THE FIFTH AMENDMENT'S PRESSING ISSUE IN THE DIGITAL ERA: PROTECTING YOUR PASSWORD BUT WHAT ABOUT YOUR PRINTS?

Taylor Ichinose[*]

I. INTRODUCTION

Suppose a suspect is detained on criminal charges and there is reason to believe that he or she may be aware of potentially incriminating evidence on his or her cellphone. Could a court order the suspect to use his or her fingerprint to unlock the cellphone to allow the government to investigate? This particular issue becomes intertwined with the Fifth Amendment's protection against compelled testimony.

This Note will explain the historical and judicial background of the privilege against self-incrimination. Then, this Note will explain the relevant technology and cases that apply the *United States v. Doe*[1] analogy. Next, this Note will explore the importance of the right to privacy, its interrelation with the Fifth Amendment, and an originalist application of the privilege in the modern era. Finally, this Note will conclude that regardless of the application of the Fifth Amendment, fingerprints deserve the same equal protection that is currently afforded to passwords.

II. BACKGROUND

A. The History and Evolution of the Fifth Amendment Privilege Against Self-Incrimination

Before applying the Fifth Amendment to technology, it is important to understand its foundation. The Fifth Amendment was revered long before the

---

[*] J.D. Candidate, May 2019, University of Louisville Louis D. Brandeis School of Law. I would like to thank my friends and family who have supported me throughout my academic career. I would especially like to thank my fiancé, Randall Roof, for his constant love and support through the late nights and millions of edits. Lastly, I would like to thank all of those who came before me and who keep fighting the good fight. As Justice Ruth Bader Ginsburg said, "fight for the things that you care about, but do it in a way that will lead others to join you."

[1] *See* Doe v. United States (*Doe I*), 487 U.S. 201, 219 (1988) (Stevens, J., dissenting).

United States was formed.[2] Minimal discussion from the founders makes it difficult to apply this historic concept to the technological era.[3]

1. From Common Law to Colonies: Fifth Amendment Protection Survived

The Fifth Amendment guarantees that no person shall "be compelled in any criminal case to be a witness against himself."[4] Although most recognize it from the Bill of Rights, this privilege can be traced back to English common law and the accusatorial criminal process,[5] and, at least in part, to the Magna Carta.[6] Scholar Leonard W. Levy amassed a detailed history of the Fifth Amendment that traces back to English common law.[7] In 1236, the "oath ex officio" was first introduced to the ecclesiastical courts of England; this forced the declarant to give a sworn statement promising the truth to all answers provided during questioning, while not knowing what he or she was accused of yet.[8] Parliament made failed attempts to enact statutes to prohibit this type of inquisitional oath.[9] The King's Council further enabled the use of the oath by imitation of the ecclesiastical courts.[10] During the fourteenth century, the Court of Star Chamber served as the judicial sector under the Council.[11] In 1557, Queen Mary established the Court of High Commission to conduct inquisitions into treasonable words, offenses against the church, and refusal to conform and attend church; the Commission was given complete discretionary power to use any method or procedure to illicit evidence under the inquisitional oath.[12] In 1583, the oath followed a new

---

[2] *See* LEONARD W. LEVY, ORIGINS OF THE FIFTH AMENDMENT 3–5, 263–65 (1986). The author credits Levy as a thorough source providing the historical background of the Fifth Amendment.

[3] *See id.* at 423.

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

[5] *See* LEVY, *supra* note 2.

[6] Provisions 38 and 39 of the Magna Carta guarantee the right of a person to know what he is accused of and the right to be judged by the law and a jury. "In the future no bailiff shall upon his own unsupported accusation put any man to trial without producing credible witnesses to the truth of the accusation. No free man shall be taken, imprisoned, disseised, outlawed, banished, or in any way destroyed, nor will We proceed against or prosecute him, except by the lawful judgment of his peers and by the law of the land." *See* A.E. DICK HOWARD, MAGNA CARTA: TEXT AND COMMENTARY 43 (1964). This early writing is for the most part consistent with the current Fifth Amendment in modern day America. *Id.*

[7] *See generally* LEVY, *supra* note 2.

[8] *Id.* at 46–47.

[9] *Id.* at 49.

[10] *Id.* (noting that the King's Council served as the judicial, executive, and legislative branch of the country and performed all duties as the most powerful political entity).

[11] *Id.* at 49–50. It used procedures that were unusual at the time. Churchmen that assisted the bishops were placed as chancellors and they applied European law rather than English common law. Initially, the Council used no juries, invited private accusations from informants, and bypassed indictments to go straight to inquisitions under oath. *Id.*

[12] *Id.* at 76.

rule—*pro confesso*—which meant failure to take the oath would result in the conclusion of admittance of guilt.[13]

The privilege against self-incrimination was cited through the Magna Carta in a seventeenth century English case.[14] John Lilburne, an advocate for fundamental rights,[15] stood trial four times in his life and spent most of his adulthood in prisons.[16] He repeatedly denied his accusations and refused to take the oath, which had never been done before.[17] Around 1645, Lilburne was charged with seditious libel[18] when he wrote under a pseudonym in pamphlets.[19] Although it was widely known that Lilburne was the author, under English law, his words could not be used against him without testimony, which he refused to give.[20] Lilburne reasoned that, "no Englishman could be compelled to incriminate himself."[21] His claim succeeded in court and demonstrated the earliest recognition of the privilege against self-incrimination.[22]

In the late eighteenth century, there was a shift in the English criminal justice system from a reply to accusations, to an opportunity for the defense to test the prosecution's case.[23] The privilege evolved in America as part of the adoption of the common law accusatorial system, but it was not adopted uniformly.[24] The colonists brought over the English model of judicial procedures and laws; criminal offenses were governed by common law and thus, the first colonists were most familiar with the application of the

---

[13] *Id.* at 55, 132.

[14] *Id.* at 289–94.

[15] Lilburne was a forward thinker of his time as he challenged procedures due within the English criminal justice system. He was the reason that the oath *ex officio* was abolished in English law and Parliament established the right to hear charges before making any oaths in court. In his trials, he challenged self-incrimination, right to counsel, right to face the accuser, and several other provisions from the Magna Carta and the Petition for Rights. *See generally id.* at 266–300.

[16] *Id.* at 272.

[17] *Id.* at 275.

[18] *Id.* at 288. In 1586, Star Chamber gave power to the Archbishop of Canterbury for censorship and to enforce its policy against books or writings that were seen as offensive to the state or to the church or if they were printed without a license. *Id.* at 270.

[19] WILLIAM J. STUNTZ, THE COLLAPSE OF AMERICAN CRIMINAL JUSTICE 70 (2001).

[20] *Id.*

[21] *Id.*

[22] *Id.* (calling this privilege "Lilburne's Law").

[23] *See generally* John H. Langbein, *The Privilege and Common Law Criminal Procedure: The Sixteenth to the Eighteenth Centuries*, *in* THE PRIVILEGE AGAINST SELF-INCRIMINATION 82–108 (1997).

[24] LEVY, *supra* note 2, at 333 (explaining it is not clear when this developed but, during the colonial period, there were legal inconsistencies in adopting fundamental rights).

common law.[25] Although the application varied in each colony, they collectively used common law as a means to guarantee individual rights.[26]

After the Declaration of Independence, the majority of states provided in their respective constitutions or statutes that they would uphold common law until legislatively altered.[27] In 1776, various states independently decided the privilege against self-incrimination held the status of a constitutional right.[28] Virginia led the way by including it in the preface to the state's constitution; consequently, a majority of the states followed Virginia's example and protected this privilege.[29]

Since the 1700s, the courts have expanded this privilege to include self-production of evidence that might be probative against an individual.[30] A further examination of the courts' expansion of this privilege will be illustrated in Part III of this Note. While this privilege has continually evolved, so has today's society as it moves into the age of technology.

2. The Fifth Amendment and the Founders' Intentions

By 1776, several states established the common law privilege against self-incrimination as a constitutional right.[31] Virginia was one of the initial states to establish rights for the individual in a preface to the state constitution called the "Declaration of Rights."[32] Levy proposes that the original drafting left ambiguity as to the intent of this right.[33] Section 8 of the Virginia Declaration of Rights, drafted by George Mason, stated:

> That in all capital or criminal prosecutions a man hath a right to demand the cause and nature of his accusation, to be confronted with the accusers and witnesses, to call for evidence in his favor, and to speedy trial by an impartial jury of twelve men of his vicinage, without whose unanimous consent he cannot be found guilty; *nor can he be compelled to give evidence*

---

[25] *Id.* at 336.

[26] *Id.* at 337–38. In fact, the First Continental Congress cited common law in their Declaration of Rights and Grievances by asserting that "the respective colonies are entitled to the common law of England." *Id.* (quoting WORTHINGTON C. FORD ET AL., 1 JOURNALS OF THE CONTINENTAL CONGRESS 1774-1789 69 (Washington ed., 1904)).

[27] *Id.* at 338.

[28] *Id.* at 405.

[29] *Id.* at 405–09. The last four to ratify the Constitution had explicitly recommended a bill of rights section, which included a clause against self-incrimination. *Id.* at 418.

[30] *Id.* at 427.

[31] *Id.* at 405.

[32] *Id.*

[33] *Id.* (suggesting that its original draft takes on an ambiguous *nemo temetur seipsum prodere* maxim from common law, which meant "no man is bound to accuse himself").

