Hastings Race and Poverty Law Journal

Volume 17
Number 2 *Summer 2020*

Article 11

Summer 2020

Secure the Smartphone, Secure the Future: Biometrics, Boyd, a Warrant Denial and the Fourth and Fifth Amendments

Aaron Chase

Secure the Smartphone, Secure the Future: Biometrics, *Boyd,* a Warrant Denial and the Fourth and Fifth Amendments.

AARON CHASE[1]

Abstract

The growing use of biometric technology—fingerprints, facial recognition and beyond—for data safekeeping—particularly for smart phones, personal computers, and identification—has raised a number of questions for Constitutional scholars. What Constitutional protections, if any, does biometric information have? Does biometric information require a warrant for law enforcement officers to compel its production? Would compelling production of a biometric password effectively force defendants to testify against themselves? Should the growing use of biometric information, by both private third parties and law enforcement, lead courts to reexamine prior precedents regarding privacy interests in personal technology and personal physical characteristics? This paper examines turns to a decision from the United States District Court of Northern California to find answers. That decision, while limited, reflects Supreme Court concerns about technology and offers a line of reasoning that could lead to heightened Constitutional protection for biometric information. This paper in turn argues that such protection, based on a more conjoined reading of the Fourth and Fifth Amendments, is necessary to prevent a new era of law enforcement intrusion into the personal sphere.

1. Aaron Chase is a third-year law student at the University of California, Hastings College of the Law, where he is completing concentrations in Criminal Law and Government Law. During his time at UC Hastings, he has extensively studied the powers and limitations on law enforcement while working as a law clerk for two California district attorney offices, the United States Attorney's Office for the Northern District of California, and the San Francisco City Attorney's Office. He also serves as an editor for the *Hastings Race and Poverty Law Journal*.

I. INTRODUCTION

Police descend upon a home in Oakland, California. They knock loudly, announce themselves, then enter under color of law when the door is opened; upon entrance, they lawfully arrest two individuals accused of engaging in extortion, extortion principally engaged in via Facebook Messenger. The police visually inspect the premises and lawfully seize electronic devices in a relatively routine arrest, until they compel both arrestees to place their thumbs on their smart phones' fingerprint scanners so that their phones' password protections unlock. Then a third individual walks out of the bathroom; this individual is the target of no investigation and not immediately subject to lawful detention or arrest. The police nevertheless detain the individual, seize the phone in her hand, and upon her refusal to unlock her phone, physically compel her to hold her head in place until the phone's facial recognition software engages and the phone unlocks.

The situation described above reflects what law enforcement officers sought in a 2019 warrant request.[2] As biometric technology becomes more integrated with personal technology, and as both become more ubiquitous, courts struggle to understand when and how police may use technology without intruding upon constitutional rights.[3] The United States District Court for the Northern District of California disapproved this particular warrant request.[4] That denial, when taken in combination with recent and past court precedent, suggests that courts may have found a way to adapt the Fourth and Fifth Amendments to the Information Age in order to protect individual rights during a time of everchanging technology.

This paper argues that the courts should embrace the reasoning behind district court's warrant denial, particularly a more expansive and linked interpretation of the Fourth and Fifth Amendment; in doing so, the Court would create a stronger shield against technological intrusion by the government into enumerated and unenumerated rights, thus fulfilling the original purpose of the amendments. As argued below, there is ample precedent, both current and dormant, from the Supreme Court and lower courts alike, that supports the use of the Fourth and Fifth Amendments as bulwarks against law enforcement efforts to use technology to circumvent reasonable warrant requirements.[5] There is, however, opposing precedent

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

3. *See* People v. Davis, 2019 CO 24, ¶ 21. ("Advances in the technology of encryption have further complicated the law surrounding cell phone searches . . . While the government is equipped with technology that allows it to bypass many cell phones' security measures, courts have started to grapple with what to do in the case of an unbreakable lock.").

4. *In re Search*, 354 F. Supp 3d. at 1013.

5. *See, e.g.*, Bryan H. Choi, *For Whom the Data Tolls: A Reunified Theory of Fourth and Fifth Amendment Jurisprudence*, 37 CARDOZO L. REV. 185, 189-90 (2015) (discussing Boyd v.

which renders law enforcement free to view those amendments as inapplicable to technological, and notably biometric, intrusion into the personal sphere.[6] When deciding between these two paths, the courts should consider the pervasiveness of biometrics and other technologies into the everyday lives of Americans, and how the eventual omnipresence of biometrics may ultimately allow law enforcement to broadly disregard traditional warrant requirements and other constitutional protections on individual privacy.

In 2019, law enforcement officers in Oakland requested a warrant to compel the availability of biometric features for all individuals at a private residence, named and unnamed, for the purpose of unlocking digital devices and searching their contents. That was denied by United States District Court for the Northern District of California, in a decision authored by United States Magistrate Judge Kandis Westmore.[7] Officers had argued that such access was needed to reach lawful evidence, evidence that here could help convict those alleged to have threatened a victim with the release of a personally damaging video.[8] The district court rejected this argument and held that: (1) compelling individuals not identified in the warrant to provide biometric information was overbroad and counter to the Fourth Amendment; and (2) the use of a biometric features to unlock an electronic device is testimonial and therefore protected by the Fifth Amendment's Self-Incrimination Clause.[9] The court tied its decision to two principles articulated in previous court holdings. The first principle is that individual rights should not be "diminished . . . due to the advancement of technology."[10] The second is that smart phones and other items of personal technology are more akin to documents than storage equipment and are therefore entitled to a high degree of privacy protection.[11] These principles are both well-rooted and far-reaching in what they could mean for technological privacy rights. The first part of this paper will deal in greater depth with that district court decision and what led to it.

The second part of the paper will discuss the counter-precedent to that line of reasoning. A 2014 decision in Virginia held that, while a defendant could not be compelled to produce a phone's passcode, due to its testimonial nature, he could be compelled to unlock the phone with a fingerprint identification; according to the Virginia court, a fingerprint involved no mental process and was therefore non-testimonial and unprotected by the

United States, 116 U.S. 616 (1886)); *see also, e.g.*, Riley v. Cal., 573 U.S. 373 (2014).

6. *See, e.g.*, State v. Diamond, 905 N.W.2d 870 (Minn. 2018).

7. *In re Search*, 354 F. Supp 3d. at 1013.

8. *Id.* at 1013, 1016.

9. *Id.* at 1013-1018.

10. *See Carpenter* at 2204 (quoting Kyllo v. U.S., 533 U.S. 27, 34 (2001)).

11. *In re Search*, 354 F. Supp 3d. at 1017 (citing Riley v. Cal, 134 S. Ct. 2473, 2492 (2014)).

Fifth Amendment's Self-Incrimination Clause.[12] This decision has origins in the U.S. Supreme Court's repeated refusal to recognize heightened privacy expectations or self-incrimination concerns in personal biological material, even when that material had identificatory properties.[13] The Court has also previously been willing to set aside privacy concerns regarding technology where that technology was owned in part by a third party.[14] Applying these precedents to a biometrically-locked phone, filled with data owned by third parties, the Virginia court's interpretation of the law seems understandable.

The third and fourth parts of the paper will discuss the changing technological environment, how the courts may appraise that environment, and why the Court should ultimately embrace the decision of and principles behind *In re Search*. As discussed in the paper's third part, it seems highly likely that technology will become more and more tied to personal use and personal biology; it also seems likely to become even more ubiquitous and perhaps more egalitarian in distribution. Were the courts to embrace these trends as subservient to and in service of Fourth and Fifth Amendment rights, it could hail a new era for individual freedom and perhaps even equal protection of the law in criminal matters. Were the courts to reject that interpretation, those amendments could become increasingly archaic as law enforcement utilizes technology to intrude further and further into the personal sphere. As discussed in the fourth part, the reasoning behind Judge Westmore's decision, taken together with other court decisions and existing precedent, offers the Supreme Court a body of reasoning with which to reestablish the Fourth and Fifth Amendments as a conjoined defense against over-intrusion, technological and otherwise, by law enforcement into the personal sphere.

II. DISTRICT COURTS TAKE ON WARRANTLESS BIOMETRICS

Judge Westmore's decision produced headlines in a number of publications, but it's impact on the wider body of law is yet to be determined.[15] A warrant denial by a single magistrate judge in a federal

12. *See* Commonwealth v. Baust, 89 Va. Cir. 267, 271 (Va. Cir. 2014).

13. *See* Md. v. King, 569 U.S. 435 (2013); *see also* Schermber v. California, 384 U.S. 757 (1966).

14. *See* Smith v. Md., 442 U.S. 735 (1979).

15. *See, e.g.*, Megan Trimble, *Police Can't Force You to Unlock Your Phone with Your Finger or Face, California Judge Says*, U.S. NEWS & WORLD REP. (Jan. 14, 2019, 1:52 PM), https://www.usnews.com/news/national-news/articles/2019-01-14/police-cant-force-you-to-unlock-your-phone-with-biometrics-california-judge-says; *see also* Thomas Claburn, *Cops Told: No, You Can't Have a Warrant to Force A Big Bunch of People to Unlock Their Phones By Fingerprint, Face Scans*, THE REGISTER (Jan. 14, 2019, 10:46 PM), https://www.theregister.co.uk/2019/01/14/biometric_

district court is not a binding authority, not "in either a different judicial district, the same judicial district, or even upon the same judge in a different case."[16] As the decision relates to the interpretation of the Fourth and Fifth Amendments, it may or may not be viewed as persuasive authority by the state and federal courts that are most likely to deal with warrant requests or other matters of criminal law.[17] Here, the question becomes whether the reasoning within the decision will weigh persuasively upon future decisions in an increasingly important aspect of criminal procedure.

