SAY CHEESE: HOW THE FOURTH AMENDMENT FAILS TO PROTECT YOUR FACE

Antonio Vayas[*]

I. INTRODUCTION

From photographs and fingerprints to facial recognition, technology has changed the tools available to law enforcement.[1] Police officers can now run an arrested individual's DNA to determine if it matches with DNA found in a previously unsolved case.[2] As the complexity of everyday technology grows (i.e., a new smartphone coming out every year), so too does the difficulty of defining the proper limits of law enforcement's power to use information generated by more complex technology. This Comment addresses one development in particular—the availability of biometric technology on mobile devices.

Opening a smartphone used to require inputting a passcode or password.[3] But on both the iPhone and the Samsung Galaxy, the two most widely owned phones on the market,[4] there are now two additional, more popular, ways to open a phone. One can open his or her phone using a fingerprint,[5] or a face scan using the dimensions of his

[*]J.D. Candidate, 2021, Seton Hall University School of Law; B.A., 2017, New York University. I would like to thank Professor Brian Murray and my Comments Editor, Alex Corson, for their constant help and guidance throughout this writing process. Further, I thank Luke Dodge, Avi Muller, and all of the members of the Seton Hall Law Review for their help throughout this editing process.

[1] *See* Jeffrey Dastin, *California Legislature Bars Facial Recognition for Police Body Cameras*, REUTERS (Sept. 12, 2019), https://www.reuters.com/article/us-california-facial-recognition/california-legislature-bars-facial-recognition-for-police-body-cameras-idUSKCN1VX2ZP.

[2] *See, e.g.*, Maryland v. King, 569 U.S. 435, 465–66 (2013) (upholding a buccal swab administrative scheme).

[3] *See, e.g.*, Dave Johnson, *How to Lock Your iPhone with a Passcode*, BUS. INSIDER (May 14, 2019), https://www.businessinsider.com/how-to-lock-iphone.

[4] *See* Sudarshan, *Most Shipped Smartphones in 2020: iPhone 11, Galaxy A51, Redmi Note 9 Pro & More*, GIZMOCHINA (Feb. 25, 2021), https://www.gizmochina.com/2021/02/25/most-shipped-smartphones-2020-omdia.

[5] *See, e.g.*, *iPhone SE*, APPLE, https://www.apple.com/iphone-se/specs/ (last visited Feb. 22, 2021); *Galaxy S10*, SAMSUNG, https://www.samsung.com/us/mobile/galaxy-s10/design (last visited Sept. 19, 2019).

or her face.[6] The phone then saves and stores this biometric information.[7]

Indeed, a person's phone is no longer just a contact book and a device to make calls. Now, it is also a repository of a person's intimate information—including emails, photos, and even essential documents. This development led to decisions, such as *Riley v. California*[8] and *Carpenter v. United States*,[9] wherein the Supreme Court held that the increase in intimate information contained in a phone, similar to that found on a computer, made warrantless searches of phones unconstitutional absent particular circumstances.[10] The Supreme Court's stance in the two opinions, both authored by Chief Justice Roberts, that mobile devices deserve increased protection has led to a dispute over the extent to which a suspect's phone and its contents are legally protected.[11]

Riley touches upon certain aspects of this dispute.[12] But *Riley*'s holding was narrow, only covering a specific exception to the Fourth Amendment.[13] So while the Court emphasized a need for additional privacy protections under the Fourth Amendment,[14] the extent and scope of said protections appear to be mostly lip service. Subsequently, in *Carpenter*, the Court reiterated much of *Riley*'s rhetoric and analysis.[15] But neither opinion provided a clear framework to the inclusion and compulsion of biometric features, except for the broad stroke analysis that phones should have some form of increased protection.

---

[6] *iPhone 11*, APPLE, https://www.apple.com/iphone-11/specs/ (last visited Mar. 21, 2021); *Use Facial Recognition Security on Your Galaxy Phone*, SAMSUNG, https://www.samsung.com/us/support/answer/ANS00062630 (last visited Mar. 10, 2021).

[7] Curtis Moldrich, *What Is Apples Touch ID and How Does It Work*, TELEGRAPH (Oct. 16, 2014, 4:19 PM), https://www.telegraph.co.uk/technology/apple/11167454/What-is-Apples-Touch-ID-and-how-does-it-work.html.

[8] 573 U.S. 373 (2014).

[9] 138 S. Ct. 2206 (2018).

[10] *See Riley*, 573 U.S. at 403. A more thorough explanation of *Riley* and its impact appears below. *See infra* Section IV.A.

[11] *See id.* at 378; *Carpenter*, 138 S. Ct. at 2214. The composition of the Court changed from *Riley* to *Carpenter*, as Justice Scalia passed and Justice Gorsuch filled his seat.

[12] *See Riley*, 573 U.S. at 401–03 (holding that the officer's warrantless search was invalid).

[13] *Id.* at 402 (regarding the context of a warrantless search and the search incident to a lawful arrest exception).

[14] *Id.* at 395 ("[T]here is an element of pervasiveness that characterizes cell phones but not physical records. . . . Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two[.]").

[15] *Carpenter*, 138 S. Ct. at 2220 (quoting *Riley*, 573 U.S. at 385) ("[C]ell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society.").

Consequently, lower courts have looked to the Fifth Amendment as a possible source of a resolution.[16] Further, state supreme courts have begun weighing in, creating a 2-2 split as to what protections the Fifth Amendment provides.[17] Courts have not come to a consensus on what protections the Fourth and Fifth Amendments afford defendants when law enforcement seeks to compel the production of encrypted or biometric information.[18] In short, the situation is a mess.[19]

This Comment addresses whether a person can be compelled in a search warrant or court order to open their phone using their biometric information, and how courts are analyzing this question under both the Fourth and Fifth Amendments. Further, it posits that a court's use of the Fifth Amendment's Self-Incrimination Clause to answer this question is improper and undermines the Fourth Amendment's purpose. Part II of this Comment describes the purpose and history of the Fourth and Fifth Amendments. Part III discusses the technology used for biometrics and how law enforcement has used this technology. Part IV then discusses the Supreme Court's Fourth Amendment jurisprudence regarding technology in *Riley* and *Carpenter* and how these cases may suggest the Supreme Court's direction on these issues. Then, it provides a brief overview of the recent state supreme court split on compelled biometric information and some scholarship surrounding the issue. Part V discusses the implications of state supreme and lower federal courts' respective applications of relevant case law and the issues at stake. This Comment concludes that the U.S. Supreme Court's failure to provide a clearer framework has led to confusion and inconsistency. Analyzing the inclusion of a person's biometric features in a search warrant ultimately invokes privacy considerations, and the Fifth Amendment is ill-suited for the analysis. But in the absence of guidance from the Supreme Court, courts should adhere to the warnings provided in *Riley*

[16] *See, e.g.*, United States v. Barrera, 415 F. Supp. 3d. 832, 838–42 (N.D. Ill. 2019) (applying the Fifth Amendment to uphold a search warrant compelling the use of a person's biometric information); United States v. Maffei, No. 18-CR-00175, 2019 WL 1864712, at *7 (N.D. Cal. Apr. 25, 2019) (same).

[17] State v. Pittman, 479 P.3d 1028 (Or. 2021); State v. Andrews, 234 A.3d 1254 (N.J. 2020); Seo v. State, 148 N.E.3d 952 (Ind. 2020); Commonwealth v. Davis, 220 A.3d 534 (Pa. 2019); Commonwealth v. Jones, 117 N.E.3d 702 (Mass. 2019).

[18] *Compare Barrera*, 415 F. Supp. 3d. at 842 (upholding a search warrant that compelled the use of a person's biometric information relying on the Fifth Amendment), *with* United States v. Wright, 431 F. Supp. 3d 1175, 1188 (D. Nev. 2020) (holding a warrant that compelled a person's biometric features violated the Fifth Amendment).

[19] Orin Kerr, *The Law of Compelled Decryption is a Mess: A Dialogue*, REASON (Aug. 10, 2020, 11:36 PM) [hereinafter Kerr, *A Dialogue*], https://reason.com/volokh/2020/08/10/the-law-of-compelled-decryption-is-a-mess-a-dialogue (writing that the New Jersey's recent decision in *State v. Andrews* left him "unable to say what the law is").

and *Carpenter* and treat technology, and in turn, biometric information, with heightened protection.