> *against himself*; that no man be deprived of his liberty, except by the law of the land or the judgment of his peers.[34]

Levy proposes that one ambiguity is in the application of this privilege in proceedings. This drafting bunched the privilege in with the rights of those accused in a criminal setting, which may indicate it was solely intended for criminal proceedings.[35] But Virginia law and eighteenth century trial manuals suggest that it was applicable in protecting parties in civil cases as well.[36] When taken out of context, Levy suggests the right applied to all parties, witnesses, and stages of proceedings.[37] But when applied in context, the suggestion of its application solely to criminal proceedings does not make sense for this time.[38] Levy suggests that this ambiguity by Mason is due to poor draftsmanship.[39] Regardless of this ambiguity, Mason's right against self-incrimination became the model for the other states and ultimately, the Bill of Rights. Eight states followed Virginia's example and added separate bills of rights to their state constitutions.[40] All of those states chose to incorporate this *nemo temetur* privilege.[41]

Although a majority of the states recognized individual rights in prefaces, no "Bill of Rights" was presented at the Constitutional Convention until Mason mentioned it days before it convened.[42] Unfortunately, it was overwhelmingly shot down when put to a vote.[43] The state representatives,

---

[34] *Id.* at 405–06 (emphasis added).

[35] *Id.* at 406.

[36] *Id.* (noting that Virginia law stated, "noe law can compel a man to sweare against himself in any matter wherein he is lyable to corporal punishment").

[37] *Id.*

[38] *Id.* at 407. A criminal defendant was not permitted to testify, nor could he be called as a witness; they would need to prove their case by cross-examining witnesses presented by the prosecution, presenting their own witnesses, and commenting on evidence presented. *Id.*

[39] *Id.* (noting his profession as a planter rather than a lawyer and his mistakes in word choice due to haste). For example, Mason omitted "impartial" before "jury," which he could not have possibly meant to purposely exclude. Additionally, Mason drafted that the right to confrontation applied to the accuser "or" witnesses, rather than "and." *Id.*

[40] *Id.* at 409–10 (noting that Rhode Island and Connecticut chose to uphold their original state charters).

[41] *Id.* at 410. Pennsylvania adopted Section 8 almost in its entirety, specifically adopting the self-incrimination clause verbatim. Other states expanded or altered the privilege. For example, Delaware explicitly expanded the right to witnesses and parties in both criminal and civil cases. Maryland followed Delaware's example but also created exceptions, such as immunity or pardon. Massachusetts chose to say "to accuse, or furnish" instead of "give" regarding evidence that would be self-incriminating. The four states that chose not to include a preface to their constitutions chose to uphold the English common law, including a variation of the privilege. *Id.*

[42] *Id.* at 414–15.

[43] *Id.* at 415; *see also* MAX FARRAND, THE RECORDS OF THE FEDERAL CONVENTION OF 1787 587–88 (2d ed. 1911).

exhausted from four months at the convention, had "planned a government of limited, enumerated powers, making unnecessary, they reasoned, a list of restraints on powers that did not exist."[44] This rationale made little sense given that the proposed constitution protected certain rights, such as the right to trial by jury, but there was nothing to stop the new national government from seizing evidence or using general search warrants; the proposed bills of rights from each state illustrated their belief that they would find security in explicitly protecting certain rights, rather than relying on the good faith of the framers and their new proposed government.[45]

Despite initial opposition, James Madison introduced a Bill of Rights proposal,[46] which included the privilege against self-incrimination:

> No person shall be subject, except in cases of impeachment, to more than one punishment or trial for the same offence; *nor shall be compelled to be a witness against himself*; nor be deprived of life, liberty, or property, without due process of law; nor be obliged to relinquish his property, where it may be necessary for public use, without a just compensation.[47]

Levy suggests that the word choice and placement in this miscellaneous article implies that Madison would apply the privilege to civil and criminal cases and at any stage of the legal process; further, Madison would expand the Fifth Amendment by applying it beyond judicial proceedings into any other type of governmental inquiry.[48] Madison's word choice was more comprehensive and would expand to protect third parties.[49] Madison created a broader amendment than what the states asked of him.

Only one motion regarding the proposed Bill of Rights was made in the House by John Lawrence, who felt that it should be confined to criminal

---

[44] LEVY, *supra* note 2, at 415.

[45] *Id.* at 416.

[46] *Id.* at 422 (noting that Federalists felt the Bill of Rights was unnecessary, while Anti-Federalists sought to halt Madison's proposal). *See also* HELMHOLZ ET AL., THE PRIVILEGE AGAINST SELF-INCRIMINATION: ITS ORIGIN AND DEVELOPMENT 1 (1997). Two anti-federalist delegates—New York and Massachusetts—supported the Bill of Rights by pointing out the potential of the national government to oppress individuals in the criminal justice system. *Id.* at 137. *See also* NEIL H. COGAN, THE COMPLETE BILL OF RIGHTS: THE DRAFTS, DEBATES, SOURCES, AND ORIGINS 315–36 (Oxford Univ. Press 1997). Madison was swayed by Thomas Jefferson and he sought to soothe the cries of the opposing party that created fear that the new national government would take away liberties. *Id.*

[47] LEVY, *supra* note 2, at 422 (emphasis added).

[48] *Id.* at 423.

[49] *Id.* at 424. In a criminal proceeding, witnesses could be compelled to give evidence, while being protected from presenting evidence against themselves if it would open them up to criminal prosecution or civil penalties. In contrast, a criminal defendant and any witness in a civil suit could not be compelled to give testimony at all and were not allowed to present evidence for or against their cases. *Id.*

cases.[50] The amendment was adopted without a discussion or debate.[51] Levy interprets the suggestion literally to severely narrow the interpretation of the Fifth Amendment privilege by excluding parties and witnesses in civil suits and witnesses in non-judicial governmental proceedings, while maintaining full constitutional protection solely in criminal cases.[52]

3. The Founders' Intent and the Right to Privacy: Levy vs. Rossum

Professor Ralph A. Rossum also notes the ambiguity of the original intent of the Fifth Amendment, but, unlike Levy, Rossum attributes the ambiguity to the two interpretations of the amendment that formed since its adoption: the original intention and the widely used reformation.[53] For numerous reasons, Rossum disagrees with Levy's assertion that strict application to criminal proceedings would serve no purpose because of the common law protection barring a criminal defendant from testifying.[54] He believes George Mason and the founders meant exactly what they said and implemented the privilege as a means to explicitly protect an individual from testifying against him or herself, as they are today.[55] Levy's broader interpretation does not consider how the states that drafted their bills of rights after those that expanded the privilege deliberately followed the Virginia model and did not follow the trend of expansion.[56] Rossum proposes that Levy expands the Fifth Amendment too broadly with the intention of allowing the courts to define "self-incrimination" with what is applicable at the time.

Rossum interprets the framers' intent through the purpose and importance of the Bill of Rights.[57] He asserts that Madison did not argue with Lawrence's motion because he felt secure that the Constitution would protect the people regardless.[58] Rossum and Levy agree that Madison did not want to include a Bill of Rights because he did not believe it served a purpose; he had faith in the Constitution itself to protect the people and to limit the power of the national government.[59] Two representatives convinced Congress that

---

[50] *See* COGAN, *supra* note 46, at 317.

[51] *Id.*

[52] LEVY, *supra* note 2, at 425.

[53] Ralph Rossum, *"Self-Incrimination": The Original Intent, in* THE BILL OF RIGHTS: ORIGINAL MEANING AND CURRENT UNDERSTANDING 273 (Eugene W. Hickok, Jr., ed., 1991).

[54] *Id.*

[55] *Id.* at 276–77.

[56] *Id.* at 277.

[57] *Id.* at 273–87.

[58] *Id.* at 282.

[59] *Id.* at 281–83 (For this reason, Madison did not want to separate the Bill of Rights, but rather incorporate it into the Constitution itself. The Constitution and the Bill of Rights had "the same objective—the latter merely declared the rights that the former secured. He saw no need to introduce a

the Bill of Rights should fall at the end of the Constitution so the original framework would be seen greater than the latter.[60] In contrast, the Bill of Rights has not been held to this anticipated standard as society progressed; in recent years, many fundamental rights came from this supplementary document.[61]

Rossum presents the notion that is fundamental to this argument. By creating a balanced government, the framers intended to protect the liberty of the individual, including the privilege against self-incrimination.[62] This privilege was also part of a core element to the right to privacy.[63] This is why Madison did not argue with this privilege in the drafting of the Bill of Rights and why he expanded this right in his initial draft: he knew it was a constitutional guarantee and put his faith in the Constitution and government to protect it.

4. Judicial Development of the Individual Privacy Interest and the Privilege

The progression of the privilege against government compulsion is shown through federal case law. Decided in 1886, *Boyd v. United States*[64] was the first Supreme Court case that analyzed if the privilege would protect an individual from a court ordered production of documents.[65] A court ordered an importing firm to produce an invoice for items it had allegedly received illegally.[66] The Court noted that papers are the owner's "dearest property" and "just as the Fifth Amendment prohibited 'compulsory discovery by extorting the party's oath,' it also prohibited discovery by 'compelling the production of his private books and papers'" because it was no more than another form of forcible compulsion of the defendant's own testimony.[67]

In 1892, in *Counselman v. Hitchcock*,[68] the Court held that a grand jury inquiry into criminal liability is relative to a criminal case and that the Fifth Amendment applies to the eventual use of the testimony; therefore, the Court

---

distinction between them."). *See also* LEVY, *supra* note 2, at 421–22.

[60] ROSSUM, *supra* note 53, at 283.