In the warrant denial, *In re Search of a Residence in Oakland* relies on a two-factor analysis. First, there is a relatively brief analysis of the warrant request in Fourth Amendment terms.[18] The court notes that sufficient facts exist to believe that evidence of crime will be found, but that that does not sanitize a violation of constitutional rights.[19] Here, the court finds that the government would violate individual rights under the Fourth Amendment by not identifying a "particular person nor a particular device" in both its warrant requests to seize electronic devices and compel submission of biometric features for the sake of unlocking those devices.[20]

The second, more comprehensive prong of the court's two-factor analysis invokes Fifth Amendment privileges.[21] The court first notes that the Fifth Amendment protects against self-incrimination and that the relevant question here is whether the act to be compelled, in this case "the use of a suspect's biometric feature to potentially unlock an electronic device" is testimonial.[22] The court examines what distinguishes an act as testimonial, noting that '"an act of production' . . . 'that impl[ies] assertions of fact can constitute testimonial communication' before holding here that that the 'use

device_access; *see also* Ryan Whitman, *Judge: Police Can't Force You to Unlock Phone With Fingerprint or Face ID*, EXTREME TECH (Jan. 14, 2019, 8:43 PM).

16. Camreta v. Greene 563 U.S. 692, 709 n.7 (2011) (citing 18 J. MOORE ET AL., MOORE'S FEDERAL PRACTICE - CIVIL § 134.02 (3d ed. 2019)).

17. "The decisions of the lower federal courts on federal questions are merely persuasive. Where lower federal court precedents are divided or lacking, state courts must necessarily make an independent determination of federal law." Rohr Aircraft Corp. v. San Diego, 51 Cal. 2d 759, 764 (1959).

18. *In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1013-1014 (N.D. Cal. 2019).

19. *Id.* at 1013 ("[i]f, however, law enforcement violates another constitutional right in the course of executing a warrant, it inherently renders the search and seizure unreasonable.").

20. *Id.* at 1014 (noting the government sought "any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features[.]" The court held that "[S]earch and seize all digital devices at the Subject Premises is . . . overbroad[.]").

21. *Id.* at 1014-18.

22. *Id.* at 1014–15 ("[T]he question, then, is whether a suspect can be compelled to use his finger, thumb, iris, or other biometric feature to unlock a digital device" and "the proper inquiry is whether an act would require the compulsion of a testimonial communication that is incriminating."); *see* Fisher v. U.S., 425 U.S. 391, 409 (1976).

of biometric features is testimonial . . . .'"[23]

The court relies on two assertions to hold the use of biometric features as testimonial. First, the court compared the use of biometric features to an act protected by the Fifth Amendment—the use of a passcode to lock or secure an electronic device.[24] The court found biometric features to be equivalent because, like a passcode, a biometric lock is "security feature to ensure that someone without the passcode cannot readily access the contents of the phone."[25] Indeed, the court noted the reason the government seemed to express "urgency" in its request to compel use of biometric features was to "bypass the need to enter a passcode" as "a passcode is generally required 'when a device has been restarted, inactive, or has not been unlocked for a certain period of time.'"[26] Second, the court compared the use of biometric features to an act generally unprotected by the Fifth Amendment—requiring a suspect to submit to fingerprinting.[27] The court reasoned that biometric features are unlike submitting fingerprints because a biometric feature "confirms ownership (or access) and control" of a device and "all of its digital contents" for a "particular" individual, which is fundamentally different from the "physical evidence" created by a fingerprint when compared to "existing physical evidence (another fingerprint) . . ."[28] The court also indicated that smartphone applications may allow access to " personal, private information—including medical records and financial accounts" that would be traditionally protected by a phone's passcode in lieu of a biometric lock, thus further distinguishing biometric features from fingerprinting.[29] Thus, by its analogous function to a numeric passcode and its purpose in protecting

23. *In re Search,* 354 F. Supp 3d. at 1015 (relying on Doe v. U.S., 487 U.S. 201, 208 (1988) and *In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1343 (11th Cir. 2012) (citing Fisher, 425 U.S. at 410)).

24. *Id.* at 1015–16 (Stevens, J., dissenting) (relying on *Doe*, 487 U.S at 219) ("A defendant can be compelled to produce material evidence that is incriminating . . . but I do not believe he can be compelled to reveal the combination to his wall safe—by word or deed.") (The *Doe* majority agreed with the dissent on this particular point. *See Doe*, 487 at 210 n.9.); *accord* U.S. v. Kirschner, 823 F. Supp. 2d 665, 669 ("[F]orcing the Defendant to reveal the password for the computer communicates that factual assertion to the government, and thus, is testimonial[.]"); *See also* United States v. Hubbell, 530 U.S. 27, 43 (2009); *see also In re* Boucher, 2007 WL 4246473, at *4 ("A password, like a combination, is in the suspect's mind, and is therefore testimonial and beyond the reach of the grand jury subpoena."), *rev'd*, 2009 WL 424718 (reversing because the modified subpoena sought the unencrypted data rather than the password itself).

25. *In re Search,* 354 F. Supp 3d. at 1015–16.

26. *Id.*

27. *Id.* at 1016.

28. *Id.*

29. *Id.*; *cf.* Robert H. Cauthen, *The Fifth Amendment and Compelling Unencrypted Data, Encryption Codes, and Passwords*, 41 AM. J. TRIAL ADVOC. 119, 121 (2017) ("The word 'witness' in the constitutional text limits the relevant category of compelled incriminating communications to those that are 'testimonial' in character.'" In other words, that means disclosing ideas, information, data, concepts, knowledge, and thoughts." (citation omitted) (quoting *Hubbell,* 530 U.S at 34)).

sensitive personal information, the court held that a biometric lock is testimonial and thus protected by the Fifth Amendment.

The court also concludes that the Foregone Conclusion Doctrine does not apply to the use of biometric features.[30] Under the Forgone Conclusion Doctrine, an act of production cannot be testimonial if the contents of what is to be produced is already known to the government.[31] The court stated that the doctrine applies where "the Government can show that no testimony is at issue . . ." and does not apply where the government "cannot show prior knowledge of the existence or the whereabouts of the documents ultimately produced . . ."[32] The court finds that, in consideration of the large amount of data held within smartphones, the 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."[33] Additionally, the court noted that the government would "be unable to articulate facts" compelling biometric unlocking when requesting a search warrant where it "could not possibly anticipate" the presence of unknown persons.[34]

Throughout the decision, the court expresses concern that "technology is outpacing the law . . ."[35] Citing a recent Supreme Court decision, the court notes that "[c]itizens do not contemplate waiving their civil rights when using new technology . . ."[36] Thus, while the government may have "an interest in accessing the contents of any electronic devices" new technology does not allow the government to "trample on" constitutional rights.[37] So strong is the court's defense of this principle that the court implies that the Fourth and Fifth Amendment prevent the government from ever being able to " access the complete contents of a digital device."[38] Of note, the court blends protections from those two amendments in articulating that defense; it couches a Fourth Amendment defense of a "degree of privacy" within its Fifth Amendment analysis.[39] To the court, both amendments serve to protect

30. *In re Search*, 354 F. Supp 3d. at 1016–18.

31. *See* Cauthen, *supra* note 29, at 124 n.26 ("It is doubtful that implicitly admitting the existence and possession of the papers rises to the level of testimony within the protection of the Fifth AmendmentFalse 'The question is not of testimony, but of surrender.'") (citation omitted) (citing Fisher v. U.S., 425 U.S. 391, 411 (1976)).

32. *In re Search*, 354 F. Supp. 3d at 1017 (quoting *In re* Grand Jury Subpoena Duces Tecum, 670 F.3d 1335, 1343 (11 Cir. 2012)).

33. *Id.* at 1017–18 (citation omitted).

34. *Id.* at 1018.

35. *Id.* at 1014.

36. *Id.* at 1014–15 (citing Carpenter v. U.S., 138 S. Ct. 2206, 2214 (2018))..

37. *See id.* at 1016.

