Catholic University Journal of Law and Technology

Volume 31
Issue 1 *Fall 2022*

Article 8

2022

# Passcodes, Protection, and Legal Practicality: The Necessity of a Digital Fifth Amendment

Ethan Swierczewski
*Catholic University of America (Student)*

# PASSCODES, PROTECTION, AND LEGAL PRACTICALITY: THE NECESSITY OF A DIGITAL FIFTH AMENDMENT

*Ethan Swierczewski*

Nothing encapsulates the advancement in cellular phone technology this century better than the phrase "out with the old and in with the new." Every year, many smartphone users wait with bated breath for an announcement from their tech company of choice about the developer's new smartphone, complete with fancy updates from the previous model and features aimed at outdoing their competitors.[1] Smartphone technology has progressed from its early days, and some even argue that the progression has reached the point of transitioning from "novel to normal" in modern life.[2] In the early 2000s, the ability to make a simple phone call, author a text message, or listen to your favorite new artist via your cellphone was novel, but today's smartphones make these capabilities seem archaic when compared with the ability to video call, update any one of a number of social media profiles, and play a high-quality video game almost simultaneously on today's smartphones.[3]

Our expectations of our smartphones have evolved considerably, but not only in terms of entertainment value. Smartphones give us directions, take and store our photographs, hold thousands of emails and work-related files, carry emergency medical information, and even function as our credit and debit cards.[4] Given the convenience of doing these activities and storing this information via our phones, it is easy to take for granted the vastness and variety

1 *See* Shira Ovide, *Smartphones Won. We Can Ignore Them.*, N.Y. TIMES https://www.nytimes.com/2021/08/12/technology/new-smartphone-models.html (Aug. 25, 2021).

2 *Id.*

3 *See generally* Ivana Križanović, *Cell Phone History: From the First Phone to Today's Smartphone Wonders*, VERSUS, https://versus.com/en/news/cell-phone-history (Dec. 2, 2021).

4 *See generally* Sarah Crow, *20 Things You Didn't Know Your Smartphone Could Do*, BESTLIFE (May 15, 2018), https://bestlifeonline.com/surprising-smartphone-features/.

of information they hold. The evolution of the smartphone passcode makes this reality even less apparent.

At their best, security protocols lock down the information we keep on our phones from outsiders. Whether one uses an alphanumeric passcode, such as a pin number, a word phrase, or a biometric protection, such as a thumbprint or facial-recognition scan, these protective layers allow us to store private information on our devices with less anxiety over prying eyes.[5] The type of protection we choose to lock our phones, however, has implications beyond keeping thieves and peers from accessing our private information.[6] Given the different kinds of information we now choose to store on our phones, and the sheer amount of data present on any given device, it comes as no surprise that law enforcement has taken a vested interest in being able to access that information in their pursuit of evidence for alleged crimes.[7] For example, after discovering the existence of potentially inculpatory evidence contained on a suspect's cell phone in a case involving sex trafficking in Massachusetts, police sought to compel the individual to enter their phone's passcode, revealing the entirety of the device's contents.[8] Faced with the prospect of police asking to go through your phone, it is safe to surmise that many would be hesitant to turn over such an intimate device for a seemingly uninhibited search. A refusal to voluntarily turn over the phone would, in theory, lead to a warrant ordered by a judge, compelling the device's unlocking.[9] Things are not so simple when it comes to the compelled production of an unlocked smartphone, a complexity on which few states have agreed.[10] This is due in large part to advancements in smartphone security, and the differences between alphanumeric passcodes and

---

5 Courtney Linder, *So, You Locked Yourself Out of your iPhone. Now What?*, POPULAR MECHS. (July 15, 2022), https://www.popularmechanics.com/technology/gadgets/how-to/a25092/locked-out-of-phone-guide/.

6 Jon Schuppe, *Give Up Your Password or Go to Jail: Police Push Legal Boundaries to Get into Cellphones*, NBC NEWS (June 7, 2019), https://www.nbcnews.com/news/us-news/give-your-password-or-go-jail-police-push-legal-boundaries-n1014266.

7 Sara Morrison, *The Police Want Your Phone Data. Here's What They Can Get—and What They Can't*, VOX (Oct. 21, 2020), https://www.vox.com/recode/2020/2/24/21133600/police-fbi-phone-search-protests-password-rights.

8 Commonwealth v. Jones, 117 N.E.3d 702, 706 (Mass. 2019).

9 *Compare In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1013 (N.D. Cal. 2019) (Ord. Denying Application for a Search Warrant), *with In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1018 (N.D. Cal. 2019) (Ord. Sealing Application) (discussing an example of the search warrant in question).

10 Scott Ikeda, *New Jersey Supreme Court Rules Phone Passcodes are Not Protected by Fifth Amendment*, CPO MAG. (Aug. 24, 2020), https://www.cpomagazine.com/data-privacy/new-jersey-supreme-court-rules-phone-passcodes-are-not-protected-by-fifth-amendment/.

biometric security methods.[11]

State and federal judges have differed on granting warrants to law enforcement to compel production of smartphone passcodes.[12] The question of law at the center of the split is how the production of smartphone passcodes fits within the protection offered by the Fifth Amendment.[13] The Fifth Amendment right in question is the protection against self-incrimination; stating "[n]o person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury . . . nor shall be compelled in any criminal case to be a witness against himself . . . ."[14] This amounts, in simpler terms, to a right to refrain from providing legal "testimony" against oneself.[15] What amounts to "testimony" is the crucial inquiry in debate between judges across the country—does the compelled production of one's smartphone passcode to police amount to a testimonial self-incrimination barred by the Fifth Amendment?[16] State courts have failed to arrive at a uniform consensus and a well-defined answer to this question has yet to be offered by the Supreme Court.[17] This paper will show that smartphones are deserving of a stringent Fifth Amendment protection scheme, one that can be rooted in a reimagined act of production, foregone conclusion, and private papers doctrine.