[61] *Id.* at 284 (explaining that Justice Harlan encapsulated his theory when he said the framers "staked their faith that liberty would prosper in the new nation not primarily upon declaration of individual rights but upon the kind of government that the Union was to have").

[62] *Id.*

[63] *See id.* at 273–84.

[64] 116 U.S. 616 (1886).

[65] WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 8.12, at 489–90 (5th ed. 2004) (discussing Boyd v. United States, 116 U.S. 616 (1886)).

[66] *Id.*

[67] *Id.*

[68] 142 U.S. 547 (1892).

expanded this privilege to a witness in grand jury proceedings because the privilege protects any witness being compelled by a subpoena to testify in any proceeding that might be incriminating in any subsequent criminal case.[69]

Two decades later, the Court started to chip away at the broad property and privacy rights implicated by the Fifth Amendment. In 1906, *Hale v. Henkel*[70] created an exception to the Fifth Amendment protection by holding that the privilege was not applicable to a corporation, because the privilege was designed to protect the individual.[71] The Court weighed the importance of the privilege in protecting the individual's privacy to be let alone and concluded that a corporation does not need this same protection.[72] It was not surprising when the Court rejected the privilege for a corporate officer in *White v. United States* five years later.[73]

Similar to these entity exceptions, the Court further created a required records exception. In 1948, the Court in *Shapiro v. United States*[74] held that the privilege would not extend to records of individuals engaged in regulated businesses.[75] This exception was later clarified in *Marchetti v. United States*,[76] where the Court identified three required elements for the record exception: (1) the government purpose must be regulatory, (2) to obtain the information it must be required to preserve records which the regulatory party would customarily have kept, and (3) the records must have public aspects that make them similar to public documents.[77]

In 1951, *Hoffman v. United States*[78] set forth a standard for potential incrimination:

---

[69] LAFAVE ET AL., *supra* note 65, § 8.10, at 477 (discussing Counselman v. Hitchcock, 142 U.S. 547 (1892)).

[70] 201 U.S. 43 (1906).

[71] LAFAVE ET AL., *supra* note 65, § 8.12(b), at 491 (discussing Hale v. Henkel, 201 U.S. 43 (1906)). The Court additionally held that a state has greater regulatory power over a corporation. *Id.*

[72] *Id.*

[73] *See id.* (discussing White v. United States, 322 U.S. 694 (1944)). The Court reasoned that officers could not ask for this protection against compulsion of records of the entity and not personal records; the Court reaffirmed the *White* reasoning that it is inappropriate for the courts to protect an impersonal collective entity. *Id.*; *see also* Bellis v. United States, 417 U.S. 85 (1974) (discussing the entity exception still applies if the office has a personal interest in the corporation or business).

[74] 335 U.S. 1 (1948).

[75] LAFAVE ET AL., *supra* note 65, § 8.12(c), at 492 (discussing Shapiro v. United States, 335 U.S. 1 (1948)).

[76] 390 U.S. 39 (1968) (the Court rejected challenges to federal wagering tax statutes requiring gamblers to be identified by registering with the government and paying a tax); *see also* Grosso v. United States, 390 U.S. 62 (1968).

[77] LAFAVE ET AL., *supra* note 65, § 8.12(c), at 492–93 (discussing Marchetti v. United States, 390 U.S. 39 (1968)).

[78] 341 U.S. 479 (1951).

> The privilege afforded not only extends to answers that would in themselves support a conviction . . . but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant for a federal crime. [They] must be confined to instances where the witness has reasonable cause to apprehend danger from a direct answer. . . . To sustain the privilege, it need only be evidence from the implications of the question, in the setting in which it is asked, that a responsive answer to the question or an explanation of why it cannot be answered might be dangerous because injurious disclosure could result.[79]

Schmerber v. California[80] became the most notable case to limit *Boyd*. The *Schmerber* Court held that the privilege did not prohibit compulsion of a blood sample from an accused that would later be submitted into evidence at trial; the Court's reasoning hinged on the "compulsion" element, requiring communicative or testimonial evidence to invoke the privilege.[81] The Court found that the compulsion element was not satisfied because forcing the accused to provide a blood sample did not make "a suspect or accused the source of real or physical evidence."[82] The Court limited this privilege to evidence compelled from the contents of the mind, which extraction of communication would reveal.[83]

The privilege was subsequently discussed in two notable cases regarding the compulsion of evidence from third parties. In *Fisher v. United States*,[84] business owners delivered paperwork prepared by their accountants to their attorneys in the process of filing tax returns; in *Couch v. United States*,[85] the proprietress of a restaurant gave financial records to her accountant to prepare her tax returns. Subsequently, the IRS required the accountants in each case to disclose those financial records and in both cases, the parties argued that there was an expectation of privacy when they delivered those records.[86] In both cases, the Supreme Court held that the privilege only applies to being compelled personally, which was not present.[87] In *Fisher*, Justice White

---

[79] *Id.* at 486–87 (1951); *see also* Malloy v. Hogan, 378 U.S. 1 (1964) (when a witness pled guilty to gambling charges and was asked about his employer's activity, the Court held that a response that gives an investigatory lead to other evidence deserves the self-incrimination protection).

[80] 384 U.S. 757 (1966).

[81] *Id.* at 777.

[82] *Id.* at 764.

[83] *Id.*

[84] 425 U.S. 391 (1976).

[85] 409 U.S. 322 (1973).

[86] LAFAVE ET AL., *supra* note 65, § 8.12(e), at 494–95 (discussing third party production of evidence).

[87] *Id.* at 494 ("The Fifth Amendment 'protects against "compelling testimony, not the disclosure of private information."'" (quoting Fisher v. United States, 425 U.S. 391, 410 (1976) (quoting United States v. Nobles, 422 U.S. 225, 233 (1975)))).

noted that producing documents per a subpoena "has communicative aspects of its own, wholly aside from the contents of the papers produced," because it could constitute authentication, acknowledgement of possession, or acknowledgement of existence or control of that evidence.[88] Justice White concluded production violates the privilege if it is compelled, testimonial, and incriminating per the facts and circumstances of each case.[89]

In *United States v. Doe II*,[90] the Court again rejected *Boyd*'s content-based analysis regarding production and followed *Fisher*. The Court held that the contents of the requested documents were privileged under the Fifth Amendment because sole ownership does not differ from personal records.[91] The Court clarified that the privilege applies to the production of the records, not the creation of them; if subpoenaed, a party may create the records, but it is not a violation until it is compelled production.[92]

In *United States v. Hubbell*,[93] the Court elaborated on the "forgone conclusion doctrine" by holding that the commonplace character of a document will not establish its location and its possession as a forgone conclusion. When the government broadly sought compulsion of a large variety of documents, the Court rejected the breadth of the request because it demanded the witness to disclose the existence and location of particular documents, which would be communicative and require the contents of the witness's mind.[94] Overall, this means that personal records are protected, but only insofar that they are testimonial.

B. Fingerprint Biometrics of Cellphones in the Courtrooms

1. Biometrics: What Are They and How Do They Apply to Me?

Biometrics are the "unique physical characteristics, such as fingerprints, that can be used for automated recognition."[95] They are not solely fingerprints, though; biometrics can include identification from palms, eyes,

---

[88] *Id.* at 495 (quoting *Fisher*, 425 U.S. at 410).

[89] *Id.*

[90] 465 U.S. 605 (1984) (where a grand jury issued a subpoena for a large range of records, which the Court rejected because it would require admittance of the existence, possession, control, and authentication of the records).

[91] LAFAVE ET AL., *supra* note 65, § 8.12(f), at 496.

[92] *Id.*

[93] 530 U.S. 27 (2000).

[94] LAFAVE ET AL., *supra* note 65, § 8.13(a), at 499–500. *Compare* Chavez v. Martinez, 538 U.S. 760, 771–72 (2003) (noting that this privilege must be invoked when being subpoenaed), *with* Hiibel v. Sixth Judicial Dist. Court, 542 U.S. 177 (2004) (rejecting the self-incrimination challenge to a defendant refusing to disclose his name pursuant to a state statute).

[95] *Biometrics*, DEP'T. OF HOMELAND SEC. (Feb. 6, 2017), https://www.dhs.gov/biometrics.

facial recognition, etc.[96] Common examples are photographs for U.S. visas and fingerprints entered into databases.[97] While biometric technology is used by various national security entities, it may also be used in the palm of your own hand. Cellphones, laptops, and tablets are all starting to incorporate biometrics into their security measures.[98]

Cellphone technology has come a long way from its first appearance in the 1940s. In 1947, society used car phones, which weighed around eighty pounds.[99] In 1973, Motorola presented the first prototype of a cellphone called the DynaTAC 8000X, which was the first handheld phone; ten years later, it was released to the public.[100] While this was revolutionary at the time, the phone took over ten hours to charge fully and cost $3,995.[101] In the early 1990s, IBM and BellSouth released the first version of what we call a smart phone; the "Simon" was the first touchscreen phone and the first phone with email capability.[102] In 1999, BlackBerry released its first two-way pager that provided email access and web browsing.[103] In 2007, Apple released its very first generation of iPhones.[104] Consider the vast change in under one hundred years; the first phones were a feat to even lift and now, technology can recognize a person by their face or fingerprint.

Another important development was the use of encryption. Encryption "prevents unauthorized access to your data . . . by keeping communication secure between the parties involved."[105] It applies to messages, emails,

---

[96] *Next Generation Identification (NGI)*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi (last visited Feb. 27, 2019).