38. *See id.*

39. *See id.* at 1014 (quoting Kyllo v. U.S., 533 U.S. 27, 34 (2001)).

individual rights, especially in the face of changing technology.[40]

A. Precedent Behind *In re Search of a Residence in Oakland*

In re Search of a Residence in Oakland does not exist in isolation. It cites a number of cases.[41] Among those is a recent decision by United States Magistrate Judge M. David Weisman of the United States District Court for the Northern District of Illinois, Eastern Division, which features similar reasoning in similar circumstances.[42] In this recent decision, the government sought to seize and remove "various forms of electronic storage media" from a premises pursuant to the Federal Rules of Criminal Procedure.[43] As part of that seizure, the government sought to compel individuals present at the scene to provide fingerprints or thumbprints in order to open electronic devices.[44] The court authorized the seizure, but denied the request to compel production of fingerprints for the purpose of opening electronic devices.[45]

Like the *Oakland* search warrant denial, this decision relies on a "cross section of protections provided by the Fourth and Fifth Amendments.[46] This court held that there is no Fourth Amendment issue in the "privacy interests of a fingerprint" nor is there a Fifth Amendment interest in "the production of physical characteristics."[47] However, the court held that there can be a Fourth Amendment interest in "the context" in which fingerprints are taken and that the forced application of fingerprints to an electronic device by "any individual at the subject premises" is beyond the government's authority under the Constitution.[48] As in the *Oakland* decision, the court here cites the idea that "an act of production" can be testimonial in finding that "Fifth Amendment concerns" are present in this case.[49] As directly cited in the

40. *See id.* at 1014 n.1, (noting that a suspect arrested under warrant does not waive the right to incrimination).

41. *See, e.g.*, *Carpenter*, 138 S. Ct.; Riley v. Cal., 573 U.S. 373 (2014).

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

43. *Id.* at 1066–1067 ("A warrant under *Rule 41(e)(2)(A)* may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in *Rule 41(e)(2)(A)* and *(f)(1)(A)* refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review." (quoting Fed. R. Crim. P. 41(e)(2)(B))).

44. *Id.* at 1067 ("[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 contents of any such device.'").

45. *Id.*

46. *Id.* at 1068.

47. *Id.* at 1070.

48. *Id.* at 1070, (relying on U.S. v. Guevara-Martinez, 262 F.3d 751, 752 (8th Cir. 2001)).

49. *Id*. at 1072–74 ("We do not believe that a simple analogy that equates the limited protection afforded a fingerprint used for identification purposes to forced fingerprinting to unlock

Oakland decision, the court here invokes the privacy concerns attached to modern cellphones to differentiate compelling production of a biometric fingerprint as opposed to compelling production of a fingerprint.[50] Both courts note the seriousness of the government's concerns while still denying the search warrant application under constitutional concerns.[51] While the language of this decision's conclusion is not as strong or far-reaching as the *Oakland* decision, in both cases the courts come to the conclusion that the government cannot compel the production of biometric features to unlock an electronic device.[52]

As both decisions employ analysis under the Fourth and Fifth Amendment, both employ case precedent relevant to each Amendment. A separate analysis of the precedents shows how each Amendment produces relevant concerns for privacy interests in the face of advancing technology. There is, as explained below, a potential direct nexus between the two Amendments in existing case law.

1. Fourth Amendment Precedent

Under the Fourth Amendment, "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."[53] When applying the protections of the Fourth Amendment to government attempts at search and seizure within the bounds, or lack thereof, of modern society, the courts consider foremost the test laid down in *Katz v. United States*.[54] By then,

an Apple electronic device that potentially contains some of the most intimate details of an individual's life (and potentially provides direct access to contraband) is supported by Fifth Amendment jurisprudence." (quoting *In re* Grand Jury Subpoena Duces Tecum, 670 F.3d 1335, 1345(11th Cir. 2012)) (citing Curcio v. U.S., 354 U.S. 118, 128 (1957)).

50. *In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1016 (N.D. Cal. 2019) ("As Judge Weisman astutely observed, using a fingerprint to place someone at a particular location is a starkly different scenario than using a finger scan 'to access a database of someone's most private information.'" (citing *In re* Application for a Search Warrant, 236 F. Supp. 3d at 1073)).

51. In *In re Search*, "[T]he Court sympathize[d] with the Government's interest in accessing the contents of any electronic devices it might lawfully seize." 354 F. Supp. 3d at 1116. The Court also reasoned in *In re Application for a Search Warrant*, "the Court sympathizes with the Government's interest in accessing the contents of any electronic devices it might lawfully seize." 236 F. Supp. 3d at 1068.

52. *In re Search*, 354 F. Supp. 3d at 1118; *In re Application for a Search Warrant* 236 F. Supp. 3d at 1074.

53. U.S. CONST. amend. IV.

54. 389 U.S. 347 (1967). *But cf.* U.S. v. Jones, 565 U.S. 400, 404–05 (2012) (holding that the warrantless placement of a GPS device on a vehicle was a search due to the government's physical intrusion, or trespass onto private property, likening such an action to actions proscribed against at the time of the Fourth Amendment's enactment).

Supreme Court had previously declared that the Fourth Amendment applied beyond the " more common tangible fruits of unwarranted intrusion."[55] The Court had declared that the Fourth Amendment mandated a right to privacy that required exclusion of illegal evidence in a criminal case.[56] The Court had also already expressed a wariness as to electronic surveillance and its intrusions into personal affairs.[57] In *Katz*, the Court struck down an attempt by the FBI to listen to a suspect's telephone conversation via an "electronic listening and recording device" without a warrant on the basis on the Fourth Amendment.[58] A concurrence within that decision, by Justice John Marshal Harlan II, used the Court's reliance on privacy in reaching its conclusion to develop a two-prong test: "[F]irst that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable."[59] This "reasonable expectation of privacy" test is still often determinative of what receives Fourth Amendment protection from search or seizure without a warrant.[60]

Courts, however, have struggled with the application of this test to evolving technology.[61] One noted scholar in the area acknowledged that there are three ongoing issues regarding "new technology" and the scope of the Fourth Amendment: (1) the "technologically innovative form" of electronic records and their comparison to other records; (2) third party consent issues that come with electronic access to personal information; and (3) shared access to electronic information and the potentially reduced expectation of privacy that comes with it.[62] These concerns have often made Court decisions regarding the Fourth Amendment and technology hard to

55. Berger v. New York, 388 U.S. 41 (1967) (citing Wong Sun v. U.S., 371 U. S. 471 (1963)).

56. *See* Mapp v. Ohio, 367 U.S. 643, 655 (1961) ("Since the Fourth Amendment's right of privacy has been declared enforceable against the States through the Due Process Clause of the Fourteenth, it is enforceable against them by the same sanction of exclusion as is used against the Federal Government.").

57. *Berger*, 388 U.S. at 49 ("The law, though jealous of individual privacy, has not kept pace with these advances in scientific knowledge.").

58. *Katz*, 389 U.S. at 354 ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth, and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment.").

59. *Id.* at 361 (Harlan, J., concurring) (noting "that electronic, as well as physical, intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment.").

60. U.S. v. Jones, 565 U.S. 400, 406 (2012) ("'[T]he Fourth Amendment protects people, not places,' and . . . a violation occurs when government officers violate a person's 'reasonable expectation of privacy[.]'" (citation omitted) (citing Katz, 389 U.S. at 360)).

61. Wayne R. LaFave, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT, § 2.6(f), (5th ed. 2018) ("[A]pplication of the *Katz* formula is especially problematical in the present context, involving 'new technologies,' for 'societal expectations linked to a technology evolve with time.' (quoting Ryan C. Reetz, *Warrant Requirement for Searches of Computerized Information*, 67 B.U. L. Rev. 179, 197 (1987)).

62. *See* Lafave, *supra* note 61.

predict.[63] This uncertainty exists in spite of the fact that computers and the Internet are ubiquitous and important to "increasingly large segments of society."[64]

Smith v. Maryland crystallizes the Court's issues with shared data and third-party consent.[65] The Court had previously held that there was no legitimate expectation of privacy in information that is "voluntarily conveyed" and owned by a third-party.[66] In *Smith*, the Court held that the warrantless monitoring of telephone communications via a "pen register" was permissible because: (1) the pen register monitored records that were held by a third-party, here a telephone company and that therefore the suspect "assumed the risk" of disclosure[67]; (2) the pen register did not acquire the "contents of communications" as occurred during the wiretapping in *Katz*.[68] Notably, the third-party doctrine has been used to compel the disclosure of subscriber information given to an Internet service provider.[69] However, the courts have repeatedly defended an justified expectation of privacy where the content of conversations, messages or files is involved.[70]

However, the Supreme Court has signaled that it is interested in safeguarding "the privacy and security of individuals against arbitrary invasions by governmental officials . . ." and thus there is a likelihood that

63. *Id.* ("In part the uncertainty is attributable to the Supreme Court's overall approach to questions regarding the Fourth Amendment's scope, involving a balancing of privacy claims against crime control interests, which for various reasons means that the 'choice of values and the legal reasoning that will be used in future cases are difficult to predict.'" (citing Randolph S. Sergent, *A Fourth Amendment Model for Computer Networks and Data Privacy,* 81 VA. L. REV. 1181, 1193 (1995)).

64. *Id.* (citing Terri A. Cutrera, *The Constitution in Cyberspace: The Fundamental Rights of Computer Users*, 60 U.M.K.C. L. REV 139 (1991)).

65. Smith v. Md. 442 U.S. 735 (1979).

66. U.S. v. Miller, 425 U.S. 435, (1976). *See also* U.S. v. White, 401 U.S. 745 (1971).

67. "When . . . petitioner voluntarily conveyed numerical information to the telephone phone company and 'exposed' that information to its equipment in the normal course of business . . . [he] assumed the risk that the company would reveal to the police the numbers he dialed." Smith, 442 U.S. at 744–36; *cf.* Miller, 442 U.S. at 435.