II. CONSTITUTIONAL FOUNDATION

A. *Fourth Amendment: Origins and Purpose*

The purpose of the Fourth Amendment is to curb government intrusion and protect citizens' privacy. The Fourth Amendment states that people have the right

> 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.[20]

At a bare minimum, the Fourth Amendment maintains that citizens have the right not to be subjected to unreasonable searches and seizures.[21] As for warrants, the text dictates that searches and seizures must be justified by probable cause and not be generalized, but rather particularized as to what is to be searched.[22] Some have interpreted the Warrants Clause, and the Fourth Amendment as a whole, to limit the power of police to search persons or places.[23] But determining the exact scope of the Fourth Amendment is a tricky task.[24]

The Fourth Amendment grew out of the American Colonies' aversion to British search and seizure practices, primarily with British use of "writs of assistance" and "general warrants."[25] Before the Bill of Rights, many state constitutions viewed the warrant "as an enemy, not a friend."[26] This outright hatred of the warrant led to a series of challenges with the common theme of protecting citizens from "arbitrary government intrusion" and preventing government abuse of

---

[20] U.S. CONST. amend. IV.

[21] *Id.*

[22] *Id.*

[23] *See* Blane Michael, *Madison Lecture: Reading the Fourth Amendment: Guidance from the Mischief That Gave It Birth*, 85 N.Y.U. L. REV. 905, 921–22 (2010).

[24] Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 757 (1994) (calling today's Fourth Amendment jurisprudence "an embarrassment").

[25] Michael, *supra* note 23, at 907–09. A writ of assistance allowed an officer to "search any place on nothing more than his own (subjective) suspicion." *Id.* at 907–08. While a general warrant similarly allowed officers "to search unspecified places or to seize unspecified persons." *Id.* at 909.

[26] Amar, *supra* note 24, at 774 (quoting TELFORD TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 41 (1969)).

this power.[27] But these challenges ultimately failed, and, as a result, the combined effect of the failed challenges gave officers carte blanche to search persons or places.[28]

Thus, the Framers established the Fourth Amendment with two vital protections: (1) freedom from unreasonable searches and (2) a requirement that any warrant must be supported by probable cause, oath or affirmation, and properly particularized to what is being searched.[29] Yet, judges and scholars have conflicting opinions on whether the Fourth Amendment establishes two separate protections (unreasonable search protection and warrant protection) or one general protection (where the absence of a warrant generally creates an unreasonable search).[30]

Professor Akhil Amar explains that the framers intentionally separated the Reasonableness and Warrants Clauses to delineate the proper analysis of police searches.[31] Professor Amar posits that the Fourth Amendment makes clear that *warrants* are not the measure of a proper search; the proper question is whether the search is reasonable.[32] Therefore, even if there is a "valid" warrant, it is still unlawful "if the underlying search or seizure it would authorize would be unreasonable."[33] The Framers included this limit to prevent any potential abuses from judges issuing warrants, who are ultimately a part of the government that the Fourth Amendment serves to check against.[34] The Warrant Clause only stipulates when a warrant is appropriately issued—not that the presence of a warrant establishes the search is presumptively reasonable, as some suggest.[35]

Thus, the "judge" of a reasonable search needs to be a jury, so a genuinely independent body steers the inquiry.[36] Revolution-era judges viewed warrants as indemnifying the searcher, not serving as a protection for a searched citizen, which further supports this

---

27 Michael, *supra* note 23, at 909–11.

28 *See id.* at 910–11.

29 *See* U.S. CONST. amend. IV.

30 *Compare* Amar, *supra* note 24, at 762–70 (arguing that the absence of a warrant during a search is not per se unreasonable, despite the Supreme Court insistence that there is a warrant requirement), *with* Mincey v. Arizona, 437 U.S. 385, 390–91 (1978) (evaluating a search's reasonableness by asking first if the Government satisfied the warrant requirement), *and* Coolidge v. New Hampshire, 403 U.S. 443, 454–55 (1971) (same).

31 *See* Amar, *supra* note 24, at 775, 782.

32 *Id.* at 801.

33 *Id.* at 774.

34 *Id.* at 773.

35 *Id.* at 774.

36 *Id.*

proposition.[37] And jury determinations of reasonableness ensured proper judicial review of any search because the standard of review was less deferential than a question of whether there was probable cause for a warrant, as determined by a judge.[38]

But, in practice, the Supreme Court has approached the two clauses as connected with the presence of a valid warrant insulating the search.[39] As such, Professor Amar's history of the Fourth Amendment may serve as more of an alternative theory. It remains notable because it shows that, when evaluating a search, any inquiry ultimately comes down to the reasonableness of the search.[40]

B. *The Fifth Amendment and the Self-Incrimination Clause's Origins and Purpose*[41]

At first blush, it may seem odd to discuss the Fifth Amendment when the focus of this Comment is the Fourth Amendment. But often, evaluating a Fourth Amendment challenge implicates an analysis of the Fifth Amendment; therefore, it is necessary to discuss the origin of the Fifth Amendment as well.[42] Similar to the Fourth Amendment, the Fifth Amendment derives from the Framers' unwillingness to grant law enforcement unrestrained powers to prosecute defendants.[43]

The Self-Incrimination Clause states, "No person . . . shall be compelled to be a witness against himself."[44] Commentators differ as to where exactly the purpose of this clause originates; some claim that it was a product of an "outgrowth of the epochal change in criminal procedure . . . as defense counsel entered the criminal courts,"[45] while others suggest it was a result of the convergence of competing criminal procedural considerations.[46] As a result, "the Fifth Amendment is an

---

[37] *See* Amar, *supra* note 24, at 779.

[38] *See id.* at 774.

[39] *See* JOHN KIP CORNWELL, THE GLANNON GUIDE TO CRIMINAL PROCEDURE 69 (Wolters Kluwer ed., 4th ed. 2019) ("Generally speaking, unless an exception applies . . . police officers need a warrant[.]").

[40] *See* Amar, *supra* note 24, at 774.

[41] For purposes of this Comment, there will only be a brief overview of the history of this Amendment and the Self-Incrimination Clause.

[42] *See* Michael S. Pardo, *Disentangling the Fourth Amendment and the Self-Incrimination Clause*, 90 IOWA L. REV. 1857, 1858–59 (2005); *see also In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1018 (N.D. Cal. 2019) (applying both Fourth and Fifth Amendment analyses).

[43] *See* Eben Moglen, *Taking the Fifth: Reconsidering the Origins of the Constitutional Privilege Against Self-Incrimination*, 92 MICH. L. REV. 1086, 1086 (1994).

[44] U.S. CONST. amend. V.

[45] *See* Moglen, *supra* note 43, at 1088.

[46] *See id.*

unsolved riddle of vast proportions."[47] Regardless of its precise origin, it is clear that Americans recognized limits on prosecutorial power, including preventing testimony through coercion.[48]

The U.S. Supreme Court has held that the Self-Incrimination Clause is a "protection against the prosecutor's use of incriminating information derived directly or indirectly from the compelled testimony [of a suspect]."[49] This protection is a reflection of the country's "'unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt' that defined the operation of the Star Chamber, wherein suspects were forced to choose between revealing incriminating private thoughts and forsaking their oath by committing perjury."[50] While the purpose of the Self-Incrimination Clause may be somewhat unclear, the practical protections evince an intent to limit prosecutorial power.

The Supreme Court has held that there are three elements of the Self-Incrimination Clause's protection: compulsion, incrimination, and testimony.[51] Compulsion has a malleable definition, but generally prohibits someone from serving as a witness against himself and the "extortion of information from the accused himself that offends our sense of justice."[52] Incrimination refers to information that would expose an individual to a criminal charge.[53] Testimony is a more complicated issue, especially considering the growth of technology and how the types of information have continually changed. But Supreme Court precedent refers to testimony as "diclos[ing] the contents of [the criminal defendant's] own mind."[54] Justice Holmes explained that this protection means there is a "prohibition of the use of . . . compulsion to extort communications from [the witness], not an exclusion of his body as evidence."[55]

---

47 Akhil Reed Amar & Renée B. Lettow, *Fifth Amendment First Principles: The Self-Incrimination Clause*, 93 MICH. L. REV. 857, 857 (1995).