[97] *Safety & Security of U.S. Borders: Biometrics*, U.S. DEP'T. OF STATE, https://travel.state.gov/content/travel/en/us-visas/visa-information-resources/border-biometrics.html (last visited Feb. 27, 2019).

[98] Lucas Mearian, *Feds Move to Secure Mobile Devices with Machine Learning, Biometrics*, COMPUTERWORLD (Mar. 2, 2018, 3:24 AM), https://www.computerworld.com/article/3259883/mobile-wireless/feds-move-to-secure-mobile-devices-with-machine-learning-biometrics.html.

[99] Corey Protin, *Here's How Drastically Cell Phones Have Changed Over the Past 40 Years*, BUS. INSIDER (July 27, 2017, 8:06 AM), http://www.businessinsider.com/cell-phone-history-cars-mobile-motorola-apple-bell-labs-samsung-google-2017-7.

[100] *Id.*

[101] *Id.* (noting the equivalent to $10,000 today).

[102] Doug Aamoth, *First Smartphone Turns 20: Fun Facts About Simon*, TIME (Aug. 18, 2014), http://time.com/3137005/first-smartphone-ibm-simon/. The "Simon" was eight inches long and weighed over a pound; additionally, its "apps" included a calculator, calendar, fax, mail, note pad, time, and to-do list. *Id.*

[103] *The History of BlackBerry: In Pictures*, TELEGRAPH, http://www.telegraph.co.uk/technology/blackberry/11347347/The-history-of-BlackBerry-in-pictures.html (last visited Feb. 27, 2019).

[104] Christina Caron, *The Times Review of the First iPhone: 'Amazing' but 'Not Perfect'*, N.Y. TIMES (Sept. 12, 2017), https://www.nytimes.com/2017/09/12/technology/personaltech/first-iphone-review.html.

[105] Lee Bell, *Encryption Explained: How Apps and Sites Keep Your Private Data Safe (and Why That's*

applications (apps), bank details, etc.[106] When something is encrypted, the only people that can decrypt the information are the sender and the receiver.[107] Many app developers allow the ability to lock the app with a password or a personal identification number (PIN), so that it is not freely accessible.[108]

In 2016, a survey showed that 95% of Americans own a cellphone of some kind, and 77% of those people have a smartphone.[109] A cellphone is no longer just for making calls like in 1947; it now serves equally as a computer and a communication device.[110] The Supreme Court has recognized that a cellphone stores vast amounts of information and that it has become routine for a person to carry that sensitive information with them, a drastic departure from history.[111] Because of this dependency and regularity, society has acquired a reasonable expectation of privacy for information contained on cellphones.[112]

2. Fingerprint Technology: The Newest Trend

As technology advances, it becomes more difficult to be mindful of fundamental rights as intended by the framers and to apply a reasonably consistent rationale to Fifth Amendment cases. How the privilege against self-incrimination applies to individual citizens and their personal technology is a growing controversy.[113] The question is: does the founders' constitutional amendment protect fingerprint technology?

Apple's "TouchID" is "an easy way to use your fingerprint instead of a password . . . . With just a touch of your finger, the sensor quickly reads your fingerprint and automatically unlocks your device."[114] Not only is fingerprint technology used to lock a product, but it also is used to authorize purchases

---

Important), WIRED (June 5, 2017), http://www.wired.co.uk/article/encryption-software-app-private-data-safe.

[106] *Id.*

[107] *Id.*

[108] *Id.*

[109] *Mobile Fact Sheet*, PEW RES. CTR. (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/mobile/.

[110] Riley v. California, 573 U.S. 373, 393–97 (2014).

[111] *Id.*; *see also* United States v. Flores-Lopez, 670 F.3d 803, 804–06 (7th Cir. 2012).

[112] United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008). *See also* Marcia Hofman, *Apple's Fingerprint ID May Mean You Can't Take the Fifth*, WIRED (Sept. 12, 2013, 09:29 AM), https://www.wired.com/2013/09/the-unexpected-result-of-fingerprint-authentication-that-you-cant-take-the-fifth/.

[113] *See infra* notes 114–40 and accompanying text.

[114] *About TouchID Advanced Security Technology*, APPLE, https://support.apple.com/en-us/HT204587 (last visited Feb. 27, 2019).

and to sign in to apps.[115] Almost all Apple products are now being made with this optional security feature.[116] Apple uses a clear material to protect the sensor and to focus on the finger when it is pressed; the steel ring around the button detects the finger and tells the program to start reading for the user's fingerprint.[117] The sensor "maps out individual details in the ridges . . . and even inspects minor variations in ridge direction caused by pores and edge structures."[118] TouchID is programmed to read multiple fingerprints at different angles of orientation; when users enroll their fingerprints in the product, TouchID does not store the image of the finger, but rather a mathematical representation.[119] Apple is not the only company that implements this measure of security.[120] With this growing trend in biometric security, it is important for individuals to know if they are protected from being forced to actively participate in testifying against themselves. This scenario is starting to make its way into the courts, and those courts have cited the same authority as its foundational starting point.

In *Doe I*,[121] John Doe was subpoenaed by a federal grand jury to produce records of transactions from international bank accounts. However, he only produced some records and invoked his Fifth Amendment privilege regarding the existence and location of additional records.[122] When the grand

---

[115] *Id.*

[116] Including the newest versions of the iPhones, iPads, and laptops. *See Macbook Pro*, APPLE, https://www.apple.com/macbook-pro/ (last visited Feb. 27, 2019); *iPad*, APPLE, https://www.apple.com/ipad/ (last visited Feb. 27, 2019); *iPhone*, APPLE, https://www.apple.com/iphone-8/specs/ (last visited Feb. 27, 2019).

[117] *See Macbook Pro*, APPLE, https://www.apple.com/macbook-pro/ (last visited Feb. 27, 2019); *iPad*, APPLE, https://www.apple.com/ipad/ (last visited Feb. 27, 2019); *iPhone*, APPLE, https://www.apple.com/iphone-8/specs/ (last visited Feb. 27, 2019).

[118] *See Macbook Pro*, APPLE, https://www.apple.com/macbook-pro/ (last visited Feb. 27, 2019); *iPad*, APPLE, https://www.apple.com/ipad/ (last visited Feb. 27, 2019); *iPhone*, APPLE, https://www.apple.com/iphone-8/specs/ (last visited Feb. 27, 2019).

[119] *See Macbook Pro*, APPLE, https://www.apple.com/macbook-pro/ (last visited Feb. 27, 2019); *iPad*, APPLE, https://www.apple.com/ipad/ (last visited Feb. 27, 2019); *iPhone*, APPLE, https://www.apple.com/iphone-8/specs/ (last visited Feb. 27, 2019).

[120] *See Use the Fingerprint Scanner on Your Samsung Galaxy Tab S*, SAMSUNG, http://www.samsung.com/us/support/answer/ANS00044932/ (last visited Feb. 27, 2019); *Understand Fingerprint Security*, GOOGLE, https://support.google.com/pixelphone/answer/6300638 (last visited Feb. 27, 2019); *Use Fingerprint Security—Moto G Plus 4th Generation*, LENOVO, https://mobilesupport.lenovo.com/us/en/solution/MS110999 (last visited Feb. 27, 2019). *See also* Robert Triggs, *How Fingerprint Scanners Work: Optical, Capacitive, and Ultrasonic Variants Explained*, ANDROID AUTH. (July 9, 2016), http://www.androidauthority.com/how-fingerprint-scanners-work-670934/ (explaining how fingerprint scanners work in technology); *Qualcomm 3D Sonic Sensor*, QUALCOMM, https://www.qualcomm.com/products/features/security/fingerprint-sensors (last visited Sept. 14, 2017) (explaining how fingerprint sensors work).

[121] 487 U.S. 201, 202 (1988).

[122] *Id.* at 202–03.

jury subpoenaed the banks, they refused to turn over records of accounts under Doe's authority without his consent.[123] The government filed a motion to order Doe to sign forms giving his consent to production of bank records and any other documents from bank accounts that he was suspected of controlling.[124] Doe was found to be in civil contempt of both the district court and Fifth Circuit for refusing to sign.[125]

The Supreme Court held that ordering Doe to sign the documents was not a violation of his Fifth Amendment privilege.[126] The Court reasoned that the Fifth Amendment only protects a person against incriminating himself by "his own compelled testimonial communications."[127] "Testimonial" communication occurs when an "accused's communication [] itself, explicitly or implicitly, relate[s] a factual assertion or disclose[s] information. Only then is a person compelled to be a 'witness' against himself."[128] The Court's determination of the compulsion to testify or provide the state testimonial evidence hinged on whether there was a disclosure of knowledge or an attempt to "force him to 'disclose contents of his own mind.'"[129] Here, the government tried to compel Doe to sign a form and it was not interpreted as an acknowledgement of an account existing or in his control, which otherwise would have been testimonial.[130] The Court reasoned that while it would give the government access, it does not guide them toward discovery of the evidence—which is the government's job—nor does it assist in the prosecution.[131] The Court held that the government did not require any statement by Doe, nor did it authenticate any records recovered from the banks.[132] It compared this order to previously upheld directives, such as producing handwriting samples or voice samples; neither case was considered testimonial, because it did not require any sort of disclosure of knowledge.[133]

In Justice Stevens's dissent, he drew the line at the point where the accused is actively aiding the prosecution in convicting him or herself.[134] He stated, "he may in some cases be forced to surrender a key to a strongbox

---

[123] *Id.* at 203.
[124] *Id.*
[125] *Id.* at 205.
[126] *Id.* at 206.
[127] *Id.* at 207 (quoting Fisher v. United States, 425 U.S. 391 (1976)).
[128] *Id.* at 210.
[129] *Id.* at 211 (quoting Curcio v. United States, 354 U.S. 118, 128 (1957)).
[130] *Id.* at 214–15.
[131] *Id.* at 213–15.
[132] *Id.* at 215.
[133] *Id.* at 217.
[134] Doe v. United States (*Doe I*), 487 U.S. 201, 219 (1988) (Stevens, J., dissenting).

containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe—by word or by deed."[135] The majority believed the actions in the case related more to the key rather than the combination.[136]

Thus, the next question to ask with fingerprint technology is whether the compulsion of a fingerprint is a directive, like giving over the key to the strongbox, or is it testimonial, like revealing the combination to the wall safe?[137] This analogy is the standard that courts use in similar proceedings involving self-incrimination and the compulsion of evidence from the accused.[138] Further, this analogy leads to the question of whether this reasoning is aligned with the framers' intent when drafting the Fifth Amendment.