68. Smith, 442 U.S. at 741, (quoting U.S. v. New York Tel. Co., 434 U. S. 159, 167 (1977) ("the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.").

69. *See* Doe v. Shurtleff, 628 F.3d 1217, 1226 (10th Cir.2010) (requiring that that registered sex offender report "his online identifiers" to state does not violate Fourth Amendment). *But see* U.S. v. Horton, 863 F.3d 1041, 1047 (8th Cir.2017) (holding that a search technique targeting IP addresses is a search where it violates a suspect's "reasonable expectation of privacy in the contents of his personal computer.").

70. *See* Reetz, *supra* note 61; s*ee also* Sergent, *supra* note 63. *But See* Orin Kerr, *Do Users of Wi-Fi Networks Have Fourth Amendment Rights Against Government Interception?* THE VOLOKH CONSPIRACY (Sept. 24, 2012, 6:17 pm) http://volokh.com/2012/09/24/fourth-amendment-rights-for-users-of-wi-fi-networks-both-encrypted-and-unencrypted/.

courts will not bless future warrantless searches no matter how cloaked they are in technology.[71] Three recent Supreme Court decisions show that the Court is willing to invoke Fourth Amendment protections in the face of technological innovation. In *United States v. Jones*, the Court held that attachment of the GPS device to the vehicle, and its use of that device to monitor the vehicle's movements, constitutes a search under the Fourth Amendment.[72] The majority opinion there relied not on the *Katz* reasonable expectation of privacy test, but on the "physical intrusion" of the government in placing a GPS on a suspect's car, which the Court described as a personal "effect".[73] Of particular note is the concurrence of Justice Sotomayor, who observed:

> People disclose the phone numbers that they dial or text to their cellular providers, the URLS that they visit and the e-mail addresses with which they correspond to their Internet service providers, and the books, groceries and medications they purchase to online retailers . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[74]

While Justice Sotomayor's concurrence was not joined by any other justice, it echoes a dissent from *Smith v. Maryland*.[75] It also foreshadows the privacy concerns that Sotomayor and other justices broadcast in the hearing for *Carpenter*.[76]

In 2014, the Court came forward with an even stronger application of the Fourth Amendment to personal privacy rights and property. In *Riley v. California*, the Court concluded that a warrant is required to search digital

71. Carpenter v. U.S., 138 S. Ct. 2206, 2213 (2018) (quoting Camara v. Mun. Ct. of City & Cty of S.F., 387 U. S. 523, 528 (1967)).

72. U.S. v. Jones, 565 U.S. 400, 413 (2012).

73. *Id.* at 404–405 (held a "vehicle is an effect" under United States v. Chadwick, 433 U.S. 1, 12, (1977)) (Later, the majority noted that "[i]t may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question." Jones, 565 U.S. at 412.

74. *Id.* at 418.

75. Smith v. Md., 442 U.S. 735, 749 (1979) (Marshall, J., dissenting) (citing Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 95–96 (1974) (Marshall, J., dissenting).

76. Amy Davidson Sorkin*, In Carpenter Case, Justice Sotomayor Tries to Picture the Smartphone Future*, THE NEW YORKER (Nov. 30, 2017), https://www.newyorker.com/news/our-columnists/carpenter-justice-sotomayor-tries-to-picture-smartphone-future (quoting Sotomayor, J., '"If it's not O.K. to put a beeper into someone's bedroom, why is it O.K. to use the signals that phone is using from that person's bedroom, made accessible to law enforcement without probable cause?"').

information from a mobile phone.[77] The Court notes that as mobile phones, particularly smart phones, are closer to a "minicomputer" in nature, searching them while searching a person is not simply a "narrow intrusion on privacy":[78]

> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life."[79] The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.[80]

2. Fifth Amendment Precedent and Counter-Precedent

In accordance with the Self-Incrimination Clause of the Fifth Amendment, no person under the jurisdiction of the Constitution "shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law."[81] Courts have interpreted this clause to mean that persons under the jurisdiction of the Constitution are protected from compelled testimonial self-incrimination.[82] This right is broad and expansive:

> The Fifth Amendment of the Constitution of the United, States gives absolute protection to a person called as a witness in a criminal case against the compulsory enforcement of any criminating testimony against himself. He is not only protected from any criminating testimony against himself relating to the offense under investigation, but also relating to any act which may lead to a criminal prosecution therefor.[83]

At least three required elements are necessary for the invocation of the Fifth Amendment's protection: "(1) compulsion, (2) a testimonial

77. 573 U.S. 373, 403 (2014).

78. *Id.* at 394.

79. *Id.* at 403 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

80. *Id.*

81. U.S. CONST. amend. V, §3.

82. Paul Cassell & Kate Smith, *The Fifth Amendment Criminal Procedure Clauses,* THE NAT'L CONST. CENT., https://constitutioncenter.org/interactive-constitution/interpretation/amendment-v/clauses/632 (last visited Mar. 9, 2020) ("The Supreme Court has many times affirmed the most natural understanding of these words: the defendant in a criminal case cannot be compelled to testify . . .").

83. Brown v. Walker, 161 U.S. 591, 630 (1896).

communication or act, and (3) incrimination."[84] Indeed, *In re Search of a Residence in Oakland* holds that the proper inquiry into a violation of Fifth Amendment rights involves where an act in question involves all three elements.[85] However, the focus of the Fifth Amendment reasoning within that case is on what is testimonial.[86]

The Court has held that there is an '"absolute right not to testify'" that extends beyond trial.[87] The Court has also held that testimony is not simply limited to oral communication.[88] It can include written words, gestures intended to communicate, and physical evidence and acts that compel "responses that are essentially testimonial."[89] Yet that privilege against compelled testimony does not extend to the compulsion of "real or physical evidence" alone, at least not under the Fifth Amendment.[90] For an act to qualify as testimonial, it must require the defendant to "disclose the contents of his own mind.[91]

Much of the debate as to whether an act is testimonial revolves around "acts of production" and when an act constitutes the contents of a defendant's mind.[92] The acts of production doctrine comes from *Fisher v. United States*, where the Court ruled that compelling a third-party to produce a defendant's

84. *In re* Grand Jury Subpoena Duces Tecum*,* 670 F.3d 1335, 1341 (11 Cir. 2012); *see also* Hiibel v. Sixth Judicial Dist. Ct., 542 U.S. 177, 189 (2004). *But see* Cauthen, *supra* note 29, at 120 (arguing there are four separate elements to be considered: (1) Compelled, (2) Criminal Case, (3) Witness, and (4) Against Himself.).

85. *In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1014 (N.D. Cal. 2019) ("The proper inquiry is whether an act would require the compulsion of a testimonial communication that is incriminating.").

86. *Id.* ("Here, the issue is whether the use of a suspect's biometric feature to potentially unlock an electronic device is testimonial under the Fifth Amendment.").

87. Salinas v. Tex., 570 U.S. 178, 184 (2013) (citations omitted).

88. *See* Michael S. Pardo*, Self-Incrimination and the Epistemology of Testimony*, 30 CARDOZO L. REV. 1023, 1027-28 (2008) (citing Schmerber v. Cal., 384 U.S. 757, 764 (1966)).

89. *Id.* (quoting *Schmerber*, 384 U.S at 764).

90. *In re Search*, 354 F. Supp. 3d at 1015 ("The distinction which has emerged, often expressed in different ways, is that the privilege is a bar against compelling 'communications' or 'testimony,' but that compulsion which makes a suspect or accused the source of 'real or physical evidence' does not violate it."). *But see Schmerber*, 384 U.S. at 764 ("To compel a person to submit to testing in which an effort will be made to determine his guilt or innocence on the basis of physiological responses, whether willed or not, is to evoke the spirit and history of the Fifth Amendment.").

91. Curcio v. U.S., 354 U.S. 118, 128 (1957); *see also* Peter Thomson, *The Fifth Amendment's Act of Production Doctrine: An Overlooked Shield Against Grand Jury Subpoenas Duces Tecum*, 20 FED. SOC. REV. 5 (2019) ("[W]hen the government compels a witness 'to use the contents of his own mind' to communicate something factual, the communication is equivalent to testimony and the Fifth Amendment bars the government from compelling its disclosure.").

92. *Id.* at 6 ("[B]ecause of the lack of judicial clarity regarding the meaning of 'testimonial,' criminal practitioners might find it difficult to discern the circumstances under which an act of production is protected by the Fifth Amendment, particularly since no bright line test has been established by the Supreme Court.").

documents, where those documents are not protected by another right or privilege, does not involve incriminating testimony and therefore does not invoke Fifth Amendment protection.[93] However, the Court affirmed that the act of producing evidence in response to a government order has communicative aspects of its own beyond the contents of the evidence, as it concedes the existence of the evidence, its control and possession by the defendant; the Court stated that whether these elements proved to be testimonial would depend on the particular facts of the case.[94] A *Fisher* concurrence by Justice Brennan came to a stronger conclusion:

> Many of the matters within an individual's knowledge may as easily be retained within his head as set down on a scrap of paper. I perceive no principle which does not permit compelling one to disclose the contents of one's mind but does permit compelling the disclosure of the contents of that scrap of paper by compelling its production.[95]

While Brennan's concurrence is *Fisher* is not binding, it did pave the way for strong links between acts of production and testimony. In *United States v. Doe* (1984), the Court took the *Fisher* decision's reasoning as to "communicative aspects" and held that an act of production was testimonial where the production concedes the "existence, possession, and authenticity" of the evidence.[96] A later, separate decision in *Doe v. United States* (1988) re-affirmed the acts of production doctrine to compel disclosure of foreign bank records, holding that the Self-Incrimination Clause could only be used to "resist compelled explicit or implicit disclosures of incriminating information."[97] However, the dissent's argument that the government could force someone "to surrender a key to a strongbox containing incriminating documents," but not "to reveal the combination to [a] wall safe[,]"[98] affirmed by the majority,[99] has formed the basis for repeated holdings that passwords

93. *See* Fisher v. U.S., 425 U.S. 391, 392 (1976).

