesting that there are times when the Fourth Amendment would preclude the authorization of these requests.[100]

In re Application for a Search Warrant and *In the Matter of the Search Warrant Application for [Redacted]* involved similar warrant requests and were decided in the same court within the same year. The fact that the two turned out differently is counter–intuitive and highlights the split among courts. One way to distinguish the two cases might be in the specificity of the warrant requests. In the warrant at issue in *In re Application for a Search Warrant* the government requested authorization to compel "any individual who is present"[101] while the request of *In the Matter of the Search Warrant Application for [Redacted]* narrowly tailored its request to four individuals.[102] It makes sense that law enforcement sought to make their request more specific after the magistrate judge highlighted the factual deficiencies of the warrant request.

C. *In the Matter of Search of [Redacted] Washington, District of Columbia*

In 2018, a magistrate judge for the U.S. District Court for the District of Columbia addressed this "emerging area of the law" in the case of *In the Matter of the Search of [Redacted] Washington, District of Columbia*.[103] Similar to the two preceding cases discussed above, the warrant application requested the following:

> "[D]uring the execution of the search of the [premises] described in Attachment A, law enforcement personnel are also specifically authorized to compel [the Subject] to provide biometric features, including pressing his fingers (including thumbs) against and/or putting his face before the sensor, or any other security feature requiring biometric recognition, of:
>
> (a) any of the [Subject Devices] found at the [premises], and
>
> (b) where the [Subject Devices] are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

99. *Id.* at 807.

100. *In re* Search Warrant Application for [Redacted Text], 279 F. Supp. 3d at 807.

101. *See In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1067 (N.D. Ill. 2017).

102. In re Search Warrant Application for [Redacted Text], 279 F. Supp. 3d at 807.

103. *In re* Search of [Redacted] Wash., D.C., 317 F. Supp. 3d 523, 526 (D.D.C. 2018).

> for the purpose of attempting to unlock the [Subject Devices'] security features in order to search the contents as authorized by this warrant."[104]

The warrant request included a disclaimer that law enforcement officials would not force the Subject to provide his passcode nor would they force him to identify which fingerprint was used in accessing the device.[105]

The judge granted the warrant application, finding that it did not conflict with Fourth or Fifth Amendment guarantees.[106] Beginning with an analysis of whether compelling biometrics violated an individual's Fourth Amendment rights, the court relied on the fact that it has been consistently held that obtaining physical characteristics from an individual does not amount to an intrusion upon a person's privacy under the Fourth Amendment.[107] The court noted that when a physical characteristic is used for investigatory purposes, different Fourth Amendment concerns are raised.[108]

When physical characteristics are used for investigatory purposes,

> [t]he question then is–even where the government is permitted to detain briefly an individual during a search warrant's execution . . . what further showing does the Fourth Amendment require before the government may be authorized to compel the use of an individual's biometric features in an attempt to unlock a digital device . . . ?[109]

The court then formulated a standard that the government must meet when attempting to unlock an electronic device for investigatory purposes:

> [T]he government may compel the use of an individual's biometric features, if (1) the procedure is carried out with dispatch and in the immediate vicinity of the premises to be searched, and if, at time of the compulsion, the government has (2) reasonable suspicion that the suspect has committed a criminal act that is the subject matter of the warrant, and (3) reasonable suspicion that the individual's biometric features will unlock the device, that is, for example, because

104. *Id.* at 526–27.
105. *Id.* at 527.
106. *Id.* at 540.
107. *Id.* at 529.
108. *Id.* at 530.
109. *In re* Search of [Redacted] Wash., D.C., 317 F. Supp. 3d at 530.