Multiple jurisdictions specifically faced with locked cellphones cases have applied *Doe I*'s approach to order the accused to provide their fingerprint. First, a Virginia circuit court, Florida court of appeals, Minnesota court of appeals, federal district court in California, and a federal district court in Texas each issued court orders or warrants to compel the defendant to unlock a cellphone with their finger.[139] Second, a federal magistrate judge in Illinois declined to follow this approach and denied the government's application for a search warrant because it was faced with the additional legal question of ownership.[140] While these are the only jurisdictions known to

---

[135] *Id.*

[136] *Id.* at 210 n.9.

[137] *See id.* at 219.

[138] *See infra* notes 146–71 and accompanying text.

[139] *See* State v. Stahl, 206 So. 3d 124 (Fla. Dist. Ct. App. 2016); State v. Diamond, 890 N.W.2d 143 (Minn. Ct. App. 2017); Commonwealth v. Baust, 89 Va. Cir. 267 (Va. Cir. Ct. 2014). *See also Federal Jury Finds Dallas Man Guilty of Child Sex Trafficking*, U.S. DEP'T OF JUST. (Feb. 15, 2017), https://www.justice.gov/usao-ndtx/pr/federal-jury-finds-dallas-man-guilty-child-sex-trafficking; Matt Drange, *Feds Want to Use Your Fingerprints to Open iPhones. Why Isn't it Working?*, FORBES (July 22, 2016, 8:30 AM), https://www.forbes.com/sites/mattdrange/2016/07/22/feds-want-to-use-your-fingerprints-to-open-iphones-why-isnt-it-working/#4bc286476891; Matt Hamilton & Richard Winton, *The Government Wants Your Fingerprint to Unlock Your Phone. Should That Be Allowed?*, L.A. TIMES (Apr. 30, 2016, 3:00 AM), http://www.latimes.com/local/california/la-me-iphones-fingerprints-20160430-story.html; Matt Hamilton, *Search Warrant for Glendale iPhone*, L.A. TIMES (May 2, 2016), http://documents.latimes.com/search-warrant-glendale-iphone/; Thomas Fox-Brewster, *Feds Walk into a Building, Demand Everyone's Fingerprints to Open Phones*, FORBES (Oct. 16, 2016), https://www.forbes.com/sites/thomasbrewster/2016/10/16/doj-demands-mass-fingerprint-seizure-to-open-iphones/#df286381288f.

[140] *See* Cyrus Farviar, *Judge: No, Feds Can't Nab All Apple Devices and Try Everyone's Fingerprints*, ARS TECHNICA (Feb. 23, 2017), https://arstechnica.com/tech-policy/2017/02/judge-no-feds-cant-nab-all-apple-devices-and-try-everyones-fingerprints/. *See also In re Application for a Search* Warrant, No. 1:17-mc-00081 (N.D. Ill. Feb. 2, 2016), https://www.documentcloud.org/documents/3472990-NDIL-Opinion-Rejecting-TouchID-SW-on-4A-amp-5A.html#document/p4/a339534 (copy of the opinion and order).

have ruled on the issue, it will be a question presented to all courts as technology continues to advance and society continues to rely on it.

III. ANALYSIS

Courts are following a trend that distinguishes a password from a fingerprint. This section will analyze the Fifth Amendment protection that the courts currently provide and how that corresponds to the fingerprint passwords in biometrics.

A. Biometrics: Next on the Docket

The privilege against self-incrimination starts to become unclear when a password is involved, especially if it is biometrically linked. After all, the fingerprint is the most personal and intimate password of them all, but is it testimonial or is it just a directive? Some courts have held that encrypted data cannot be accessed because it is testimonial and requires the contents of a defendant's mind.[141] Other courts have taken the opposite approach and have found it is not a Fifth Amendment violation to compel passwords or unencrypted data.[142]

This creates tension between states seeking justice through investigating cases and the interests of the individual's Fifth Amendment privilege. The individual has a constitutional right not to testify against himself in court and requiring the accused to unlock their phone with their fingerprint may be equivalent; on the other hand, the state has an interest in enforcing justice and investigating cases that may cause disorder and danger.[143] The individual's constitutional rights are not absolute, but there is no affirmative duty to incriminate oneself; there is merely the duty to not obstruct justice.[144] The state does not have unlimited power to enforce justice; it must always bear in mind the individual's rights and limit its actions accordingly.[145] The Supreme

---

[141] United States v. Doe, 670 F.3d 1335, 1345 (11th Cir. 2012).

[142] *See* United States v. Smalcer, 464 F. App'x 469 (6th Cir. 2012); United States v. Fricosu, 841 F. Supp. 2d 1232 (D. Colo. 2012); *In re* Boucher, No. 2:06-MJ-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009). *See also* David Kravets, *Man Jailed Indefinitely for Refusing to Decrypt Hard Drives Loses Appeal*, ARS TECHNICA (Mar. 20, 2017, 6:11 PM), https://arstechnica.com/tech-policy/2017/03/man-jailed-indefinitely-for-refusing-to-decrypt-hard-drives-loses-appeal/.

[143] *See* David Kravets, *supra* note 142.

[144] Kessler v. State, 991 So. 2d 1015, 1021 (Fla. Dist. Ct. App. 2008) (stating that the Fifth Amendment "protects an accused from being compelled to testify against himself, or otherwise provide the state with evidence of a testimonial or communicative nature").

[145] *See* Patrick M. Garry, *Liberty Through Limits: The Bill of Rights as Limited Government Provisions*, 62 SMU L. REV. 1745, 1745–48 (2009).

Court will inevitably be asked to look at fingerprint passwords and their testimonial value.

There have been several cases where courts have ordered the criminally accused to press his or her finger on a cellphone to unlock it and allow investigation within the device.[146] The first case was from Virginia in 2014. In *Commonwealth v. Baust*,[147] a victim of assault alleged that the defendant had texted videos of them engaging in sexual intercourse. Pursuant to a search warrant, the police retrieved the phone, recording devices, discs, flash drives, and computer equipment; however, the phone could not be unlocked without a passcode or fingerprint.[148] The court recognized the three Fifth Amendment requirements.[149] However, it differentiated compelling a person to follow a directive that might lead to incriminating evidence and using compulsion to extract testimony.[150] The court quoted *Hubbell*:

> Even though the act may provide incriminating evidence, a criminal suspect may be compelled to put on a shirt, to provide a blood sample or handwriting exemplar, or to make a recording of his voice. The act of exhibiting such physical characteristics is not the same as sworn communication by a witness that relates either express or implied assertions of fact or belief.[151]

The court held that a defendant cannot be compelled to produce a password to a cellphone, but may be required to unlock it with a fingerprint.[152] It reasoned that the video on the cellphone was created voluntarily, and therefore, the contents within it that are created voluntarily are not protected.[153] Following *Doe I*'s analogy, the court held that the fingerprint is no more than a key, requiring no mental divulging of information or communication of knowledge.[154] The holding from this case created many implications for modern America. It created a distinction between a password and a fingerprint, which are now regularly used synonymously. The fingerprint serves as a password of sorts, but this court created the implication that only a lettered or numbered password will be

---

[146] *See* discussion *supra* Section III.A.
[147] 89 Va. Cir. 267 (Va. Cir. Ct. 2014).
[148] *Id.* at 267–68.
[149] *Id.* at 268.
[150] *Id.* at 269.
[151] United States v. Hubbell, 530 U.S. 27, 35 (2000).
[152] *See* Commonwealth v. Baust, 89 Va. Cir. 267, 271 (Va. Cir. Ct. 2014).
[153] *Id.*
[154] *Id.*

protected.[155] It lumped the fingerprint into a category of a directive and made this "safety feature" essentially pointless; in other words, while it is safe in common usage, it is not safe in a courtroom—where liberty and privacy should be protected most. Shortly after this case, another motion to compel fingerprints was granted in the Eastern District of Michigan.[156]

In 2016, a similar case arose in Florida. In *State v. Stahl*,[157] the defendant was charged with video voyeurism and he consented to his phone being searched after giving over the cellphone type and its location; he withdrew consent after its retrieval from his residence.[158] The police were unable to unlock the cellphone without a passcode, and the defendant refused to provide it.[159] Applying *Baust*, the court held that the Fifth Amendment does not provide any additional protection to cellphones that are locked with passwords instead of fingerprints; it reasoned that the information on the cellphone is not protected and is similar to the key per *Doe I*.[160] The court stated that testimonial communication can be explicit or implicit, so long as it relates a factual assertion or discloses information.[161]

The implication is that using a fingerprint to unlock a cellphone does not explicitly or implicitly give over any information, which is an incorrect assumption.[162] A fingerprint can disclose information implicitly by allowing the state to go through a cellphone and thereby, perhaps, finding incriminating information which can be used as evidence in a case against the individual. It does not matter if a defendant is speaking or not; this compulsion is an implicit disclosure of facts. As these cases demonstrate, globalization is leading to a diminished right to privacy.