94. *Id.* at 419 (Brennan, J., concurring) ('"that the privilege protects an accused . . . from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature . . ."' (alteration in original) (quoting *Schmerber*, 384 U.S. at 761)).

95. *Id.* at 420 (Brennan, J., concurring).

96. U.S. v. Doe, 465 U.S. 605 (1984).

97. Doe v. U.S., 487 U.S. 201, 212 (1988).

98. *Id.* at 219. *But see* Orin Kerr, *The Fifth Amendment and Touch ID*, WASH. POST: THE VOLOKH CONSPIRACY (Oct. 21, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/21/the-fifth-amendment-and-touch-id/?utm_term=.41ca1c7d93aa ("The problem is that this passage is really vague. Stevens wrote that a person may 'in some cases' be forced to surrender a key, but that suggests that there are other cases in which a person couldn't be forced to surrender a key.").

99. *Doe,* 487 U.S at 210 n.9.

are protected by the Fifth Amendment.[100]

Fifth Amendment self-incrimination privileges were further defined in *United States v. Hubbell.*[101] Under *Hubbell*, the government could not order production of documents if the government could not demonstrate, with reasonable particularity, that the documents existed and were in the possession of the defendant.[102] Additionally, the documents were protected not just if they contained incriminating evidence, but would '"furnish a link in the chain of evidence'" needed to prosecute a crime.[103] The Court also stated that the "Fifth Amendment privilege against self-incrimination [only] applies to acts that imply assertions of fact."[104] '"[I]n order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information . . . .'"[105] While the decision itself related to testimony and documents ordered produced by subpoena, the concurrence notedly pointed out that at the time of the Fifth Amendment's creation, the privilege against self-incrimination was widely held to grant a right against giving or furnishing evidence.[106] This concurrence could provide a pathway for a more expansive reading of the Fifth Amendment than provided for by the *Hubbell* majority.[107]

However, *Hubbell* also reaffirmed a serious limiting factor to the self-incrimination privilege by stating that acts providing evidence that is not testimonial in nature is not protected.[108] Particularly excluded were acts exhibiting "physical characteristics" that are not analogous to communicative acts expressing or implying assertions of fact or belief.[109] This exception had previously been used to force compulsion of various acts, including providing blood, handwriting, and voice samples, along with standing in a lineup and wearing a particular piece of clothing.[110] Effectively, the

100. *See, e.g.*, U.S. v. Kirschner, 823 F. Supp. 2d 665, 668-69; Commonwealth v. Baust, 89 Va. Cir. 267 (Va. Cir. 2014); *In re* Grand Jury Subpoena Duces Tecum, 670 F.3d 1335, 1345-46 (11th Cir. 2012); SEC Civil Action v. Huang, 2015 U.S. Dist. LEXIS 127853, at *3-7 (E.D. Pa. Sept. 23, 2015). *But see* Phillip R. Reitinger*, Compelled Production of Plaintext and Keys,* 1996 U. CHI. LEGAL F. 171, 195 (arguing that if the password is physically recorded somewhere, the government can subpoena the production of that password).

101. U.S. v. Hubbell, 530 U.S. 27 (2000).

102. *Id.* at 28.

103. *Id.* at 38 (quoting Hoffman v. U.S., 341 U.S. 479 (1951)).

104. *Id.* at 36 n.19.

105. *Id.*

106. *Id.* at 50-52; *See also* John Duong, *The Intersection of the Fourth and Fifth Amendments in the Context of Encrypted Personal Data at the Border*, 2 DREXEL L. REV. 313, 330 (2009).

107. *See* Duong, *supra* note 106, at 332 n. 98.

108. *Hubbell*, 530 U.S. at 36.

109. *Id.* at 35 (citing Pa. v. Muniz, 496 U.S. 582, 594-598 (1990)).

110. *See Doe*, 487 U.S. at 210; Gilbert v. Cal., 388 U.S., 263, 266-267 (1967) (handwriting exemplar); U.S. v. Dionisio, 410 U.S. 1, 7 (1973) (voice exemplar); U.S. v. Wade, 388 U.S., 210, 221-222 (1967) (standing in a lineup); Holt v. U.S., 218 U.S. 245, 252-253 (1910) (wearing a particular piece of clothing).

decisions hold that "[t]he Fifth Amendment does not protect against forced physical acts."[111] The most common reasoning behind these exclusion is that such acts are not testimonial because they do not disclose the contents of the mind.[112] As one scholar puts it, "Communications requiring extensive mental use are testimonial, and those requiring little are not."[113]

III. A FUTURE WHERE BIOMETRICS ARE NOT PROTECTED BY THE FIFTH AMENDMENT

As more people have smartphone that are locked using fingerprint or facial recognition locks, law enforcement have included language in warrants to compel the unlocking of phones via these methods.[114] The line of precedent distinguishing physical acts that do not involve "cognitive content" or "implied communications" has led a number of scholars that the use of biometrics to encrypt a phone is not protected under the Self-Incrimination Clause.[115] A number of courts have now agreed with that reasoning.[116] If this reasoning is embraced by higher courts and law enforcement, the consequences for society at large could be severe and far-reaching.

Commonwealth v. Baust, a 2014 Virginia Circuit Court decision, may be the first decision explicitly dealing with biometric smartphone passwords.[117] There, police sought to compel a defendant to produce video, possibly stored on his phone, that may have recorded him assaulting a victim within defendant's bedroom.[118] Defendant's phone was protected by both passcode and fingerprint encryption, and defendant claimed that both of these are testimonial and production of either of these would violate his rights under the Self-Incrimination Clause of the Fifth Amendment.[119] The court first held that the existence and location of the contents of the phone are a foregone conclusion and not protected by any Fifth Amendment right.[120]

111. *See* Dan Terzian, *The Micro-Hornbook on the Fifth Amendment and Encryption*, 104 GEO. L. REV. 168, 169 (2016).

112. *See* Dan Terzian, *The Fifth Amendment, Encryption, and the Forgotten State Interest*, 61 UCLA L. REV. 298, 304 ("Many compelled acts . . . do not require meaningful mental use, so they are not testimonial.").

113. *Id.*

114. *E.g.*, *In re* Search of, 317 F. Supp. 3d 523 (D.D.C. 2018); *In re* Application for a Search Warrant, 236 F. Supp. 3d 1066 (N.D. Ill. 2017); *In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010 (N.D. Cal. 2019).

115. Terzian, *supra* note 112, at 304-305; *see also, e.g.*, Cauthen, *supra* note 29, at 12; Lafave, *supra* note 61, at §2.2(f).

116. *E.g.*, Commonwealth v. Baust, 89 Va. Cir. 267 (Cir. Ct. 2014); ST. v. Diamond, 905 N.W.2d 870 (Minn. 2018).

117. 89 Va. Cir. 267 (Cir. Ct. 2014).

118. *Id*. at 267-68.

119. *Id.* at 268.

120. *Id.* at 269 (quoting Doe v. U.S. *(In re* Grand Jury Subpoena), 383 F.3d 905, 910 (9th Cir.

However, it did hold that passcode was testimonial and protected.[121] It held the opposite for fingerprints—the government could compel the defendant to produce a non-testimonial fingerprint to unlock the phone:[122]

> The fingerprint like a key, however, does not require the witness to divulge anything through his mental processes. On the contrary, like physical characteristics that are non-testimonial, the fingerprint of Defendant if used to access his phone is likewise non-testimonial and does not require Defendant to 'communicate any knowledge' at all. Unlike the production of physical characteristic evidence, such as a fingerprint, the production of a password forces the Defendant to 'disclose the contents of his own mind. For this reason, the motion to compel the passcode should be DENIED but the motion to compel the fingerprint should be GRANTED.'[123]

The Minnesota Supreme Court came to similar reasoning in *State v. Diamond.*[124] Reaffirming an earlier decision by the Minnesota Court of Appeals,[125] the Minnesota Supreme Court held that a defendant, suspected of involvement in a home burglary, could be compelled to provide a fingerprint to unlock his phone under threat of civil and criminal contempt.[126] The court held that providing fingerprint are not testimonial because the "compelled act merely demonstrated Diamond's physical characteristics and did not communicate assertions."[127] The court held that "merely providing" the fingerprint here could not involve a "mental process" because the defendant did not have to "self-select" the finger used to unlock the phone or even be "conscious" for the application.[128] Thus, because providing the "physical characteristics" of the fingerprint involved no mental process and because the compelled act did not determine the defendant's guilt or innocence on the basis of physiological responses, providing the fingerprint for the purpose of

2004)).