48 Moglen, *supra* note 43, at 1118.

49 United States v. Hubbell, 530 U.S. 27, 38 (2000).

50 Pennsylvania v. Muniz, 496 U.S. 582, 596 (1990) (quoting Doe v. United States, 487 U.S. 201, 212 (1998)).

51 Caren Myers Morrison, *The Intersection of Facebook and the Law: Symposium Article: Passwords, Profiles, and the Privilege Against Self-Incrimination: Facebook and the Fifth Amendment*, 65 ARK. L. REV. 133, 144 (2012).

52 Couch v. United States, 409 U.S. 322, 328 (1973).

53 Morrison, *supra* note 51, at 144.

54 *Id.* at 145 n.48.

55 Holt v. United States, 218 U.S. 245, 252–53 (1910).

Taken together, the Self-Incrimination Clause can serve as a powerful barrier to admitting certain statements from a suspect. Consequently, the Fourth Amendment demonstrates the American people's hesitance in granting law enforcement broad powers. History shows that as technology develops and the number of tools available to law enforcement increases, a need arises to reconsider these constitutional protections.

III. TECHNOLOGY AND ITS INFLUENCE ON LAW ENFORCEMENT

Technology has had a profound impact on the protections afforded to Americans in the context of an arrest. When James Madison proposed the Bill of Rights, the technology available to police officers would have been inconceivable. This is why, as our reliance on technology has increased, personal privacy has become an increasingly vital concern.[56] This is especially true in the wake of something like the Facebook-Cambridge Analytica scandal.[57] The fallout from the scandal demonstrates the increased pressure on companies to guarantee that information is not freely accessed without the proper protections.[58] Thus, considering the profoundly intimate information on a person's phone, users benefit from the smartphones' privacy protections. This Part sets forth the current biometric protections in smartphones and provides some modern examples of the privacy implications at play to establish this issue's precarious nature.

A. *Smartphones and the Evolution of Passcodes*

Passcodes used to open a smartphone are generally four- or six-digit numerical personal identification numbers (PINs) or alphabetical codes.[59] But these security measures do not provide absolute protection

[56] *See, e.g.*, *Privacy*, APPLE, https://www.apple.com/privacy (last visited Dec. 22, 2020) ("Privacy is a fundamental human right."); Rebecca Heilwell, *Jeff Merkley and Bernie Sanders Have a Plan to Protect You from Facial Recognition*, VOX (Aug. 4, 2020, 2:00 PM), https://www.vox.com/recode/2020/8/4/21354053/bernie-sanders-jeff-merkley-national-biometric-information-privacy-act (the proposed act "would require private companies and corporations to get written consent from people in order to collect their biometric data").

[57] *See generally* Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. In 2018, the New York Times and other news outlets discovered a data breach of millions of Facebook users whose information was harvested and then sold by the former political consulting firm, Cambridge Analytica. *Id.*

[58] *See id.*

[59] *See Smart Phone Thefts Rose to 3.1 Million in 2013*, CONSUMER REPS. (May 28, 2014, 4:00 PM), http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-

to the information in the device, as both four-digit and six-digit PINs can be hacked within a matter of hours.[60] Therefore, it is logical for smartphone users to recognize that their information is potentially vulnerable and be increasingly conscious of protecting their phones. This awareness helps explain the implementation of stricter measures to protect phones, such as biometric passcodes.

Biometrics are unique biological characteristics used to "verif[y] the identity of a human being."[61] They are increasingly replacing PINs, which are less secure.[62] A smartphone using a biometric passcode should only open for the phone's actual owner after verifying the physical feature registered with the phone.[63] Apple popularized biometric passwords in 2013 when Apple released its iPhone 5s.[64] Apple equipped the phone with "Touch ID," which allowed users to unlock their phones with a fingerprint.[65] Touch ID allowed users to have a more secure passcode than the traditional four or six-digit PIN, with the added convenience of just touching a button.[66] Fingerprints are unique to each person, and they are more unique than a person's DNA.[67] Theoretically, this ensures that a person's phone can only be opened by their unique touch.

rose-to-3-1-million-last-year/index.htm (observing that the most commonly used passcode was a four-digit PIN).

60 *See, e.g.*, Robert Hackett, *How Long It Takes to Break a Passcode*, FORTUNE (Mar. 18, 2016, 4:50 PM), http://fortune.com/2016/03/18/apple-fbi-iphone-passcode-hack (showing the average times to hack alphabetical or numerical passcodes).

61 Colin Soutar et al., *Biometric Encryption, in* ISCA GUIDE TO CRYPTOGRAPHY 650 (Randall K. Nichols ed., 1999), http://www.cse.lehigh.edu/prr/Biometrics/Archive/Papers/BiometricEncryption.pdf.

62 *See* Heather Kelly, *5 Biometric Alternatives to the Password*, CNN (Apr. 4, 2014, 5:07 PM), http://www.cnn.com/2014/04/04/tech/innovation/5-biometrics-future.

63 *See, e.g.*, *About Face ID Advanced Technology*, APPLE, https://support.apple.com/en-us/HT208108 (last visited Feb. 13, 2020) (explaining the Face ID system).

64 *See* Press Release, APPLE, *Apple Announces iPhone 5s—The Most Forward-Thinking Smartphone in the World* (Sept. 10, 2013), http://www.apple.com/newsroom/2013/09/10Apple-Announces-iPhone-5s-The-Most-Forward-Thinking-Smartphone-in-the-World.

65 *Id.*

66 *See id.*

67 *See* Khidr Suleman, *How Secure Is Apple's Touch ID?*, IT PRO (Oct. 8, 2013), http://www.itpro.co.uk/mobile/20728/how-secure-apples-touch-id. An identical set of fingerprints has yet to be discovered. Anahad O'Connor, *The Claim: Identical Twins Have Identical Fingerprints*, N.Y. TIMES (Nov. 2, 2004), https://www.nytimes.com/2004/11/02/health/the-claim-identical-twins-have-identical-fingerprints.html.

But biometric passcodes did not stop at fingerprints, as Apple released their iPhone X in 2017 and introduced "Face ID."[68] This allowed users to save the dimensions of their faces to unlock their phones.[69] This creates a three-dimensional scan to compare a user's face and unlock the phone.[70] This technology is so advanced that between Face ID and Touch ID (and other brands' equivalent features), it is near impossible to unlock a phone without the proper scan.[71]

B. *Abuses of Facial Recognition Technology and Privacy Issues at Stake*

Despite the rapid development of technology and the public's excitement over the convenience it brings, a concern arises when law enforcement uses technology for policing. For example, California legislators recently struck down a law that allowed police departments to use facial recognition software in body cameras worn by police officers.[72] Legislators were concerned over citizens' privacy and that the technology available was not reliable enough.[73] This concern over privacy in the digital age has led to a more critical eye from the general public on private companies and users' information.[74]

---

[68] Press Release, APPLE, *The Future is Here: iPhone X* (Sept. 12, 2017), https://www.apple.com/newsroom/2017/09/the-future-is-here-iphone-x.

[69] *See* Andy Greenberg, *How Secure is the iPhone X's FaceID? Here's What We Know*, WIRED (Sept. 12, 2017, 5:08 PM), https://www.wired.com/story/iphone-x-faceid-security.

[70] *Id.*

[71] *Id.*

[72] Rachel Metz, *California Lawmakers Ban Facial-Recognition Software from Police Body Cams*, CNN, https://www.cnn.com/2019/09/12/tech/california-body-cam-facial-recognition-ban/index.html (last updated Sept. 13, 2019).

[73] *Id.* ("Studies have shown, for instance, that the technology is worse at accurately identifying women and people of color."). This article may be underselling the inaccuracies, as the Detroit Police Chief recently announced the recognition software misidentifies someone 96% of the time. Jason Koebler, *Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time*, VICE (June 29, 2020, 12:56 PM), https://www.vice.com/en_us/article/dyzykz/detroit-police-chief-facial-recognition-software-misidentifies-96-of-the-time.

[74] Notably, Senator Jeff Merkley and Senator Bernie Sanders have proposed a bill to regulate the biometric information companies can collect from their consumers. Rebecca Heilweil, *Jeff Merkley and Bernie Sanders Have a Plan to Protect You From Facial Recognition*, VOX (Aug. 4, 2020, 2:00 PM), https://www.vox.com/recode/2020/8/4/21354053/bernie-sanders-jeff-merkley-national-biometric-information-privacy-act.