> there is a reasonable suspicion to believe that the individual is a user of the device.[110]

Turning to the Fifth Amendment analysis, the court found the guarantee against self–incrimination protects an individual "from having to reveal, directly or indirectly, knowledge of facts relating him to the offense or from having to share his thoughts and beliefs with the Government."[111] The federal public defender argued that compelling biometrics "is inherently testimonial because it would implicitly communicate that the suspect possessed or controlled the device with incriminating evidence."[112] The court rejected this argument, finding that the compelled production of biometrics is "far more akin to the surrender of a safe's key than its combination," referring to the infamous *Hubbell* distinction.[113]

The compulsion of the individual's biometric features was found to be more analogous to compelling a safe's key, which is unprotected, because "there will be no revelation of the contents of the Subject's mind with the procedure proposed by the government for collection of the Subject's biometric features."[114] In this case, "[t]he government chooses the finger to apply to the sensor, and thus obtains the physical characteristic—all without the need for the person to put any thought at all into the seizure."[115] The court found this case to be analogous to drawing blood to test the blood–alcohol level or requiring a suspect to put on a specific shirt for identification purposes and concluded that the compelled production of biometrics was non–testimonial.[116] "[T]he Fifth Amendment privilege is not triggered where, as here, 'the [g]overnment merely compels some physical act, *i.e.*, where the individual is not called upon to make use of the contents of his mind."[117]

D. *In the Matter of the Search of a Residence in Oakland, California*

More recently, the U.S. District Court for the Northern District of California faced this issue.[118] Here, the magistrate judge denied the warrant request finding that it ran afoul of Fourth and Fifth Amendment

---

110. *Id.* at 532–33.

111. *Id.* at 534 (citing Doe v. United States, 487 U.S. 201, 213 (1988)).

112. *Id.* at 535 (internal quotation marks omitted).

113. *Id.* (referring to United States v. Hubbell, 530 U.S. 27, 43 (2000)).

114. *Id.* at 535–36.

115. *In re* Search of [Redacted] Wash., D.C., 317 F. Supp. 3d at 536 (quoting *In re* Search Warrant Application for [Redacted Text], 279 F. Supp. 3d at 804).

116. *Id.* at 536–37 (citing Schmerber v. California, 384 U.S. 757, 764–65 (1966)).

117. *Id.* at 537 (quoting *In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1345 (11th Cir. 2012)).

118. *In re* Search of a Residence in Oakland, Cal., 354 F. Supp. 3d 1010, 1013–14 (N.D. Cal. 2019).

guarantees.[119] In *In the Matter of the Search of a Residence in Oakland, California*, the government submitted an application for a search warrant that paralleled the warrant applications seen in the previously explained cases.[120] The Government's application requested the authority to seize various items at an identified location and "to compel any individual present at the time of the search to press a finger (including a thumb) or utilize other biometric features, such as facial or iris recognition, for the purposes of unlocking the digital devices found in order to permit a search of the contents as authorized by the search warrant."[121] It should be noted that the government requested authorization to compel *any* individual in its request here.[122]

Similar to the previously discussed opinions, the court began its analysis with whether the warrant infringed upon Fourth Amendment guarantees.[123] The court focused on the broad language of the warrant request and easily found that it violated the Fourth Amendment as it lacked sufficient probable cause to compel *any* individual to produce biometrics and to seize *all* digital devices.[124] The court also left the door open for the government to resubmit the warrant application, suggesting that the warrant would comply with Fourth Amendment requirements if it were specifically tailored.[125]

Then the court turned to the Fifth Amendment.[126] The court focused on the purpose of the fingerprints, and it noted that fingerprints serve the same purpose as a passcode–they are used to unlock a device.[127] So, the seemingly non–testimonial physical characteristic is made testimonial because of the way the characteristic is being used.[128] For this reason, the court held that the biometrics could not be compelled by the government.[129] If the feature unlocks the device, "the act concedes that the phone was in the possession and control of the suspect, [sic] and authenticates ownership or access to the phone and all of its digital contents."[130]

Due to the implicit communication, the court found that using a fingerprint or facial scan to unlock a phone was fundamentally different from drawing blood or identifying a person from a voice exemplar.