121. *Id.* at 270 (citations omitted).

122. *Baust*, 89 Va. Cir. at 271.

123. *Id.*

124. *Diamond,* 905 N.W.2d at 870.

125. ST. v. Diamond, 890 N.W.2d 143 (Minn. Ct. App., 2017).

126. *Diamond,* 905 N.W.2d at 872, 878.

127. *Id.* at 878.

128. *Id.* at 877. *But see* Kerr, *supra* note 98 (Stating that where the government doesn't know the owner of the phone, compelling a person to biometrically unlock a phone in question "implies testimony because Touch ID is programmed to respond to only one body part. That choice of body part acts like a password . . . [S]o responding to the order by unlocking the phone using the correct body part tends to show that the person is the owner.").

unlocking the phone could not be testimonial.[129] Like *Baust, Diamond* rules conclusively that where physical characteristics do not communicate assertions of fact from a defendant's mind, they cannot be testimonial, leaving biometric locks unprotected by the Fifth Amendment under current precedent.[130]

There are also cases and scholars who go beyond the reasoning articulated in *Baust* and *Diamond* in terms of seeking to limit the self-incrimination privilege in regard to passwords and biometrics.[131] Judge Charles Breyer of the United States District Court for the Northern District of California reasoned in *United States v. Spencer* that a rule where the government can never compel decryption of a password-protected device leads to "absurd results."[132] Instead, courts should consider access to encrypted data based on whether the "foregone conclusion rule" applies to the encrypted data or passwords.[133] "Whether turning over material, either in the form of documents or bits, implicates the Fifth Amendment should not turn on the manner in which the defendant stores the material."[134] Dan Terzian argues that passwords, and the encrypted data they protect, should not be protected in the same manner than safe combinations are.[135] Instead, courts should consider a "fair state-individual balance" that "where there is a societal need to limit" the Self-Incrimination Clause, the state should permit compulsion upon defendants.[136] Terzian argues that this is possible as there is only no "absolutes" within the values underlying the Fifth Amendment and only a "strong preference" for not permitting compulsion;[137] Terzian argues that as data encryption is increasingly used, it will become "unfairly difficult" to prosecute crimes with balancing Fifth Amendment interests more toward state interests.[138]

An examination of current circumstances shows some of the risks of weighing the balance of state-individual interests further toward the state. As

129. *Diamond*, 890 N.W.2d at 877-888 (citation omitted).

130. *Id.* at 878.

131. *See, e.g.*, Terzian, *supra* note 112; U.S. v. Spencer, No. 17-cr-00259-CRB-1, 2018 U.S. Dist. LEXIS 70649 (N.D. Cal. Apr. 26, 2018).

132. *Spencer*, 2018 U.S. Dist. LEXIS 70649, at *5 ("Whether a defendant would be required to produce a decrypted drive would hinge on whether he protected that drive using a fingerprint key or a password composed of symbols.").

133. *Id.* at *6-*8 (holding that the government should be held to establish with "reasonable particularity" that it had independent knowledge of the "existence, possession, and authenticity" of the information requested. (quoting U.S. v. Hubbell, 167 F.3d 552, 579 (D.C. Cir. 1999)); *cf.* Commonwealth v. Gelfgatt, 11 N.E.3d 605 (Mass. 2014) (arguing that password encrypting computer was a foregone conclusion).

134. *Spencer*, 2018 U.S. Dist. LEXIS 70649, at *6-*7.

135. *Terzian*, *supra* note 112, at 306.

136. *Id.* at 307.

137. *Id.*

138. *Id.* at 309-10.

is, roughly three-quarters of Americans use smartphones, and an increasing number use biometric locks due to their convenience, without consideration of the risk biometrics may pose to their Constitutional rights.[139] Furthermore, this risk may phone more heavily, as it often does, on African-Americans, and others who are less likely to buy more expensive smartphones with "panic buttons" that disable biometric locks in favor of passcodes.[140] To definitively make biometrics unprotected would deny a massive number of Americans the privacy they expect to have in their smartphone sand would likely disproportionately affect vulnerable segments of American society.[141]

It is also likely that the government exposure of private data and records via biometrics will continue to expand. An FBI program called Next Generation Identification is engaged in expanding biometric interoperability across all branches of the government.[142] This program seeks to have biometric information—fingerprints, palm scans, iris scans, facial and scar recognition, and more—taken from local, state, and federal background checks, criminal and otherwise, and place this information in a single database, accessible by local, state and federal government agencies.[143] At the same time, federal authorities have been using genetic information gleaned from private databases (mostly used for genealogy) for criminal law enforcement;[144] beyond privacy concerns, this is notable as genetic information is now being used to make advanced biometric locks for the sake of data encryption.[145]

The government would likely argue that such information is being gathered either voluntarily, from latent sources or from less-protected societal segments like immigrants and criminals.[146] However, these databases have led to the retention of data from lawful, natural-born

139. *See* Riana Pfefferkorn, *Oh, So Everybody's a Legal Expert Now: Minnesota v. Diamond, Microsoft Ireland, and User-Hostile Path Dependence in the Law*, THE CENT. FOR INTERNET & SOC'Y. AT STAN. L. SCH., (Jan 19, 2018) http://cyberlaw.stanford.edu/blog/2018/01/oh-so-everybody%E2%80%99s-legal-expert-now-minnesota-v-diamond-microsoft-ireland-and-user.

140. *Id.*

141. *Id.*

142. Next Generation Identification (NGI) Documents, UNCOVERING THE TRUTH, http://uncoverthetruth.org/foia-documents/ngi-documents (last visited Apr 10, 2019).

143. *Secure Communities and Next Generation Identification: The FBI's "Big Brother" Surveillance Agenda*, UNCOVERING THE TRUTH, (July 6, 2011), http://uncoverthetruth.org/wp-content/uploads/2011/07/7-6-11-Scomm-NGI-Fact-Sheet.pdf. (last visited Apr 10, 2019).

144. *See* Natalie Ram, *The U.S. May Soon Have a De Facto National DNA Database*, SLATE: FUTURE TENSE (Mar. 19, 2019), https://slate.com/technology/2019/03/national-dna-database-law-enforcement-genetic-genealogy.html.

145. *See* Pierluigi Paganini, *The Future of Data Security: DNA Cryptography and Cryptosystems,* SECURITY AFFAIRS (Feb. 15, 2015), https://securityaffairs.co/wordpress/33879/security/dna-cryptography.html.

146. *See* Ram, *supra* note 144; *supra* note 142; s*upra* note 143.

citizens.[147] Data that can be easily accessed and used by the government against individuals without Fourth and Fifth Amendment protection for biometrics. Without the democratic consent of the American people, which has not yet been given, the surrender of massive amounts of personal data to the government for use in criminal prosecution seems less like a balancing of interests between the state and individuals and more like an abrogation of individual Constitutional protections for the sake of government convenience.[148]

IV. BIOMETRICS AND THE NEXUS BETWEEN THE FOURTH AND FIFTH AMENDMENTS

Were the Supreme Court to decide that biometric locks deserve Constitutional protection, it could very well decide to accept that biometric locks are analogous to passcodes, as in *In re Search of a Residence in Oakland*.[149] In light of the Court's manifested reservations about advancing technology,"[150] the Court could extend a reasonable expectation of privacy to personal biometric and genetic information, thus granting heightened Fourth Amendment protection.[151] To limit attempts by law enforcement to use sweeping techniques to unlock phones of individuals not specifically mentioned in a warrant,[152] the Court could enforce a "reasonable particularity" standard when the government seeks to have a cell phone or electronic device unlocked or unencrypted.[153] All of these measures would potentially increase the level of protection for the biometric encryption that Americans increasingly rely on.[154]

However, these protections may not be sufficient to prevent digital devices from "betray(ing) us" to law enforcement.[155] The foregone conclusion doctrine may allow forced decryption of a digital device, and while some courts require "reasonable particularity" or knowledge of a

147. *Id.*

148. *See* Ram, *supra* note 144 (discussing attempts to set up compressive expansion of Arizona's DNA database and the opposition with which the effort was met).

149. *In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1015-16 (N.D. Cal. 2019); *See also In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073-74 (N.D. Ill. 2017).

150. Carpenter v. U.S., 138 S. Ct. 2206, 2221 (2018).

151. *See* Ram, *supra* note 144.

152. *See In re Search*, 354 F. Supp. 3d at 1013

153. *See* U.S. v. Pearson, No. 1:04-CR-340, 2006 U.S. Dist. LEXIS 32982 (N.D.N.Y. May 24, 2006); *see also In re* Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d 87, 93 (2d Cir. 1993) (holding the standard the government must meet for required production is reasonable particularity).

154. *See* Pfefferkorn, *supra* note 139.

155. *See* Choi, *supra* note 5, at 187.