Examples of the abuses of facial recognition technology have led to a variety of consequences. China, which is among the world's leaders in monitoring its citizens,[75] recently required anyone who registers a mobile phone to submit to facial scans.[76] The justification for this increased surveillance and use of technology is similar to that in the United States—better protecting its citizens.[77] In Xinjiang, home to China's internment camps for the Uighar Muslim population, there are cameras and police checkpoints about every 150 feet.[78] Chinese police use these cameras to monitor citizens, cross-reference their faces, and search citizens' phones.[79] The goal is to help Chinese police find Uighurs who practice their faith and then send them to reeducation camps.[80] Despite the potential "benefits," the dangers of this type of surveillance state are clear.

Even in less extreme examples, justifying a surveillance system (even in a limited capacity) to protect citizens can lead to drastic consequences. In 2019, New Jersey police officers arrested Nijeer Parks for "shoplifting candy and trying to hit a police officer with a car."[81] Police identified Mr. Parks solely using facial recognition technology, despite him being thirty miles away from the crime scene.[82] Mr. Parks was held in jail for ten days, and eventually all charges were dismissed for lack of evidence.[83] Law enforcement often justifies their use of facial recognition technology by claiming that the technology was just another tool used in the larger investigation.[84] In practice, however, a match in

---

75 Paul Bischoff, *Surveillance Camera Statistics: Which Cities Have the Most CCTV Cameras?*, COMPARITECH, https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities (last updated July 22, 2020).

76 James Griffiths, *China is Rolling Out Facial Recognition for All New Mobile Phone Numbers*, CNN (Dec. 2, 2019 4:52 AM), https://www.cnn.com/2019/12/02/tech/china-facial-recognition-mobile-intl-hnk-scli/index.html.

77 *See id.*

78 Matt Rivers & Lily Lee, *Security Cameras and Barbed Wire: Living Amid Fear and Oppression in Xinjiang*, CNN, https://www.cnn.com/2019/05/08/asia/uyghur-xinjiang-china-kashgar-intl/index.html (last updated May 9, 2019, 6:48 PM).

79 *Id.*

80 Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, N.Y. TIMES (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.

81 Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES (Dec. 29, 2020), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

82 *See id.*

83 *Id.*

84 *Id.* ("[I]t is used only as a clue in a case and will not lead directly to an arrest.").

the software can be the *only* evidence to link a suspect to a crime and lead to false arrests.[85]

Despite these overwhelming privacy concerns, courts still have often deferred to law enforcement and the benefits of technology. As discussed below, Supreme Court precedent and lower courts' treatment of technology and access to biometric information demonstrate this deference.

IV. LEGAL PRECEDENT AND BIOMETRIC INFORMATION

Federal appellate litigation concerning biometrics and constitutional protections has been sparse; however, in a recent line of Fourth Amendment cases, the Supreme Court has given some indication on how technology and privacy protections interact and the type of framework it could use for analysis. But despite some lofty declarations from the Supreme Court, there remains some doubt as to the Fourth Amendment adequacy in protecting a person's face or other features, if included in a search warrant. Consequently, courts have looked to the Fifth Amendment and the Self-Incrimination Clause as a means of protection. This Part focuses on this recent case law and attempts to delineate the principles guiding the Supreme Court's opinions through its recent opinions concerning cell phones and the Fourth Amendment. Then, it discusses an emerging split among state supreme courts concerning compelled decryption. Finally, it explains how magistrate judges are dealing with this issue, in practice.

A. *Cell Phones and the Fourth Amendment:* Riley v. California *and* Carpenter v. United States

Riley v. California[86] and *Carpenter v. United States*[87] may appear like resounding victories for personal privacy in the modern era. And in some ways the decisions are; the Supreme Court concretely recognized in both decisions that the cell phone is now almost a "feature of human anatomy."[88] *Riley* illustrated how the Supreme Court weighs privacy concerns in the wake of cell phones and that traditional Fourth Amendment doctrine could not easily dictate the analysis.[89] *Carpenter* continued this trend and also declined to apply previous Fourth

85 *See id.*
86 573 U.S. 373 (2014).
87 138 S. Ct. 2206 (2018).
88 *Riley*, 573 U.S. at 385.
89 *See id.* at 385–91 (declining to extend *Chimel* and *Robinson* to cover cell phones).

Amendment principles to modern technology.[90] But ultimately, it is not easy to discern how far these opinions go. It would be easy to characterize both opinions narrowly, as courts have done. This Section outlines the two opinions and highlights that while they may patently appear like victories for privacy, the two opinions leave far too many questions for lower courts to answer.

1. *Riley v. California*

In 2014, the defendant in *Riley v. California* challenged the search of his smartphone incident to arrest.[91] *Riley* showed that the Supreme Court recognizes that privacy concerns are more apparent in the wake of technological developments like these new minicomputers in everyone's pocket.[92] The case began with a traffic stop, where an officer discovered that the driver had been driving with a suspended license.[93] This prompted the officer to conduct a full search of the driver incident to the arrest, during which the officer seized the driver's phone from his pants pocket.[94] The officer went through the phone and found some indications that the driver was associated with the "Bloods" street gang.[95] After an additional search of the phone, the officer discovered evidence linking the driver to a previously unsolved shooting. The driver was ultimately indicted for the shooting and a related weapons charge, and in turn, found guilty of the crimes charged. After the Supreme Court of California declined to hear the case, the Supreme Court granted certiorari.[96]

The Court attempted to balance the privacy interests at stake with the legitimate government interest in solving crime.[97] But the Court decided to depart from the traditional Fourth Amendment analysis because of the difference between physical objects, such as a car or a coat, and digital objects, such as photos and texts saved onto a phone.[98] Digital objects stored on a phone diminished the usual considerations of

[90] *Carpenter*, 138 S. Ct. at 2216–17 (declining to extend *Smith* and *Miller*, cases concerning the "third-party doctrine," to the circumstances here).

[91] *Riley*, 573 U.S. at 378. This categorical exception to the warrant requirement allows for a contemporaneous search of a person incident to a lawful arrest. *See* United States v. Robinson, 414 U.S. 218, 235 (1973).

[92] *See Riley*, 573 U.S. at 395, 401.

[93] *Id.* at 378.

[94] *Id.* at 378–79.

[95] *Id.*

[96] *Id.* at 380.

[97] *Id.* at 407.

[98] *Riley*, 573 U.S. at 400–01.

officer safety and evidence preservation.[99] The Government failed to show, besides some anecdotal examples, that a normal arrest would prompt either consideration.[100] Further, the suspect's usual diminished expectation of privacy during a search does not apply to a cell phone search because a cell phone is much more expansive and includes "vast quantities of personal information."[101] Applying this framework, the Court held that the privacy issues presented by a cell phone and its contents outweighed the cost to law enforcement in preventing the search.[102]

Notably, though, Chief Justice Roberts made clear that a search warrant could include the searched information (the contents of one's phone).[103] Additionally, law enforcement can use the same technology that creates this protection to obtain warrants quickly enough to protect the Government's interests.[104] *Riley* marked a transition in the Court's treatment of technology and the Fourth Amendment. Before *Riley*, it was unclear whether the Supreme Court was prepared to square Fourth Amendment precedent with digital information's unique nature. The *Riley* Court, with a near-unanimous majority, acknowledged that digital data deserves a different level of privacy protection than physical data.[105] But just as quickly as the Court announced these principles, the Court included enough caveats to hollow out the opinion.[106]

2. *Carpenter v. United States*

The Court followed up these lofty statements of just how intimate information on a cell phone is in *Carpenter v. United States.*[107] There, the concern was over cell site location information ("CSLI"), which is effectively an imprecise GPS monitoring system.[108] In 2011, officers

99 *Id.* at 405 (Alito, J., concurring).

100 *See id.* at 387–90 (majority opinion) ("[N]either the United States nor California offers evidence to suggest that their [safety] concerns are based on actual experience. . . . We have also been given little reason to believe [remote wiping] is prevalent. The briefing reveals only a couple of anecdotal examples of remote wiping triggered by an arrest.").

101 *Id.* at 386.

102 *Id.* at 386, 401.

103 *See id.* at 401.

104 *Riley*, 573 U.S. at 401.

105 *Id.* at 400–01. Justice Alito's concurrence did express some doubt to the majority's analysis; however, he appeared more concerned that the legislature needed to step in and dictate the proper protections. *Id.* at 407–08 (Alito, J., concurring).