119. *Id.* at 1013.
120. *Id.*
121. *Id.*
122. *Id.*
123. *Id.* at 1013–14.
124. *See In re* Search of a Residence in Oakland, Cal., 354 F. Supp. 3d. at 1014.
125. *See id.*
126. *Id.*
127. *See id.* at 1015.
128. *Id.* at 1016.
129. *Id.*
130. *In re* Search of a Residence in Oakland, Cal., 354 F. Supp. 3d. at 1016.

"'[W]ith a touch of a finger, a suspect is testifying that he or she has accessed the phone before, at a minimum, to set up the fingerprint password capabilities, and that he or she currently has some level of control over or relatively significant connection to the phone and its contents.'"[131] The court stressed that the foregone conclusion doctrine would not be able to save these types of requests from invalidation because law enforcement could not anticipate the full contents of a mobile device.[132] "[T]he Government inherently lacks the requisite prior knowledge of the information and documents that could be obtained via a search of these unknown digital devices, such that it would not be a question of mere surrender," so the foregone conclusion doctrine would not apply.[133]

VI. THIS ISSUE IN THE NEWS

The issue of compelling biometrics has started to receive more attention from the courts and the public. For example, this issue was recently seen in the news after the warrant applications for Michael Cohen's devices were released. On March 20, 2019, CNN reported that the "FBI made use of Cohen's use of Touch ID and Face ID on his Apple devices."[134] "[A]n FBI agent requested authorization 'to press the fingers (including thumbs) of Cohen to the Touch ID sensors of the Subject Devices, or hold the Subject Devices in front of Cohen's face, for the purpose of attempting to unlock the Subject Devices via Touch ID or Face ID.'"[135] The article pointed out that Touch ID and Face ID are marketed as being more secure, when in fact, each really gives law enforcement another way to access the contents of private devices.[136] CNBC also picked up this story and highlighted that Apple has traditionally fought against law enforcement's efforts to access devices, but here law enforcement has found a way around Apple.[137] CNBC reported that previous court rulings have varied on whether or not individuals can

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

132. *Id.* at 1017 (citing Riley v. California, 573 U.S. 373, 399 (2014)).

133. *In re* Search of a Residence in Oakland, Cal., 354 F. Supp. 3d at 1017–18 (citing United States v. Hubbell, 530 U.S. 27, 44–45 (2000)).

134. Kevin Collier & Marshall Cohen, *Michael Cohen warrants show how the FBI can unlock your phone and track your movements*, CNN POLITICS, https://www.cnn.com/2019/03/19/politics/michael-cohen-warrants-fbi-phone/index.html [https://perma.cc/LX4Y-E77Q] (Mar. 20, 2019, 2:56 PM).

135. *Id.* (citing warrant application).

136. *Id.*

137. Lauren Feiner, *Investigators sought to use Michael Cohen's face and fingerprints to access his Apple devices*, CNBC (Mar. 19, 2019, 12:12 PM), https://www.cnbc.com/2019/03/19/investigators-asked-to-use-michael-cohens-face-id-to-access-iphone.html [https://perma.cc/T4VC-TC33].

legally be compelled to produce biometric data so that law enforcement officials can gain access to their electronic devices.[138]

VII. IS THE SOLUTION TO REQUIRE A PASSCODE?

A passcode is made up of a sequence of letters, numbers, and other characters. A passcode can be required prior to accessing an electronic device. Just like biometric recognition in cell phones, passcodes are a way to protect a device from unwanted intrusion. Although biometrics and passcodes serve the same purpose, passcodes are treated differently under the law. Courts have afforded more protections to passcodes finding that passcodes, as opposed to biometrics, are protected under the Fifth Amendment as testimonial communications.[139]