"certain file" to invoke the doctrine, this is not a universal standard.[156] "Other courts apparently require only that the government know of the potential for unencrypted files, even if it doesn't know the contents of those files because they're encrypted."[157] There is also the required records doctrine, which is rarely invoked but could lead to troubling government actions if it was.[158] Under the doctrine, if the government were to stipulate that a specific type of record must be kept by law, then those types of records are categorically excluded from the privilege against self-incrimination.[159] Thus, even with increased constitutional protections, the government could continue to force decryption of smartphone, perhaps without specific knowledge of the records it was searching for, or simply mandate that certain records be kept on smartphones and access those without invoking Fifth Amendment protections.[160]

There is case that may point to a more comprehensive protection of individual Fourth and Fifth Amendment rights in the face of government attempts at technological intrusion—*Boyd v. United States*.[161] The case is referenced within the dicta of *In re Search of a Residence in Oakland*, specifically within a citation to the 1988 *Doe* case, which derives the quote "[t]he expression of the contents of an individual's mind falls squarely within the protection of the Fifth Amendment[.]" from a reading of *Boyd*.[162] *Boyd* is also quoted in *Carpenter*, where the opinion argues that the Fourth Amendment seeks to "secure 'the privacies of life' against 'arbitrary power.'"[163] The *Boyd* references in these cases are not essential to their

156. *See* Terzian, *supra* note 111, at 173 (citation omitted) (requiring "knowledge as to the files on the hard drives" and [w]here the location, existence, and authenticity of the purported evidence is known with reasonable particularity, the contents of the individual's mind are not used against him, and therefore no Fifth Amendment protection is available.").

157. Terzian, *supra* note 111, at 173-74; *see also* U.S. v. Fricosu, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012) (stating that "[t]he fact that [the government] does not know the specific content of any specific documents is not a barrier to production"); *cf. In re* Grand Jury Subpoena, Dated April 18, 2003, 383 F.3d 905, 910 ("the government's knowledge of the existence and possession of the actual documents, not the information contained therein, that is central to the foregone conclusion inquiry.").

158. *See* Choi, *supra* note 5, at 188-89; *see e.g.*, Samuel A. Alito, Jr., *Documents and the Privilege Against Self- Incrimination*, 48 U. PITT. L. REV. 27, 73 (1986) ("The Supreme Court has been wary of embracing the required records rule, and government authorities have been markedly reluctant to rely on it.").

159. Choi, *supra* note 5, at 188-89.

160. *Id.*

161. 116 U.S. 616 (1886).

162. *In re* Search of a Residence in Oaklan*d*, 354 F. Supp. 3d at 1015 (quoting Doe v. U.S., 487 U.S. 201, 219 (1988) (Stevens, J. Dissenting) (citing Boyd v. United States 116 U.S. 616, 633-635 (1886).

163. Carpenter v. U.S., 138 S. Ct. 2206, 2214 (quoting Boyd v. U.S., 116 U.S. 616, 630 (1886) (noting that the *Boyd* quotation does specifically refer to the Fourth Amendment, but to the opinion in totality as relating to its analysis of the Fourth and Fifth Amendment).

holdings, but both allude to the principle elucidated in *Boyd*—that the Fourth and Fifth Amendments both exist to secure the "very essence of constitutional liberty and security" against "invasion" of "sacred right(s)."[164]

Boyd occurred in response to an 1874 federal statute that compelled defendants in revenues cases under federal court jurisdiction to produce private books, invoices and papers at court, lest the government attorney's allegations be taken as confessed.[165] Following a civil action under customs revenue laws, relating to unpaid customs fees on glass vases where the government first seized the vases before compelling the business responsible to turn in financial invoices, the Court held the law unconstitutional.[166] The Court held that the seizure efforts ran afoul of both the Fourth and Fifth Amendments:

> [W]e are . . . of opinion that a compulsory production of the private books and papers of the owner of goods sought to be forfeited in such a suit is compelling him to be a witness against himself within the meaning of the Fifth Amendment to the Constitution, and is the equivalent of a search and seizure—and an unreasonable search and seizure—within the meaning of the Fourth Amendment.[167]

The Court also held that the two amendments have an "intimate relation" and mutually "throw great light on each other" as both relate to the personal security of the citizen.[168] For the purposes of protecting private papers against government scrutiny, the Court effectively fused the two amendments.[169]

Boyd's linking of the Fourth and Fifth Amendments is no longer considered good law.[170] However, despite one Supreme Court concurrence

164. *Boyd*, 116 U.S. at 630.

165. *Id.* at 617.

166. *Id.* at 617-18 (noting that the court also held that the civil action undertaken by the government was of a "quasi-criminal" nature due to the penalties and forfeitures for which a defendant would liable if committing an offense against the law).

167. *Id.* at 634-35.

168. *Id.*at 633.

169. Choi, *supra* note 5, at 189.

170. Choi, *supra* note 5, at 192 ("Conventional wisdom has now traveled the opposite extreme, with most jurists convinced the two Amendments share no overlap at all."); *see also e.g.*, Fisher v. United States, 425 U.S. 391, 407 (1976) ("Several of Boyd's express or implicit declarations have not stood the test of time."); Schmerber v. Cal., 384 U.S. 757, 760–72 (1966) (noting that the values of the two amendments "substantially overlap" but not their application). *But see* Richard A. Nagareda, *Compulsion "To Be a Witness" and the Resurrection of Boyd,* 74 N.Y.U. L. REV. 1575, 1642 n.254 (1999) ("The Supreme Court has not definitively resolved the Fifth Amendment status of personal diaries and the like.").

declaring *Fisher*'s act of production doctrine the "death knell" of *Boyd*,[171] the Court has never expressly overruled Boyd's absolute protection of private papers.[172] *Boyd* is also increasingly found in the dicta of cases dealing with smartphones and data encryption.[173] Perhaps, in light of the growing dangers of government technological intrusions into personal spheres, the Court should reconsider whether or not the central holding of *Boyd* was correctly decided.[174]

One scholar, Bryan H. Choi, argues that "[t]he basic tenet of Boyd was that a person's essential "self' extends beyond his ephemeral thoughts and speech to his tangible papers and effects.[175] It is within that meaning that "compulsory production of the private books and papers" of a person was equivalent to "compelling him to be a witness against himself.[176] Choi argues that this comports with the modern use of technology like smartphones, where the massive amount of personal data stored within works like an "artificial extension" of one's brain and a "virtual extension" of the person.[177] Using this construct, the focus of a court inquiry, vis-à-vis a government seizure and/or compelled production/decryption of personal technology, is not the nature of that technology but the "character of the government's action."[178] The fundamental question would be—whether by subpoena, by warrant, or without either—is the government trying to avoid proper Constitutional process through technology?[179] Were this the focus of Court reasoning, as opposed to which Fourth and Fifth Amendment exceptions

171. U.S. v. Doe, 465 U.S. 605, 618 (1984) (O'Connor, J., concurring) ("The notion that the Fifth Amendment protects the privacy of papers originated in *Boyd v. United States*, but our decision in *Fisher v. United States* sounded the death-knell for Boyd."). *But see* Choi, *supra* note 5, at 248 n. 337 (quoting H. Richard Uviller, *Foreword:* Fisher *Goes on the Quintessential Fishing Expedition and Hubbell Is off the Hook,* 91 J. CRIM. L. & CRIMINOLOGY 311, 315 n.20 (2001)) ("Boyd itself was shot down more than once, only to rise again like a Phoenix.").

172. Duong, *supra* note 106, at 333 (citing Fisher*,* 425 U.S. at 414) (majority declining to consider whether the Fifth Amendment would protect a taxpayer from producing his own tax records).

173. *See, e.g.,* Carpenter, 138 U.S. at 2214-17; *Riley*, 573 U.S. at 403; People v. Davis, 2019 CO at ¶19. *But see* Carpenter, 138 U.S at 2253-2255 (Thomas J., dissenting) (accusing the majority of "resurrecting Boyd")*; cf.* Carpenter, 138 U.S at 2271 (Gorsuch J., dissenting) (which is wary of "a return" to Boyd but urges the court to reconsider the scope of the Fourth and Fifth Amendment based on original interpretations of the amendments).

174. *See* Choi, *supra* note 5, at 246.

175. *Id.* at 189; *cf*. Alito, *supra* note 158 ("Boyd was more a defense of property than of privacy.").

176. Choi, *supra* note 5, at 246 (quoting Boyd*,* 116 U.S. at 634-35); *see also* Fisher v. U.S., 425 U.S. 391, 405 (1976) ("The proposition that the Fifth Amendment prevents compelled production of documents over objection that such production might incriminate stems from *Boyd v. United States*.").

177. *See* Choi *supra* note 5, at 244.