106 *Id.* at 401 (majority opinion) ("Our holding, of course, is not that the information on a cell phone is immune from search . . . a warrant is generally required[.]").

107 138 S. Ct. 2206 (2018).

108 *See id.* at 2211–12.

compelled disclosure of certain telecommunication records for a four-month period, during which a string of robberies had occurred.[109] Using this information, officers were able to charge the suspect with robbery.[110] On appeal, the question was if this data collection even amounted to a search under the Fourth Amendment.[111] The Court ultimately found that collecting CSLI data did constitute a search and remanded the case to determine whether the search was reasonable.[112]

Chief Justice Roberts harped on the pervasive role cell phones play in current society, as he did in *Riley*.[113] Further, Fourth Amendment precedent is difficult to rely on because when these cases were decided, "few could have imagined a society in which a phone goes wherever its owner goes, conveying . . . a detailed and comprehensive record of the person's movements."[114] Much like in *Riley*, the Court noted how technology has changed society and that these types of questions do not fit neatly into Fourth Amendment analysis. Yet, what *Carpenter* means in practice is unclear, as the Court held that the vast amount of information obtained in *Carpenter* would not be allowed, but did not establish clear parameters for what would be allowed.

On their face, *Riley* and *Carpenter* appear to be big shifts in how courts treat technology under the Fourth Amendment. But, as discussed below, these opinions seem to be more narrowly interpreted and, as such, are seemingly more lip service than prescient protection.

B. *The Fifth Amendment as a Source of Potential Resolution or Further Confusion?*

At the outset, it is important to note that while this Comment concerns the Fourth Amendment, the Supreme Court has tried to clarify that the Fourth and Fifth Amendments are independent of each other. But often, a Fourth Amendment question implicates the Fifth Amendment as well.[115] So, it is necessary to evaluate what protections the Fifth Amendment provides. Thus far, only one state supreme court has determined if compelled biometric information is protected under

109 *Id.* at 2212.

110 *Id.*

111 *Id.* at 2211.

112 *Id.* at 2222–23.

113 *See Carpenter*, 138 S. Ct. at 2220 (Roberts, C.J.) (referencing his prior opinion in *Riley*, Chief Justice Roberts stated that cell phones are "indispensable to participation in modern society").

114 *Id.* at 2217.

115 *See* Pardo, *supra* note 42, at 1858–59.

the Fifth Amendment, and that court ruled that it is not.[116] As discussed below, lower federal courts have been inconsistent in this area.[117] This Section looks at how courts have applied the Fifth Amendment to compelled encryption, as a general matter, for possible insight into the proper framework for compelled biometric. In turn, this Section explains that the split only further complicates the analysis of compelled *biometric* passcodes,[118] as demonstrated by a developing state supreme court split. This Section concludes with some recent scholarship theorizing how the Supreme Court may rule on compelled decryption and what that may mean for compelled biometrics.

States have begun weighing in on compelled decryption,[119] starting from a Supreme Judicial Court of Massachusetts opinion, *Commonwealth v. Jones*. These recent decisions are especially notable because they suggest that, as the split grows, the U.S. Supreme Court will review one of the decisions in the coming terms.[120] This could lead to clarification on how compelled encryption is treated under the Fifth Amendment, and possibly some suggestions on how to analyze compelled biometric information. But there are a few preliminary points to set forth before discussing the cases.

First, state supreme courts have tried to answer two questions: (1) is the password testimonial, and (2) is the Government compelling an act to learn it? If the password is testimonial and the Government is compelling an act to learn the information, the order would violate the Self-Incrimination Clause of the Fifth Amendment. If the act is non-testimonial, then the clause is not implicated at all. Further, if the Government already knows the implied speech, then the foregone

116 *See* State v. Diamond, 905 N.W.2d 870, 872 (Minn. 2018) (holding that the defendant's act of providing a fingerprint to unlock a cell phone was not testimonial communication).

117 *See*, *infra*, Section IV.C.

118 *See* Orin Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767, 768–69 (2019) [hereinafter Kerr, *Compelled Decryption*]; *see also* Kerr, *A Dialogue*, supra note 19.

119 Compelled decryption refers to when "investigators have a warrant to search a cell phone or computer, but they cannoy execute the search because the data is encrypted" by a password or passcode. Kerr, *Compelled Decryption*, *supra* note 118, at 768. Then investigators seek a "court order directing a suspect to" enter the password to open the phone. *Id.*

120 Prior to publication, the Supreme Court denied certiorari of an appeal from Pennsylvania. Commonwealth v. Davis, 220 A.3d 534 (2019), *cert. denied*, 141 S. Ct. 237 (2020). Before the denial, Professor Kerr suggested in a recent Twitter post that the Supreme Court will likely weigh in on this issue in an upcoming term but is likely looking for the right case to do so. *See* @OrinKerr, TWITTER (Sep. 25, 2020, 2:19 AM), https://twitter.com/OrinKerr/status/1309379972356743168.

conclusion doctrine applies.[121] Second, the split itself is not clear cut, as the bases for the four respective decisions differ. Thus, it could be considered two related 1-1 splits, or one 2-2 split.[122] This Comment will characterize the approaches by the four courts as two approaches: (1) the only implicit testimony when a suspect unlocks a phone is that the suspect knew the passcode, and (2) unlocking a phone implies more testimony than just knowledge of the passcode.

Thus far, Massachusetts and New Jersey have embraced the first approach to compelled decryption.[123] Under the first approach, a suspect's testimony, presented by unlocking their phone, is limited by knowledge of the passcode, placing the compulsion under the foregone conclusion doctrine.[124] Essentially, because the Government already knows the facts presented (the suspect knows their passcode), disclosing those facts does not force a suspect to incriminate themselves.[125] This is because knowing the passcode does not reveal anything about the actual contents of the device. Professor Orin Kerr[126] provides an example to illustrate this point: If a person knows their sibling's passcode, they could comply with a court order to enter the passcode. The only revelation from the passcode entry is that the person knows the passcode and can unlock the device. Thus, the contents of the device are still only known by the owner of the device.[127] The only thing the Government needs to prove to force a suspect to provide their passcode is that the suspect knows the passcode and can access the device under the foregone conclusion doctrine.[128]

---

121 The Foregone Conclusion is an exception to the Self-Incrimination Clause. Generally speaking, it is when the information compelled "adds little or nothing to the sum total of the Government's information." Fisher v. United States, 425 U.S. 391, 411 (1976). In practice, if "the facts implicitly disclosed through the act of production are already known [by the Government], they are considered a 'foregone conclusion' and do not force a defendant to incriminate himself or herself." Commonwealth v. Jones, 117 N.E.3d 702, 709 (2019).

122 *See* Orin Kerr, *Indiana Supreme Court Creates a Clear Split on Compelled Decryption and the Fifth Amendment* (June 4, 2020, 3:21 AM) [hereinafter Kerr, *Split on Compelled Decryption*], https://reason.com/volokh/2020/06/24/indiana-supreme-court-creates-a-clear-split-on-compelled-decryption-and-the-fifth-amendment.

123 *See generally* State v. Andrews, 234 A.3d 1254 (N.J. 2020); Commonwealth v. Jones, 117 N.E.3d 702 (Mass. 2019).

124 *Jones*, 117 N.E.3d at 709–10.

125 *Id.* at 709.

126 The Massachusetts Supreme Judicial Court relied on both Professor Kerr's Law Review article regarding Compelled Decryption and Professor Kerr's amicus brief in its 2019 decision. *See id.* at 711 (citing Kerr, *Compelled Decryption*, *supra* note 118).

127 Kerr, *Compelled Decryption*, *supra* note 118, at 779.

128 *Jones*, 117 N.E.3d at 710.

The Massachusetts Supreme Judicial Court, in applying this framework, held that because the state created a strong inference that the defendant knew the phone in question's passcode, compelling the defendant to open the phone did not violate the Fifth Amendment.[129] The Supreme Court of New Jersey held similarly and added a key criticism of the split's other side. The *Andrews* court noted that the other side of the split essentially conflated compelling production of the passcode with the act of producing the contents, which imports Fourth Amendment privacy principles into a Fifth Amendment inquiry.[130] Then, the Supreme Court of New Jersey held that the only compelled act of production is producing the passcodes, those passcodes have little to no testimonial value, and this production fits squarely within the foregone conclusion doctrine.[131]

The second view introduces an additional consideration: unlocking the phone not only indicates knowledge of the passcode but also recognizes that unlocking a "phone is a gateway to a treasure of potential evidence."[132] The Indiana Supreme Court and Supreme Court of Pennsylvania have supported this approach.[133]

The Indiana Supreme Court found that the documents produced are inherently linked to the compelled production of the passcode. In turn, the passcode creates two analogies: "First, entering the password to unlock the device is analogous to the physical act of handing over documents. . . . And second, the files on the smartphone are analogous to the documents ultimately produced."[134] So, any time a suspect is compelled to unlock their phone, they communicate three things: (1) they know the passcode, as suggested in the first view; (2) evidence is on the device; and (3) the suspect possesses that evidence.[135] The Supreme Court of Pennsylvania focused less on the consequences of the

129 *Id.* at 720.