While there are some exceptions, most courts have ruled that an individual cannot be forced to reveal their passcode, as this requires an individual to reveal the inner contents of their mind.[140] In the 2014 decision of *Commonwealth of Virginia v. Baust*,[141] the state court held that the defendant's passcode could not be compelled because of the Fifth Amendment right against self-incrimination.[142] In the same breath, the court held that the defendant could be forced to produce his fingerprint.[143] The court reasoned that compelling a passcode required the defendant to reveal his mental processes, which is testimonial, but compelling fingerprints would not require the defendant to communicate anything so it did not qualify as a protected communication under the Fifth Amendment.[144] Despite the fact that passcodes and fingerprints are being used for the same purpose here, courts have tended to distinguish the two. In light of this, requiring a passcode appears to be the most secure method of protecting electronic devices.

CONCLUSION

The question of whether law enforcement can compel an individual to produce fingerprints and other biometrics for the purpose of unlocking a lawfully seized electronic is an important one due to the pervasive presence of cellphones and the amount of data contained within a device.

---

138. *Id.*

139. *See* Pratik Parikh, *IPHONE X: Unlocking the Self Incrimination Clause of the Fifth Amendment*, 45 RUTGERS COMPUTER & TECH. L.J. 58, 78 (2019) (citing United States v. Kirschner, 823 F. Supp. 2d 665, 668 (E.D. Mich. 2010)).

140. Commonwealth v. Baust, 89 Va. Cir. 267, 270 (Va. Cir. Ct. 2014) (citing United States v. Doe, 487 U.S. 201, 211 (1988)); *but see* State v. Stahl, 206 So. 3d 124, 137 (Fla. Dist. Ct. App. 2016) (holding that requiring the defendant to produce his passcode was not testimonial).

141. 89 Va. Cir. 267 (Va. Cir. Ct. 2014).

142. *Id.* at 271.

143. *Id.*

144. *Id.*

Currently, there is a split among lower courts on whether the request to compel biometrics infringes upon constitutional rights. The major focus in these cases appear to be whether the compelled production of biometrics is a protected testimonial communication or an unprotected non–testimonial communication within the meaning of the Fifth Amendment.

On one hand, there is an argument that this is a non–testimonial communication because the participation of the individual is irrelevant. In a sense, the act is like the production of a key to the safe. The individual hands over the key and while it may lead to incriminating information, it does not require the revelation of any mental processes.

On the other hand, the alleged non–testimonial act is being used for the purpose of unlocking a cell phone. If the physical trait successfully unlocks the device, then the individual is conveying an implicit communication that they had at least some control over the device. Additionally, the physical characteristic serves the same purpose as a passcode, which is generally afforded more protection.

In light of the heightened privacy concerns implicated by cell phones and the Court's decision in *Riley*, the Fourth Amendment may also bar the very broad and generalized requests to compel biometrics. When weighing an individual's privacy interests with law enforcement's interests, it appears that the privacy interests significantly outweigh the competing interests as an individual's entire private life can be reconstructed through the data stored on their cell phone.

However, this is not to say that law enforcement should be precluded from compelling biometrics completely. The ability to access the contents of a device serves important investigatory purposes. The government should be able to utilize these requests to gain access to cell phones, especially since cell phones are not precluded from being searched. In *Riley*, the Court held that a cell phone could be searched if law enforcement secured a warrant.

At a minimum, law enforcement officials should be required to plead with particularity who can be compelled to produce biometrics and what devices are likely to be involved. This would make any warrant application requesting authorization to compel "any" individual to produce biometrics facially invalid. Additionally, law enforcement should also need to specify the contents of the phone they plan to search to limit the intrusion on an individual's privacy. Whether that entails specifying applications included in the search or pinpointing the particular communications, there must be some limit to the search.

Ultimately, to have clarity on this issue, the Supreme Court will have to weigh in on the constitutionality of compelling biometrics. The widespread use of cell phones coupled with the lack of uniformity among

the lower courts suggests that this issue will be one the Court will address sooner rather than later.