178. *Id.*

179. *Id.*; *see also* Carpenter, 138 S. Ct. at 2221 (noting Court's exhortation for the government to fulfill its Constitutional obligations and "get a warrant.").

might apply, the Fourth and Fifth Amendments may more closely fulfill their purpose as protections of the "indefeasible right of personal security, personal liberty, and private property."[180]

To properly constrain and further elucidate this interpretation of *Boyd*, one may look to the original jurisprudence and legal atmosphere at the time of the creation of the Bill of Rights, as the Supreme Court increasingly does today.[181] The Fourth Amendment protects "persons, houses, papers, and effects" against "unreasonable search and seizures."[182] A dictionary from 1755 defines "paper" as "substance on which men write and print" and defines "effects" as "goods (or) movables."[183] It would not be a stretch to define a smartphone as both a movable good and a substance upon which people write and print, thus granting personal smartphones Fourth Amendment protection; likewise, it doesn't strain credulity to says that biometrics—fingerprint, facial shape, genetic markers—are part of the "person" that is to be protected by the Fourth Amendment. As for the Fifth Amendment, it is accepted that at the time of its creation, the Fifth Amendment applied to "natural persons" as opposed to artificial entities.[184] There is also a colorable argument that the Fifth Amendment was intended to be more expansive: that a "witness" was intended to mean "a person who gives or furnishes evidence" and that therefore the amendment was intended to protect against the compelled giving or furnishing of evidence.[185] These interpretations of the Fourth and Fifth Amendments, considered together, would produce a body of law that provided heightened protections against search and seizures of persons and their personal devices, including their biometrics, and heightened protections against compelled production of records. This would likely be more in line with the original interpretations

180. Boyd*,* 116 U.S. at 630.

181. *See, e.g.*, U.S. v. Jones, 565 U.S. 400 (2012) (Applying a traditional trespass-based analysis to a Fourth Amendment question as opposed to the more modern reasonable expectation of privacy test.).

182. U.S. CONST. amend. IV.

183. SAMUEL JOHNSON, A DICTIONARY OF THE ENGLISH LANGUAGE 675,1446 (1st Folio, 1755), https://johnsonsdictionaryonline.com/page-view/ (last accessed April 13, 2019).

184. *See* Alito*, supra* note 158, at 190; *see also* Choi, *supra* note 5, at 240 (citing Braswell v. U.S., 487 U.S. 99, 119 (1988)) (Kennedy, J., dissenting) ("Our . . . decisions concerning artificial entities and the Fifth Amendment . . . illuminated two of the critical foundations for the constitutional guarantee against self-incrimination: first, that it is an explicit right of a natural person, protecting the realm of human thought and expression; second, that it is confined to governmental compulsion.").

185. *See* Duong, *supra* note 106, at 330-31; *see also* U.S. v. Hubbell, 530 U.S. 27, 49 (2000) (Thomas, J. concurring) (Justice Thomas, joined by Justice Scalia, reasoned that "the Fifth Amendment privilege protects against the compelled production not just of incriminating testimony, but of any incriminating evidence" and expressed a willingness to "reconsider the scope and meaning of the Self-Incrimination Clause").

and purpose of the amendments.[186]

V. CONCLUSION

Public comment on *In re Search of a Residence in Oakland* was varied and included some criticism.[187] This is understandable. The majority of Fifth Amendment precedent and scholarship interprets most physical characteristics, and therefore likely biometrics, as nontestimonial and therefore unprotected by Fifth Amendment privilege.[188] The conjoined reading of the Fourth and Fifth Amendment that seems hinted at in *In re Search of a Residence in Oakland* would be counter to the common modern reading of the two amendments as covering fundamentally different spheres.[189] It would be easy to dismiss *In re Search of a Residence in Oakland* as a "baffling" decision unlikely to affect the wider body of law.[190]

To dismiss *In re Search of a Residence in Oakland* is to dismiss a wider change in society, and it could mean dismissing an opportunity for the courts to confront that change. The Supreme Court, in *Riley* and *Carpenter,* has recognized that changing technology, and the opportunity for its abuse, means that an "equilibrium-adjustment" is necessary in how the courts weigh the balance between government power and individual rights.[191] Were the courts to embrace the reasoning within *In re Search of a Residence in Oakland*, and re-embrace at least some of the reasoning behind *Boyd*, the

186. *See* Duong, *supra* note 106, at 335; s*ee also* Choi, *supra* note 5, at 193 ("Somehow, texts that were originally intended to limit government authority have become instruments used to expand it. Our Constitution of limited government has gotten twisted into a government of limited Constitution.").

187. *See, e.g.*, Orin Kerr, *Search Warrants and Compelled Biometric Access to Phones*, REASON: THE VOLOKH CONSPIRACY (Jan. 15, 2019, 5:11 AM), https://reason.com/2019/01/15/search-warrants-and-compelled-biometric ("I agree that the compelled biometric provision is impermissible. But I mostly disagree with Judge Westmore as to why that's the case."); Josephine Wolff*, Biometrics vs. the Fifth Amendment*, SLATE (Jan. 17, 2019 11:24 AM), https://slate.com/technology/2019/01/fifth-amendment-biometrics-fingerprint-search-warrant-ruling.html ("Magistrate Judge Kandis Westmore . . . issued a ruling denying a search warrant that dealt with both Fourth and Fifth Amendment rights and profoundly misunderstand the latter.").

188. *Id.*

189. *See In re* Search of a Residence in Oakland*,* 354 F. Supp. 3d 1010, 1013-14, 1014 n.1 (N.D. Cal. 2019). *Contra* Alito, *supra* note 158, at 36 (discussing the "quite different" and "differently regulated" nature of the Fourth and Fifth Amendment vis-à-vis search and seizure as opposed to subpoena.) ("A search or seizure operates on inanimate objects and does not require the cooperation or even the presence of those who may be adversely affected. A subpoena, by contrast, is directed to a person and seeks to compel his cooperation.").

190. *See* Wolff, *supra* note 187.

191. *See* Orin Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767, 770 (2019) (citing Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment,* 125 HARV. L. REV. 476 (2011) (introducing the concept in the Fourth Amendment context).

courts could ensure that individual rights, especially in regard to digital devices and the biometric locks that are so commonly used with them, are fundamentally protected at a time when technology could allow government power to grow exponentially.[192] Such a change would not be a "death knell" for law enforcement, but simply mean that law enforcement must consider the conditions required for two amendments instead of one.[193] In a time where person and inanimate object are as conjoined as people and their smart phones are, and where cooperation of one is often needed to access the other, considering the search and seizure together with the subpoena may now be reasonable.[194]

As technology races forward at blinding speed, the light of discovery can still leave us in the dark as to how to use that technology, and what it means it for our rights. A "jurisprudential lodestar," a line of reasoning to help courts and scholar articulate standards when balancing technology, government interests, and individual rights, could help us navigate this ever-changing era.[195] *In re Search of a Residence in Oakland* may be too small a decision to be that lodestar, but it does provide a line of reasoning for other courts to consider on an issue that the courts must consider in the future.[196] Ultimately, it may provide the glimmer of a new path for higher courts to walk, a path that would lead to more comprehensive protections for American civil liberties, or at least for American smartphones.[197]

192. *See generally* Choi, *supra* note 5, at 248.

193. *Id*. at 241; *see also In re Search,* 354 F. Supp 3d. at 1014 n.1 ("Probable cause does not permit the Government to compel a suspect to waive rights otherwise afforded by the Constitution, including the Fifth Amendment right against self-incrimination.").

194. *Supra* note 186.

195. *See* Terzian, *supra* note 112, at 307.

196. *See* People v. Davis, 2019 CO 24, ¶21, (referencing *In re* Search of a Residence in Oakland. 354 F. Supp. 3d 1010 (N.D. Cal. 2019)) ("Specifically, courts have begun considering whether the Fifth Amendment allows the government to compel an individual to provide it with his phone passcode or to use a biometric feature such as a fingerprint to unlock his phone.")); *See also* Seth Rosenblatt, *Despite ruling, pro-privacy biometric laws still face long road to change in U.S.*, THE PARALLAX (Jan. 17, 2019), https://the-parallax.com/2019/01/17/biometric-privacy-ruling-slow-change/ ("[o]ver the last 5 to 10 years, magistrates [like Westmore] have been the leading voices on this stuff . . . It's probably is just a matter of time that a case jumps through all the hoops you'd need to reach an appellate court." (quoting Brett Max Kaufman, staff attorney for the ACLU Center for Democracy)).

197. *See* U.S. v. Wright, Case No. 319CR00012MMDWGC1, 2020 U.S. Dist. LEXIS 1414, 2020 WL 60239 (D. Nev. Jan. 6, 2020), referencing *In re Residence in Oakland* at 24-25 ([T]here are fundamental. . .differences between using a biometric feature to unlock a device and submitting to fingerprinting or a DNA swabFalse The Court therefore finds that . . . unlocking of Defendant's phone with his face . . . violated Defendant's Fifth Amendment rights because the unlocking of the phone with Defendant's face was a testimonial act."). *See also* People v. Davis*,* 2019 CO at ¶21, referencing *In re* Residence in Oakland ("Specifically, courts have begun considering whether the Fifth Amendment allows the government to compel an individual to provide it with his phone passcode or to use a biometric feature such as a fingerprint to unlock his phone."). *See also* Seth Rosenblatt, *Despite ruling, pro-privacy biometric laws still face long road to change in U.S.*, THE

PARALLAX (Jan. 17, 2019), https://the-parallax.com/2019/01/17/biometric-privacy-ruling-slow-change/ (". . .over the last 5 to 10 years, magistrates [like Westmore] have been the leading voices on this stuff. . .It's probably is just a matter of time that a case jumps through all the hoops you'd need to reach an appellate court.") (quoting Brett Max Kaufman, staff attorney for the ACLU Center for Democracy).