130 State v. Andrews, 234 A.3d 1254, 1271, 1274–75 (N.J. 2020). It is important to note that the Supreme Court of New Jersey "views the protection against self-incrimination as incorporating privacy considerations." *Id.* at 1277.

131 *Id.* at 1274

132 Kerr, *Split on Compelled Decryption*, *supra* note 122; *see also* Laurent Sacharoff, *What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr*, 97 TEX. L. REV. ONLINE 63, 68–69 (2019) (explaining the slippery slope that opening a phone creates).

133 *See* Seo v. State, 148 N.E.3d 952, 957 (Ind. 2020); Commonwealth v. Davis, 220 A.3d 534, 545 (Pa. 2019)

134 *Seo*, 148 N.E.3d at 957.

135 *Id.*

compulsion than on the compulsion itself.[136] The court held that requiring a suspect to recall and then disclose a memorized password reveals "the contents of one's mind," and so the password is testimonial in nature.[137] While the two courts had different rationales, they reached the same conclusion that a passcode reveals more than just the fact that the suspect knows the passcode.

As mentioned before, the law surrounding compelled decryption is, quite bluntly, a mess. It is tough to reconcile that the first approach ignores the practical effects that compelling a passcode's production reveals. But it is equally difficult to ignore that the second approach is not directly rooted in current Fifth Amendment jurisprudence. Further, as Professor Kerr posits in a recent article, the U.S. Supreme Court's decision on this matter could turn on the choice of these characterizations.[138] Accordingly, there is little benefit to parsing through this muddled analysis to find the parameters for compelling production of biometric features. In fact, the Supreme Court of Pennsylvania made sure to note that its decision did not address biometric features.[139] As a result, what is left is essentially a blank slate for magistrate judges, which has exacerbated the unclear mix of approaches.

C. *The Principles in Practice and Magistrate Judges' Inconsistency*

After *Riley* and *Carpenter*, it remains unclear how biometric passcodes fit into current Fourth and Fifth Amendment protections. The Supreme Court in *Riley* outlined just how vital privacy protections are to individuals and the information on their phones.[140] Looking to recent state Supreme Court opinions on compelled decryption only complicates matters.[141] And while the Fifth Amendment seems to provide the best protection in accessing a person's phone, so long as an

---

[136] *See Davis*, 220 A.3d at 545. This situation is partially a mess because courts that tend to come to the same result are analyzing the solution from different analytical frameworks.

[137] *Id.* at 548.

[138] Orin S. Kerr, *Decryption Originalism: The Lessons of* Burr, 134 HARV. L. REV. 905, 960 (2021) [hereinafter Kerr, *The Lessons of* Burr] ("If compelled entry is treated as akin to compelled production, then it may be barred by the Fifth Amendment. If compelled entry is treated as akin to admitting knowledge of the password, then the rules for compelled entry should match those for compelled disclosure of the password.").

[139] *Davis,* 220 A.3d at 550 n.7 ("[W]e need not address the related, but distinct, area involving biometric features like fingerprints, thumbprints, iris scanning, and facial recognition, or whether the foregone conclusion rationale would be appropriate in these circumstances.").

[140] *See* Riley v. California, 573 U.S. 373, 386 (2014).

[141] *See* discussion *supra* Section IV.B.

individual strictly uses a numerical passcode, that could change with a potential Supreme Court decision on the issue. But, as this Section shows, the Fifth Amendment was not designed to protect an individual's privacy, and this protection's shortcomings are evident in recent magistrate opinions and the inconsistent analysis of this issue. The magistrate opinions analyzed in this Section present three approaches: (1) applying the Fifth Amendment in place of the Fourth Amendment; (2) applying the Fourth Amendment but focusing on solely the scope of the warrant at issue; and (3) a hybrid of the two.

1. Applying the Fifth Amendment in Place of the Fourth Amendment

Two recent opinions highlight the imperfect fit that relying on the Fifth Amendment in lieu of the Fourth Amendment creates. Both opinions ignored any privacy concerns and instead focused on whether a fingerprint is compelled information.[142]

First, on review of a magistrate decision, the District Court for the District of Idaho overruled a magistrate judge and held that the biometric information sought was a "physical characteristic."[143] Regardless of the decision, the issue was that the magistrate judge focused on and whether or not the fingerprint was a "compelled testimonial communication."[144] This approach eliminates any consideration as to whether compelled production of biometric information amounts to a reasonable search. Further, as compared to Supreme Court and federal circuit precedent, a fingerprint can be justified as a non-testimonial act, as the district court judge noted in the court's holding.[145]

Second, in *United States v. Barrera*, the magistrate judge quickly discarded any Fourth Amendment concerns because the warrant was more limited than the usual challenges, and so did not address the Fourth Amendment.[146] The challenge, much like the one in *In re Search of a White Google Pixel 3XL Cellphone in a Black Incipio Case*, concerned the Government's attempt to unlock a suspect's phone using his biometric information.[147] The analysis the *Barrera* court used is

142 *See In re* Search of a White Google Pixel 3 XL Cellphone in a Black Incipio Case, 398 F. Supp. 3d 785 (D. Idaho 2019) [hereinafter *Google Pixel*]; United States v. Barrera, 415 F. Supp. 3d 832, 833 (N.D. Ill. 2019).

143 *Google Pixel*, 398 F. Supp. 3d at 793.

144 *Id.* at 790.

145 *See id.* at 793–94.

146 *Barrera*, 415 F. Supp. 3d at 835, 835 n.1.

147 *Id.* at 833–34.

notable. The court assessed three considerations in evaluating the Fifth Amendment protections: (1) whether biometric information is closer to a key than a combination; (2) whether biometric information is more physical than testimonial; and (3) whether the implicit inferences from the biometric information can be considered testimonial.[148] Following precedent, the court found clearly established that a fingerprint is more analogous to a physical key, especially in the context of using a fingerprint to open a phone.[149] Additionally, the court found that because a suspect is not reciting any words and the Government is dictating the compulsion, the process used none of the suspect's thoughts.[150] Finally, the court found that the information provided by compelled production of biometric features was not enough to warrant the implicit inference of identifying the phone as someone's property because up to five different fingerprints can be programmed.[151]

The magistrate judge also explicitly referenced *Riley v. California* and summarized why the magistrate could not rely on the Fifth Amendment for privacy protection.[152] The court recognized that old analogies are not nearly as applicable as they once were; however, there is no Fourth Amendment protection under typical Fifth Amendment analysis, and *Riley* never addressed these same privacy concerns.[153] Therefore, the court found that any broader interpretation of the Fifth Amendment would diminish the purpose of the Fourth Amendment because limiting access to evidence is squarely within the Fourth Amendment's parameters.[154]

This type of analysis is not limited to just these two courts[155] and shows how easy it can be to justify compelling production of a person's biometric information via the Fifth Amendment.

2. Applying the Fourth Amendment

In re Search of is one of the few cases that considers the Fourth Amendment in its analysis. The warrant at issue sought "any" evidence in cell phones and computers found upon the premises.[156] This included

148 *Id.* at 838–39.

149 *Id.* at 839.

150 *Id.* at 840.

151 *Id.* at 841.

152 *See Barrera*, 415 F. Supp. 3d at 842.

153 *Id.*

154 *Id.*

155 *See, e.g.*, United States v. Maffei, No. 18-CR-00175-YGR-1, 2019 WL 1864712, at *7 (N.D. Cal. Apr. 25, 2019) (holding that compelling the defendant to unlock their phone via biometric information did not violate the Fifth Amendment).