In 2017, a case in Minnesota presented the same issue. In *State v. Diamond*,[163] the police sought a warrant for the defendant's property after they suspected he was involved in a robbery. The police seized his cellphone to search and his shoes to compare to the footprint found at the scene.[164] The detective was unable to unlock the cellphone, so the State filed a motion to

---

[155] *Id.*

[156] Hall, *E.D. Mich.: Government's Motion to Compel Fingerprinting of Person in Custody on Indictment Granted*, FOURTHAMENDMENT.COM (Apr. 16, 2014), http://fourthamendment.com/?p=10967 (quoting United States v. Adams, No. 13-20874, 2014 U.S. Dist. LEXIS 51735 (E.D. Mich. 2014)).

[157] 206 So. 3d 124, 127 (Fla. Dist. Ct. App. 2016).

[158] *Id.* at 128.

[159] *Id.*

[160] *Id.* at 133–35.

[161] *Id.* at 132.

[162] *Id.*

[163] 890 N.W.2d 143 (Minn. Ct. App. 2017).

[164] *Id.* at 145–46.

compel the defendant's fingerprints.[165] The court affirmed the production of a fingerprint was not testimonial; it further reasoned that taking samples of all of the defendant's fingerprints without asking—which would unlock the cellphone—did not show any acknowledgement of possession, control, or any disclosure of information.[166]

Additionally, a federal judge granted a motion to compel a defendant in Texas to unlock his cellphone.[167] The defendant's iPhone was locked with his fingerprint and the Federal Bureau of Alcohol, Tobacco, Firearms, and Explosives sought to go through emails, texts, contacts, and photos to link the defendant to a sex trafficking case.[168] In 2016, this same request was granted by a federal court in Oakland, California when authorities got a search warrant to compel the girlfriend of an alleged Armenian gang member to unlock a cellphone seized from the home; the cellphone used Apple's fingerprint encryption and could not be unlocked by authorities.[169]

One judge has denied this type of motion. A federal judge in Chicago denied the government's motion to compel all people within a building to press their fingerprint onto any seized Apple devices that were locked as part of a child pornography investigation; this was due to a lack of specified facts of who might be involved.[170] While this case presents a legal question involving the identity of the accused, the court recognized that the context of how the fingerprints are taken can raise concerns.[171] The implications of this case demonstrate that the states' police power is not absolute, as they must abide by and weigh the constitutional protections granted to the citizens of this country.

B. Fingerprint vs. Password: To Protect or Not To Protect

As the above cases demonstrate, the courts have drawn a line between the protection of a cellphone with a numerical or linguistic password and a fingerprint-protected cellphone. One has shown to deserve more protection than the other. It appears that there is a judicial struggle with the entire concept of the fingerprint.[172] In the most literal interpretation, it is not

---

[165] *Id.* at 146.

[166] *Id.* at 150–52.

[167] *See* U.S. DEPT. OF JUST., *supra* note 139.

[168] Drange, *supra* note 139; *see also* U.S. DEPT. OF JUST., *supra* note 139.

[169] Hamilton & Winton, *supra* note 139.

[170] Farviar, *supra* note 140.

[171] *Id.*

[172] Jack Linshin, *Why the Constitution Can Protect Passwords But Not Fingerprint Scans*, TIME (Nov. 6, 2014), http://time.com/3558936/fingerprint-password-fifth-amendment/.

testimonial; it does not speak to any facts other than identity.[173] Fingerprints are used in police stations to verify an individual's identity and are even used when traveling; they have been integrated into the criminal justice system. But the fingerprint has become more than this interpretation. Now, the issue hinges on what is associated with that fingerprint.[174] Today, so much personal information has become associated with a fingerprint.[175]

The courts all recognize that a password in the traditional sense is explicitly protected. In *United States v. Kirschner*,[176] the defendant invoked his Fifth Amendment privilege against testifying in a grand jury proceeding to give a password for his computer.[177] The court held that giving a password forces communication of information by requiring the defendant to communicate knowledge.[178] The court quashed a subpoena from the government and noted that compulsion of testimony that "may 'lead to incriminating evidence' is privileged even if the information itself is not inculpatory."[179] The implications from similar cases are that the Fifth Amendment will protect an individual from testifying to passwords to devices such as computers and cellphones. This interpretation of the Fifth Amendment will allow the privilege to grow with advancing society.

So why is the password different from the fingerprint? The knowledge behind a password compared to the physical fingerprint is essential to courts' determinations. They see that the privilege "may not apply when it comes to biometric-based fingerprints (things that reflect who we are) as opposed to memory-based passwords and PINs (things we need to know and remember)."[180] They have decided that fingerprints carry no knowledge because they do not reveal anything the accused might know; this rationale is being carried to all biometrics, such as DNA, voice, and writing samples.[181] Delving into the minds of individuals and requiring them to give over

---

[173] *Id. See also* Hoffman, *supra* note 112.

[174] *See* Kara Goldman, *Biometric Passwords and the Privilege Against Self-Incrimination*, 33 CARDOZO ARTS & ENT. L.J. 211, 211–12 (2015).

[175] *Id.* at 229 (noting that things such as bank records, telephone bills, and personal correspondences can be created and stored in digital forms and sometimes can replace hard copies, which is dangerous to give over access to).

[176] 823 F. Supp. 2d 665 (E.D. Mich. 2010).

[177] *Id.* at 668.

[178] *Id.* at 669 (citing United States v. Doe, 487 U.S. 201, 212 (1987)).

[179] *Id.* (citing United States v. Hubbell, 530 U.S. 27, 38 (2000)).

[180] Hoffman, *supra* note 112.

[181] *Id. See also* United States v. Mara, 410 U.S. 19 (1973) (writing exemplars); United States v. Dionisio, 410 U.S. 1 (1973) (voice exemplar); Gilbert v. California, 388 U.S. 263 (1967) (writing exemplars); Schmerber v. California, 384 U.S. 757 (1966) (blood samples).

knowledge is seen as abhorrently violating their constitutional rights. The password is not absolutely protected, though.[182]

While it is comforting to know that passwords may be protected, this distinction is troubling to the twenty-first century cellphone user. Some have said that with fingerprints, "you're not using your brain, ... It can't be testimonial if you cut their finger off."[183] The courts view the fingerprint as a key and the phone as a strongbox; in reality, the fingerprint is the password combination to a safe.[184] One argument is that the fingerprint is only matching a stored image to unlock a phone.[185] Albert Gidardi, Director of Privacy at Stanford University's Center for Internet and Society, stated, "when you put your fingerprint on the phone, you're actually communicating something, . . . You're saying 'Hi, it's me. Please open up.'"[186] The purpose of the fingerprint is to communicate information and serve as a replacement for the traditional password.[187] Today, the fingerprint is a proxy password.[188] "An iPhone user preloads his fingerprint onto the memory of his device to ensure his privacy and only he, as the owner, can access the device."[189]

Companies like Apple have begun to also worry about this vulnerability. Apple created an emergency mode on its newer phones, which disables the fingerprint reader and requires a password.[190] Also, if the phone is plugged into a computer, it now requires a PIN or passcode instead of the fingerprint.[191] A PIN or passcode is required when a phone is turned on after it has not been used after so many days. Moreover, the use of the fingerprint is not the only quality similar to a password, but how it is set up. To set up

---

[182] Jeff Welty, *Update on Fingerprints, Phones, and the Fifth Amendment*, N.C. CRIM. L. (Jan. 23, 2017), https://nccriminallaw.sog.unc.edu/update-fingerprints-phones-fifth-amendment/. If it is a foregone conclusion that the evidence in question belongs to the defendant, the court may compel them to testify to the password; if a defendant is given adequate immunity, the court might also rule that providing a password is permitted. *Id.*

[183] Farivar, *supra* note 140.

[184] Orin Kerr, *The Fifth Amendment and Touch ID*, WASH. POST (Oct. 21, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/21/the-fifth-amendment-and-touch-id/?utm_term=.74fcbe6b193b.

[185] Vindu Goel, *That Fingerprint Sensor on Your Phone is Not as Safe as You Think*, N.Y. TIMES (Apr. 10, 2017), https://www.nytimes.com/2017/04/10/technology/fingerprint-security-smartphones-apple-google-samsung.html.

[186] Kaveh Waddell, *Can Cops Force You to Unlock Your Phone with Your Face? Apple's New Face ID Technology Raises Questions About Constitutional Protections for Personal Devices*, ATLANTIC (Sept. 13, 2017), https://www.theatlantic.com/technology/archive/2017/09/can-cops-force-you-to-unlock-your-phone-with-your-face/539694/.

[187] Goldman, *supra* note 174, at 229.

[188] *Id.* at 211–12.

[189] *Id.* at 229.

[190] Waddell, *supra* note 186.