156 *In re* Search of, 317 F. Supp. 3d 523, 525–26 (D.D.C. 2018).

any devices that "reasonably could contain evidence of the offenses under investigation."[157] The Government also sought an order permitting law enforcement officials to unlock any device within the scope of the warrant through the use of biometric passcodes.[158] The Government argued that obtaining an individual's physical characteristics does not infringe on their Fourth Amendment rights because compelling production of these characteristics is not an intrusion upon the individual's privacy.[159]

The court set forth a standard to analyze this issue and noted that there should be a nexus between the Government's evidence and the device trying to be searched.[160] The court held that the Government may compel the use of biometric features to unlock a device if there is reasonable suspicion the suspect committed the crime, if the procedure is "carried out with dispatch and in the immediate vicinity of the premises to be searched," and if there exists reasonable suspicion that the suspect's biometric information will unlock the device.[161] The court found all of these elements present and concluded that the Government could compel the use of biometrics to unlock any devices found at the premises.[162]

This case is interesting because the magistrate judge appeared to reinforce the principles presented in *Riley v. California*, but then upheld a warrant that allowed the use of biometrics for any device.[163] The conclusion seemingly counters the principles set forth by the magistrate judge.

3. A Hybrid Approach Using Both the Fourth and Fifth Amendments

These opinions each contain a muddled analysis. The through line in the analyses is that these courts recognize the protections that the Fourth Amendment and *Riley* afford but ultimately rely on the Fifth Amendment in their conclusions.

First, in *In re Search Warrant Application for [redacted text]*, the district court disagreed with the magistrate judge, who had held a warrant application unconstitutional because the warrant required *any* individual present to provide fingerprints to unlock any device

157 *Id.* at 525.
158 *Id.* at 525–26.
159 *Id.* at 529.
160 *See id.* at 527–28, 528 n.3.
161 *Id.* at 533.
162 *In re Search of*, 317 F. Supp. 3d at 540.
163 *See id.* at 533, 540.

discovered.[164] The court relied on Touch ID's time-sensitivity, noting that waiting could lead police to be unable to unlock the phone using Touch ID through several ways, such as a 48-hour wait period since last unlocking the phone, someone remotely locking the phone, or the phone turning off and being restarted.[165] After balancing the interests at stake, the court found that compelling the use of biometrics was reasonable.[166] Further, the court noted "the intensity of the privacy interests at stake in accessing smart devices,"[167] and found that "although *Riley* certainly instructs courts to avoid mechanical application of legal principles in the face of technological advances, the constitutional text dictate[d]" upholding the warrant.[168]

But the court, confusingly, did not rely on the Fourth Amendment in its conclusion and explicitly did not address it.[169] Instead, the *Matter of Search Warrant* court upheld the warrant because the compelled production of biometric information was not self-incriminating under the Fifth Amendment.[170]

This hybrid approach has led to inconsistent results, as a similar case with similar analysis led to the opposite conclusion. In *In re Residence in Oakland, California*, the Government sought a warrant to seize electronic devices and "to compel any individual present . . . to press a finger . . . or utilize other biometric features." to unlock those found devices.[171] The court in this case also noted the breadth of the information sought and that any search would need to be much more limited to comply with the Fourth Amendment.[172] In its Fifth Amendment analysis, the court disagreed that using a fingerprint to unlock a device was akin to fingerprinting in the booking process for two reasons.[173] First, the fingerprint here replaced a passcode; therefore, the fingerprint should be treated as a passcode because they are functionally equivalent.[174] Second, compelling someone to use their fingerprint on a device served to identify the owner of that device.[175]

164 *See In re* Search Warrant Application, 279 F. Supp. 3d 800, 801–02 (N.D. Ill. 2017).
165 *See id.*
166 *Id.* at 806–07.
167 *Id.* at 806.
168 *Id.* at 806–07.
169 *Id.* at 807.
170 *In re Search Warrant*, 279 F. Supp. 3d at 807.
171 *In re* Search of a Residence in Oakland, California, 354 F. Supp. 3d 1010, 1013 (N.D. Cal. 2019).
172 *Id.* at 1014.
173 *Id.* at 1015.
174 *Id.*
175 *Id.* at 1016.

This, in turn, exceeded the physical evidence created when someone submits their fingerprints for booking.[176]

A biometric feature is used "to access a database of someone's most private information." For this reason, it is closer to "physiological responses elicited during a polygraph test," which are protected under the Fifth Amendment.[177] In deciding this case, the court emphasized, relying on *Riley v. California*, that mobile phones are inherently different devices and should have stronger protection.[178] When law enforcement officers open a phone, it likely contains significantly more information than anticipated. Therefore, it could not be subject to the foregone conclusion doctrine.[179] This case illustrates many of the principles that guided the *Riley* decision; however, these principles came in the form of a Fifth Amendment protection.

This muddling is exacerbated as more courts rely on these very decisions and create a starker split, further showing a need for guidance.[180] For example, in *United States v. Wright*, the District of Nevada held a warrant unconstitutional by relying on *In re Residence in Oakland, California*.[181] But, another opinion—relying on the same cases and reasoning—found a similarly constructed warrant constitutional.[182]

V. MOVING FORWARD

Riley v. California established that the modern smartphone is more similar to a home than a telephone because of the immense amount of private information contained in it—thus, smartphones deserve increased protection under the law.[183] *Carpenter v. United States* confirmed the U.S. Supreme Court's peculiar approach concerning these devices. But now, the implications of these two cases and their broader applicability are unclear, as exacerbated by the state supreme court split regarding compelled decryption. Lower federal courts have attempted to apply the Fifth Amendment, but there are some analytical gaps inherent in using the Fifth Amendment in place of the Fourth

176 *Id.*

177 *In re Residence*, 354 F. Supp. 3d at 1016.

178 *Id.* at 1017.

179 *Id*. at 1017–18.

180 *Compare* United States v. Wright, 431 F. Supp. 3d 1175, 1188 (D. Nev. 2020) (holding that a warrant violated the Fifth Amendment by relying on the aforementioned cases in this Comment), *with In re* Search of, 317 F. Supp. 3d 523, 539–40 (D.D.C. 2018) (upholding a warrant, relying on the same cases).

181 *Wright*, 431 F. Supp. 3d at 1188 (citing *In re Residence*, 354 F. Supp. 3d at 1016).

182 *In re* Search of, 317 F. Supp. 3d at 539–40.

183 *See* Riley v. California, 573 U.S. 373, 394–97, 401 (2014).

Amendment.[184] Therefore, a few questions stem from biometric information's inclusion in search warrants: (1) are courts giving the privacy considerations outlined in *Riley* the proper deference; (2) what provides better protection, the Fourth or Fifth Amendment; and (3) which amendment *should* be used, and why?

A. *Privacy Considerations in* Riley

First, the Framers created the Fourth Amendment to prevent arbitrary and unreasonable searches.[185] *Riley* establishes that absent "exigent circumstances," the Fourth Amendment protects cell phones from warrantless searches.[186] Further, the sheer amount of personal information contained on cell phones creates a need for additional protection.[187] Therefore, there should have to be a compelling reason to grant law enforcement access to such an intimate device. Otherwise, as Justice Scalia[188] and Professor Amar suggested,[189] the freedom from unreasonable searches provided in the Fourth Amendment will be irreparably distorted.

Modern cell phones contain a multitude of intensely personal information that may or may not be related to the crime being investigated; therefore, digital data deserves an increased level of privacy protection. It can contain someone's *entire* life. The ability to access this information needs to be reasonably limited to prevent law enforcement from abusing their power. Based on *Riley* and *Carpenter*, there appears to be support for this proposition.[190] Chief Justice Roberts made clear that cell phones are "indispensable to participation in modern society."[191] Accordingly, the Court refused to apply the third-party doctrine to cell phones and their data and instead used a more protective approach.[192] But in both *Riley* and *Carpenter*, the Court made sure to show just how narrow the opinions were.[193] Consequently,

184 *See supra* Section IV.C.

185 *See* Amar, *supra* note 24, at 773, 776–77; Michael, *supra* note 23, at 921–22.

186 *Riley*, 573 U.S. 373, 402 (2014).

187 *Id.* at 386, 407.

188 *See* Maryland v. King, 569 U.S. 435, 466, 482 (2013) (Scalia, J., dissenting).

189 Amar, *supra* note 24, at 801.

190 See *supra* Section IV.A for a discussion on *Riley* and *Carpenter*.

191 Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

192 *Id.*

193 *See id.* ("Our decision today is a narrow one."); *see also* Riley v. California, 573 U.S. 373, 402 (2014) ("Our holding, of course, is not that the information on a cell phone is immune from a search[.]").

lower courts have flouted these considerations in favor of deference to governmental interest.[194]

B. *What Offers the "Better" Protection*

The Fourth Amendment, as demonstrated above, provides little protection to the inclusion of biometric information in search warrants. Therefore, defendants have most successfully relied on the Fifth Amendment to protect biometric information against unlawful seizure.[195] Among just the opinions explicitly mentioned in Part IV, five ruled that the inclusion of biometrics in a search warrant was reasonable, and two ruled their respective warrants were overbroad.[196] Among the five that ruled that there was no constitutional violation, three did not address the Fourth Amendment or its protections.[197] Even when a court found a Fourth Amendment issue, it ultimately relied on a Fifth Amendment violation to deny access to the evidence sought.[198]

But in light of recent decisions, both on the state and federal level, the Fifth Amendment's reliability in compelled biometric information is now in doubt. The recent state supreme court split will likely compel the U.S. Supreme Court to evaluate the Fifth Amendment's protection to compelled decryption. Professor Kerr suggests that any ruling on this issue would be a close call and depends on a choice of analogies.[199] Further, this seemingly minute distinction between the characterization of what law enforcement seeks to compel can be dispositive in practice.[200] And while only one state supreme court has weighed in on compelled biometric information, the court ruled the Fifth Amendment does not protect biometric information.[201] So, while the Fifth Amendment may initially appear as providing the best protection, it

194 *See, e.g.*, *In re* Search of [Redacted] Washington, D.C., 317 F. Supp. 3d 523, 533, 540 (D.D.C. 2018) (agreeing, after balancing some factors, that the government interest outweighed the defendant's and upheld the warrant).

195 *See supra* Section IV.C.

196 *See id.*

197 *See supra* Sections IV.C.2, IV.C.3.

198 *Id.*

199 Kerr, *The Lessons of* Burr, *supra* note 138, at 960 ("If compelled entry is treated as akin to compelled production, then it may be barred by the Fifth Amendment. If compelled entry is treated as akin to admitting knowledge of the password, then the rules for compelled entry should match those for compelled disclosure of the password.").

200 *See supra* Section IV.B.

201 *See generally* State v. Diamond, 905 N.W.2d 870 (Minn. 2018); *see also supra* Section IV.B (discussing a recent state Supreme Court split regarding compelled decryption).

would be difficult to trust it will remain a viable option to challenge compelled biometric information.

C. *Lower Courts Are Improperly Relying on the Fifth Amendment*

While possibly disappointing from a civil liberties perspective, the lack of constitutional protection for biometric information seems logical. The Fifth Amendment provides an imperfect framework to the question. The Supreme Court has never applied the Fifth Amendment to prevent the use of evidence that "did not involve compelled testimonial self-incrimination," [202] meaning that the Fifth Amendment is definitively not intended to protect personal privacy. The Supreme Court has held that Fourth and Fifth Amendment protections may overlap in what they protect but has not addressed why they overlap.[203] The overriding concern of the Fifth Amendment is to prevent compelled self-incrimination, while the Fourth Amendment protects privacy interests.[204]

Using the Fifth Amendment to protect biometric information has been somewhat successful; it is apparent, however, that lower courts have struggled with the fit.[205] In *In re Residence in Oakland, CA*, and *United States v. Barrera*, as discussed above, both courts relied on the same principles to justify their respective holdings but reached opposite holdings.[206] Just because the Fifth Amendment may overlap with the Fourth Amendment in the scope of their protections does not mean that one amendment can be substituted for the other. The split in *Residence in Oakland, CA*, and *Barrera* demonstrates courts' confusion when substituting the Fourth Amendment for the Fifth Amendment in analyzing the use of biometric information in the process of a Fourth Amendment search.

Further, the magistrate judge in *Barrera* referenced that a broader application of the Fifth Amendment creates a murky constitutional framework, and in turn, undercuts the purpose of the Fourth Amendment.[207] The Fourth and Fifth Amendments serve distinct purposes, and muddling the two renders them redundant. Because of this redundancy, if a challenge in this line of cases reached an appellate

202 Fisher v. United States, 425 U.S. 391, 399 (1976).

203 *See id.* at 400.

204 *See id.*

205 *See, e.g.*, United States v. Barrera, 415 F. Supp. 3d 832, 838 (N.D. Ill. 2019).

206 *See id.* at 839 (holding that biometric information was more akin to a key and not testimonial); *In re* Search of a Residence in Oakland, California, 354 F. Supp. 3d, 1010, 1016 (N.D. Cal. 2019) (citing Schmerber v. California, 384 U.S. 757, 764–65 (1966)) (holding that biometric information can establish guilt and was testimonial).

207 *See Barrera*, 415 F. Supp. 3d at 842.

court, it is unclear if that court would even consider privacy concerns in applying the Fifth Amendment.[208] But the Framers created the Fourth Amendment for this type of challenge. It was enacted to prevent the use of general warrants that allowed law enforcement officers to search a person and uncover *something* incriminating during the search.[209] Analyzing the inclusion of something in a warrant is better suited for the Fourth Amendment despite the lack of success in these challenges.

As the magistrate in *In re Search Warrant Application* suggested, there needs to be some clarification to this framework.[210] Determining whether a search violates the Fourth Amendment should not hinge solely on the inclusion of biometric information in a warrant but on whether, under the particular circumstances, the search itself is reasonable. As Professor Amar argues, reasonableness is the linchpin of the Fourth Amendment, not a warrant requirement.[211] This reprioritization of reasonableness would allow Fourth Amendment doctrine to keep pace with technological advancements. In its current formulation, briefly assessing whether a search warrant application included biometrics (assuming the relevant court chooses to apply the Fourth Amendment) ignores a commonsense evaluation of the search and its reasonableness.[212] Accordingly, this focus on the Warrant Clause and current reliance on the Fifth Amendment is another example of how courts have weakened the protections the Fourth Amendment provides.[213]

VI. CONCLUSION

Riley v. California established a need for *some* departure from the traditional Fourth Amendment analysis in a warrantless search of a cell phone and held that exceptional circumstances were required to search the cell phone in that case.[214] A similar level of rigor is also necessary when law enforcement officers apply for a warrant that includes biometric information. Cell phones are much closer to a computer than the traditional phone they once were. Further, even something as

208 *See* Fisher v. United States, 425 U.S. 391, 399 (1976) (stating that absent a self-incrimination compulsion challenge the Fifth Amendment is inapplicable).

209 Michael, *supra* note 23, at 912.

210 *See In re* Search Warrant Application, 279 F. Supp. 3d 800, 807 (N.D. Ill. 2017).

211 *See* Amar, *supra* note 24, at 801 ("The core of the Fourth Amendment, as we have seen, is neither a warrant nor probable cause, but reasonableness.").

212 As Professor Amar argues, "[T]he Court's obsession with warrants, probable cause, and criminal exclusion has often made it difficult for the Justices to admit what common sense required." *Id.*

213 *See supra*, Section IV.B.

214 *See* Riley v. California, 573 U.S. 373, 400–01 (2014).

simple as the means to open a phone frequently changes. But lower courts' analyses have failed to fully embrace this idea.

Relying solely on a probable cause standard or the Fifth Amendment dilutes the language of the Fourth Amendment and subverts its original purpose—reasonable searches.[215] With that in mind, courts should consider if someone's face or fingerprint should be used to open something that could contain the equivalent amount of intimate information that a person's home does. Thus, in the absence of clarification from the judiciary or Congress, courts should not compel the use of biometric information for just *any* warrant, as they routinely do. There should be a particularized device, person, and purpose in the warrant, and a nexus demonstrating the link between the need for the biometric information and the crime investigated.[216] Further, courts must more stringently consider the privacy implications at issue.

For that reason, until this issue is clarified, magistrate judges and district courts need to ensure search warrants are properly tailored. There should be a clear nexus between the search warrant, the device implicated, and the crime investigated to avoid the dangers the Fourth Amendment was enacted to prevent. Instead of rubber-stamping biometric-inclusive search warrants, it is necessary to ensure the search is reasonable—avoiding further dilution of the Fourth Amendment's protections and purpose.

215 *See* Amar, *supra* note 24, at 776–77.

216 *See In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1014 (N.D. Cal. 2019).