[191] *Id.*

TouchID on the iPhone, a password must be created first and thus, the fingerprint is linked to the password.[192]

C. How Does This Affect the Fifth Amendment Right?

1. The Fifth Amendment and the Right to Privacy

Oftentimes, an individual's "right to privacy" is interrelated with the Fifth Amendment.[193] If a court orders compulsion of certain evidence, it could violate an individual's right to privacy.[194] To understand the right, it is important to understand what "privacy" itself means. Within the last fifty years, privacy rights arose in a series of Supreme Court cases and have become valued in society.[195] Webster's Dictionary defines "privacy" as "the quality or state of being apart from company or observation; freedom from unauthorized intrusion."[196] This broad definition includes any type of intrusion or invasion that someone might not want.

In comparison, Black's Law Dictionary defines privacy as "the quality, state, or condition of being free from public attention to intrusion into or interference with one's acts or decisions."[197] Under "privacy," three types of privacy are notable: (1) autonomy, (2) informational, and (3) personal.[198] Autonomy is defined as the individual's right to control their personal activities or personal decisions without outside interference, observation, or intrusion.[199] Informational privacy developed from tort law and is defined as "a private person's right to choose to determine whether, how, and to what extent information about oneself is communicated to others."[200] Personal privacy is defined as "a person's interest in nondisclosure or selective disclosure of confidential or private information or matters relating to his or her person."[201] Erwin Chemerinsky, noted constitutional law scholar, also supports this idea of different types of privacy. He identifies three different

---

[192] *Use Touch ID on iPhone and iPad*, APPLE, https://support.apple.com/en-us/HT201371 (last visited Mar. 1, 2019).

[193] *See* discussion *infra* Section II.C.1 and accompanying notes.

[194] *See* discussion *infra* Section II.D and accompanying notes.

[195] *See generally* Erwin Chemerinsky, *Rediscovering Brandeis's Right to Privacy*, 45 BRANDEIS L. J. 643, 643–57 (2007).

[196] *Privacy*, MERRIAM WEBSTER'S DICTIONARY, https://www.merriam-webster.com/dictionary/privacy (last visited Feb. 27, 2019).

[197] *Privacy*, BLACK'S LAW DICTIONARY (10th ed. 2014).

[198] *Id.*

[199] *Id.* (noting further that if it is a fundamental activity or decision, the state must present a compelling interest that surpasses the private interest and if so, the court must apply a balancing test).

[200] *Id.* (noting that this particularly revolves around sensitive and confidential information).

[201] *Id.*

types of privacy rights: (1) freedom from government intrusion into an individual's home or person, (2) freedom to make personal decisions, and (3) the ability to restrict dissemination of personal information.[202]

In 1890, Louis D. Brandeis and his law partner Samuel D. Warren wrote an article called *The Right to Privacy*.[203] Justice Brandeis acknowledged this fundamental right to privacy decades before he would become a Supreme Court Justice, and long before the Supreme Court would even discuss the right.[204] Brandeis wrote, "that the individual shall have full protection in person and in property is a principle as old as the common law."[205] He discussed how the right to privacy includes the "right to be let alone":[206]

> The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others. Under our system of government, he can never be compelled to express them (except upon the witness stand); . . . . The existence of this right does not depend upon the particular method of expression adopted. It is immaterial whether it be by word or by signs, in painting, by sculpture, or in music. Neither does the existence of the right depend upon the nature or value of the thought or emotions, nor upon the excellence of the means of expression.[207]

While primarily talking about the media invading individuals' private lives with their publications, Justice Brandeis and Warren established that there is a fundamental right to privacy.[208] They noted while it is not absolute, it is a constitutional right and should be protected.[209] Further, they recognized that the state must present a compelling interest that will outweigh the individual's privacy interest when it seeks to infringe upon this autonomy right.[210] This same privacy notion is a core rationale behind the Fifth Amendment's self-incrimination clause. Remarkably ahead of their time, this notion was reflected in the Supreme Court's subsequent cases.[211]

---

[202] Chemerinsky, *supra* note 195, at 645–49.

[203] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). *See generally* Chemerinski, *supra* note 195, at 643–57.

[204] *See generally* Chemerinsky, *supra* note 195.

[205] Warren & Brandeis, *supra* note 203, at 193.

[206] *Id.*

[207] *Id.* at 198–99.

[208] *See id.*

[209] *Id.* at 214–19.

[210] *Id.*

[211] *See* Tehan v. United States *ex rel.* Shott, 382 U.S. 406, 416 (1966). Justice Stewart described self-incrimination: "like the guarantees of the Fourth Amendment, [it] stands as a protection of quite different

Justice Brandeis' dissent in *Olmstead v. United States*[212] emphasized the importance of privacy:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect . . . . They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred as against the government, the right to be let alone-the most comprehensive of rights and the right most valued by civilized men. . . . And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth.[213]

While some may consider the worth of privacy to society a value judgment, the Constitution and case law support the high value of privacy.[214] This privacy interest serves as a core element of an individual's liberty interest; it is the control over our intimate integrity and decision making.[215] This "encompasses the ability to withhold information about ourselves, or reveal it, as we choose."[216] Compelling testimony raises concerns because it invades this privacy interest—specifically, if the court lacks grounds to do so and is effectively fishing for information.[217] Then it becomes an intrusion on the individual's liberty without a compelling interest. But this "privacy" that we want to protect so dearly is an evolving concept.

With technology growing and globalizing, the scope of our privacy interest is becoming narrower. The internet makes information significantly more accessible to the public—the common user—and thereby, information, once private, is now exposed in a quick Google search.[218] Technology makes accessing information quicker and more efficient, but it can sacrifice privacy in doing so. With technology advancing, it may become easier to invade a person's privacy, thus making it nearly nonexistent in a public setting.[219]

---

values—values reflecting the concern of our society for the right of each individual to be let alone." *Id.*

[212] 277 U.S. 438 (1928).

[213] *Id.* at 478–79 (1928) (Brandeis, J., dissenting).

[214] MARK BERGER, TAKING THE FIFTH 43 (1980).

[215] *Id.*

[216] *Id.*

[217] *Id.*

[218] *See* Flerida Ruth P. Romero, *Legal Challenges in Globalization*, 15 IND. INT'L & COMP. L. R. 501, 503 (2005).

[219] Bridget A. Sarpu, *Google: The Endemic Threat to Privacy*, 15 J. HIGH TECH. L. 97, 106–07 (2014) ("[L]ack of privacy in public is 'even more troubling since technology has evolved to invade privacy in more surreptitious and invasive ways than Warren and Justice Brandeis could have ever imagined.'" (quoting Josh Blackman, *Omniveillance, Google, Privacy in Public, and the Right to Your Digital Identity:*

Justice Brandeis and Warren's "right to let alone" clashes with many internet apps that are common today, such as social networking, Google mapping services, or facial recognition on Facebook or iPhoto.[220] This further enables the idea that compelling the accused to provide his or her fingerprint is not considered an intrusion on something personal, but rather, it is now freely available.[221] It is becoming difficult for the courts to recognize that with developing technology and publicity, a fingerprint guards a large amount of personal information; it should be "understood as something private and subject to protection, like a password, rather than a photograph that is easily obtainable by the public."[222] Although technology constantly changes, the right to privacy should not.

2. Originalism and the Privilege: The Right to Privacy

Rossum argues that the framers intended to maintain a balanced government that would protect a defendant against self-incrimination through his or her right to privacy.[223] The framers' intent was to limit the government's power and to maintain checks and balances; the idea of compelling testimonial evidence from the accused is counterintuitive to their intent.[224] Doing so would create a broader police power for the government and expand the power in a way that the framers feared.[225] When Madison drafted the Bill of Rights, he believed all of those rights would be secured by the separation of powers, federalism, and democracy; he believed that the newly structured government would not violate the Fifth Amendment, which is why he did not object when it was limited by Laurence's motion.[226]

Madison believed the Constitution would serve as a safeguard to "secur[e] the public good, and private rights, against the danger of a [tyrannical majority]."[227] The framers were explicitly concerned about private rights being infringed by expanding government power.

Technology is diminishing Justice Brandeis and Warren's right to be let alone, but it should not do so. The right to privacy is a fundamental "right

---

A Tort for Recording and Disseminating an Individual's Image Over the Internet, 49 SANTA CLARA L. REV. 313, 319 (2009))).

[220] *Id.* at 110–14.

[221] Goldman, *supra* note 174, at 226.

[222] *Id.*

[223] ROSSUM, *supra* note 53, at 279.

[224] *Id.*

[225] *See id.* at 273–87.

[226] *Id.* at 282.

[227] *Id.* at 273.

that was within the Framers' contemplation."[228] By compelling a defendant to reveal a passcode, or use the fingerprint proxy, it is not only invading privacy, but it is forcing active participation in that infringement. The framers might have not contemplated the existence of biometrics, but they did contemplate the weight and importance of protecting citizens' privacy from the government, which was a matter of utmost importance to them.

3. Possible Implications for the Criminal Justice System and Police Power

Not only are individuals' privacy interests being marginalized, but courts' compulsion orders also have adverse effects within the criminal justice system. First, using fingerprint technology, and biometrics in general, may limit an individual's opportunity to invoke the privilege.[229] It removes the need to compel a defendant to produce a passcode or PIN and thus, it gives the government more access to devices once a search warrant is obtained.[230] Once done, the accused has a very slim chance at successfully proving that his or her privilege has been violated, because the courts do not view this violation as compelled testimony.[231]

Second, a defendant is forced to serve as physical evidence to strengthen the state's case against him or her. Using the accused serves to provide more reliable proof that "the accused has knowledge, possession, or control over the incriminating evidence."[232] If the fingerprint was uploaded to the phone from the sole user to ensure privacy and it was previously used to access the contents, a "court [will] easily come to the conclusion that he is the owner of the phone as well as its contents."[233] A defendant should not serve as an authenticator for the state in a case against himself or herself.

Finally, by allowing the government more access, the institutions gain more police power without consideration of the diminution of the right to privacy and constitutional protections. The courts acknowledge that the privilege does not protect the content within technology itself, but rather, the compulsion of testimonial knowledge from a defendant; however, this compulsion by the government goes beyond its police powers. Through the Tenth Amendment, the states retain this police power to promote public

---

[228] *Id.*

[229] Erin M. Sales, *The Biometric Revolution: An Erosion of the Fifth Amendment Privilege to Be Free from Self-Incrimination*, 69 U. MIAMI L. REV. 193, 232 (2014).

[230] *Id.*

[231] *Id.*

[232] *Id.* at 235.

[233] *See* Goldman, *supra* note 174, at 229.

safety, health, and morals.[234] While the government has a strong interest in promoting this by investigating criminal activity, it must be weighed against the infringement of the defendant's constitutional rights. In a criminal justice system that is constantly being called on for reform, the courts cannot allow shortcuts on constitutional rights.

IV. RESOLUTION

Fingerprints deserve Fifth Amendment protection because the courts should not compel a defendant to unlock his or her cellphone with a fingerprint. Even under an originalist application, the framers' intent and our history and tradition demonstrate that this protection expands even in this technological era. The courts are following the correct rationale but are improperly analyzing the fingerprint itself in their application. This Note proposes that courts apply the Fifth Amendment to protect a defendant from being compelled to provide their fingerprint and advises the courts to find the balance between the individual's right to privacy and the state's interests in the modern era.

A. Originalism and the Self-Incrimination Privilege

Our founders had the foresight to recognize that issues would arise with our system of government. Justice Brewer said, "the Constitution is a written instrument. As such, its meaning does not alter. That which it meant when adopted it means now."[235] It does not matter if cellphones or biometrics were not in the contemplation of the framers. The framers had foresight to recognize there might be a point in time, like there had been before, where a court might try to compel a defendant to testify, implicitly or explicitly, against himself or herself; thus, the framers explicitly created that protection for them. That protection should be applied today as it would be applied then: it should shield the individual from testifying against themselves. Essentially, placing a finger on a cellphone is just that—compelling a defendant to actively serve as evidence against him or herself. It is not the directive that courts have applied it as; rather, it represents the privacy of the individual and it is implicitly communicative.

---

[234] *See* Santiago Legarre, *The Historical Background of the Police Power*, 9 U. PA. J. CONST. L. 745, 745 (2007).

[235] South Carolina v. United States, 199 U.S. 437, 439 (1905). *See generally* Antonin Scalia, *Originalism: The Lesser Evil*, 57 U. CIN. L. REV. 849 (1989).

Further, the Fifth Amendment itself is deeply rooted in the history and tradition of our country.[236] *Nemo tenetur seipsum accusare* or "no one is bound to accuse himself" was a common law right.[237] It was brought from our roots in England to the colonies and used long before it was placed in the Constitution as a historical practice of our courts.[238] The privilege was so fundamentally important to the framers that it was adopted by each of the states before it was explicitly implemented in the Bill of Rights.[239]

Justice Thomas and Justice Scalia analyzed the history, tradition, and scope of the Fifth Amendment in *United States v. Hubbell*.[240] The Justices acknowledged that the meaning of "witness" at the time of the framers had a broader meaning of "a person who gives or furnishes evidence."[241] The broad definition of "witness" was supported by the eighteenth century common law privilege and it was "an ancient principle of the law of evidence."[242] The Justices also noted Madison's phrasing deliberately substituted "to be a witness" for "to give evidence" and "to furnish evidence" in response to prominent voices.[243] Madison's language attracted very little opposition or attention, but when it did, the phrases were treated synonymously.[244] The Justices noted the term "witness" is consistent in both the Fifth and Sixth Amendments, and ultimately adopted the broader definition as Chief Justice Marshall did in his interpretation of the Sixth Amendment shortly after the adoption of the Bill of Rights.[245]

In a parallel discussion of the Fourth Amendment, in *Kyllo v. United States*,[246] Justice Scalia said, "it would be foolish" to believe that the privacy interest of the individual has been unaffected by technological advances.[247] The Court held that thermo-imaging was an unlawful invasion of privacy without a warrant; while this was a relatively new advancement in technology, it was challenged by the protections guaranteed in the Constitution.[248] Writing for the majority, Justice Scalia recognized that the Constitution itself does not change with technology; rather, it is applied to

---

[236] *See supra* Sections II.A and II.B.

[237] LEVY, *supra* note 2, at 42.

[238] *Id.* at 333.

[239] *See supra* Section II.A.

[240] 530 U.S. 27, 49–55 (2000) (Thomas and Scalia, JJ., concurring).

[241] *Id.* at 50 (noting the support from legal dictionaries at this time and no change in definition until 1828).

[242] *Id.* at 51 (quoting Counselman v. Hitchcock, 142 U.S. 547, 563–64 (1892)).

[243] *Id.* at 53.

[244] *Id.* at 53.

[245] *Id.* at 54 (discussing United States v. Burr, 25 F. Cas. 30 (Va. 1807)).

[246] 533 U.S. 27 (2001).

[247] *Id.* at 33.

[248] *Id.* at 40.

new situations and can still work with modern advances.[249] Using this analysis, the courts should protect a defendant from being compelled to provide his or her fingerprint through their interpretation of the Fifth Amendment.

B. Privacy: The Double-Edged Sword

As discussed above, it would seem that advances in technology diminish the right to privacy, but this is not always the case. Technology can enhance privacy. For example, in the 1950s, credit cards were mostly flimsy paper and when a person sought to use one, the clerk would have to imprint the image; the credit card number would be stored on a piece of paper all day for the clerk to hold.[250] Today, a person merely swipes his or her card, which is significantly more protective of privacy than the imprint being held all day. While this technological progress protects privacy, it also has flaws.[251] Very few, if any, technologies will be inherently privacy-protecting or inherently privacy-diminishing.[252]

Noted computer crime law professor Orin Kerr believes an "equilibrium adjustment" is the courts' response to growing technology.[253] When new technology is introduced to expand the police power of the government, he proposes the courts should adjust the level of protection afforded to privacy to try and restore equilibrium between the two competing interests.[254] By doing so, the court acts as a "correction mechanism"; in the past, when it was easier for the government to access information through technology, the Supreme Court would adopt a high level of individual protection, but when

---

[249] *Id.* at 36 ("[T]he rule we adopt must take account of more sophisticated systems that are already in use or in development.").

[250] Livia Gershon, *Brief History of the Credit Card*, JSTOR DAILY (Nov. 14, 2016), https://daily.jstor.org/a-brief-history-of-the-credit-card/.

[251] *See* Bill Hardekopf, *This Week in Credit Card News: Hacks at Sonic, Whole Foods; Equifax Offers Free Lifetime Credit Lock*, FORBES (Sept. 29, 2017), https://www.forbes.com/sites/billhardekopf/2017/09/29/this-week-in-credit-card-news-hacks-at-sonic-whole-foods-equifax-offers-free-lifetime-credit-lock/#41fb860b35e2; *see also* Selena Larson, *The Hacks That Left Us Exposed in 2017*, CNN (Sept. 20, 2017), http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html.

[252] Benjamin Wittes & Jodie C. Liu, *The Privacy Paradox: The Privacy Benefits of Privacy Threats*, BROOKINGS (May 21, 2015), https://www.brookings.edu/research/the-privacy-paradox-the-privacy-benefits-of-privacy-threats/ (a door is a privacy enhancing technology because it blocks out the outside world, but it is not absolute with peeking in keyholes or listening through a door).

[253] *See generally* Orin S. Kerr, *An Equilibrium-Adjustment Theory on the Fourth Amendment*, 125 HARV. L. REV. 476 (2011).

[254] *Id.* at 480.

technology made it harder for the government, it would adopt a lower standard of protection.[255]

Recognizing the government has an interest in promoting justice and safety that should be balanced against the individual's Fifth Amendment right, this Note suggests that the courts must restore equilibrium with fingerprint technology. To maintain this equilibrium, courts should hold that the compelled fingerprint is equal to a compelled password. To allow this compulsion is an imbalance in favor of the government's interest and creates an easy mechanism to search cellphones. Thus, a court should seek an equilibrium adjustment and implement a higher level of protection for the individual.[256] As discussed above, the Court has held that passwords to computers are protected and in today's society, a cellphone works equivalently to a computer. Thus, if a fingerprint were treated as a password, it would maintain that same protection from being compelled to unlock a device.

V. CONCLUSION

Following the framers' intent of the Fifth Amendment, an individual should be protected from testifying against himself or herself. This privilege is ingrained in American history and tradition since its founding. In the modern era, this privilege is still applicable and workable with technology continually advancing. Applying the privilege, the courts should recognize that a fingerprint is no longer solely a fingerprint; it is the gateway to sensitive, personal information and now serves as a proxy passcode. As such, it should be given the same constitutional protection as a password. The courts should apply a heightened protection because it is becoming exceedingly easy for the government to infringe individuals' constitutional rights and doing so would maintain equilibrium throughout the technological era.

---

[255] *Id.*
[256] *Id.*