This article will proffer a new legal framework regarding smartphone passcodes and their relation to the Fifth Amendment, filling a gap left by prior Supreme Court rulings. First, it will outline the current variety of legal frameworks surrounding the compelled production of smartphone passcodes, demonstrating biometric passcodes as a catalyst for change in Fifth Amendment interpretations across state courts. Next, it will discuss the pertinent history of the Fifth Amendment in relation to self-incrimination, the act of production doctrine, the foregone conclusion doctrine, and the history of "private papers." Finally, it will argue for a more robust protection for smartphones and their passcodes while allowing for narrow exceptions. This will be achieved through a synthesis of historical Fifth Amendment doctrines with current Supreme Court precedents on smartphone protection and technology. The result will be a modernized Fifth Amendment framework of protection for smartphones, one

---

11 *Oakland*, 354 F. Supp. 3d at 1015–16.

12 Kaveh Waddell, *Can Cops Force You to Unlock Your Phone With Your Face?*, ATLANTIC (Sept. 13, 2017), https://www.theatlantic.com/technology/archive/2017/09/can-cops-force-you-to-unlock-your-phone-with-your-face/539694/.

13 *Id.*

14 U.S. CONST. amend. V.

15 Rachel Kraus, *The Face ID Ruling is a Big Win for Digital Rights. Here's What Needs to Happen Next*, MASHABLE (Jan. 17, 2019), https://mashable.com/article/police-force-you-unlock-iphone-faceid.

16 *Id.*

17 *Id.*

that the Supreme Court must address to solve the current inconsistencies in interpretation between the states.

## I. THE ISSUE: THE CURRENT VARIETY IN LEGAL INTERPRETATION OF THE SMARTPHONE PASSCODE

Across the country, state courts are split on how to interpret the question of whether the compelled unlocking of a smartphone amounts to a testimonial incrimination barred by the Fifth Amendment.[18] This question largely boils down to a legal determination of what incrimination counts as testimonial and what counts as nontestimonial.[19] To be considered testimonial, "an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information."[20] Historically, smartphone passcodes were comprised of alphanumeric characters or patterns; the dispute in front of state courts was thus a question of whether these snippets of factual information could be compelled from an individual without violating the Fifth Amendment.[21] That analysis turned largely on whether a combination of alphanumeric characters or patterns could be considered "testimonial"; in jurisdictions that hold these characters as such, the smartphone is protected.[22] That analysis changed with the introduction of biometric passcodes due to a major distinction between security methods: passwords and codes are information a user knows, while biometrics are a *part* of that user.[23] Now, state courts are tasked with the determination of whether physical attributes can relay factual information for purposes of being testimonial.[24] Consequently, many courts have held that biometric passcodes are nontestimonial as they require no "cognition or speech"; while a password contains information such as letters and numbers, a thumbprint or facial scan requires no "mental effort."[25] Such an interpretation provides a loophole within the Fifth Amendment, whereby law enforcement is able to compel an individual to unlock their smartphone with their thumb or face with almost no grounds for protest from the user.[26] A reduction in digital privacy at the hands of technological advancement seems paradoxical. This incongruity is not without

---

18 *Id.*
19 *Id.*
20 Doe v. United States, 487 U.S. 201, 209–210 (1988).
21 *See* State v. Andrews, 234 A.3d 1254, 1274 (N.J. 2020) (discussing that the compelled act of producing passcodes is presumptively protected by the Fifth Amendment regardless of whether the passcode was alphanumeric or biometric).
22 Morrison, *supra* note 7.
23 Waddell, *supra* note 12.
24 *Id.*
25 Kraus, *supra* note 15.
26 *Id.*

a resolution however; a new legal perspective on how to interpret biometric passcodes, one that considers the smartphone's unique place in modern society, in conjunction with the Fifth Amendment, necessitates a new framework of protection for the device.[27] The current variety in legal interpretation largely ignores the devices' uniqueness, creating a circuit split where jurisdictions apply the same Fifth Amendment doctrines with disparate results.[28] The split has created two interpretive camps: one that believes that smartphones and their passcodes fall within Fifth Amendment protection, given their contents and the information conveyed in their unlocking, and another that believes they fall within the foregone conclusion exception to the amendment.[29]

On January 10, 2019, Judge Kanis Westmore, a magistrate judge in the Northern District of California, denied the application for a search warrant seeking to compel two suspects in an extortion case to unlock their smartphones using biometric features.[30] While Westmore ruled that the search warrant in question was unreasonably overbroad in violation of the Fourth Amendment, she also held that compelling an individual to use their thumbprint or face to unlock a smartphone is testimonial for two reasons: one, because such an act serves the same function as a passcode; and two, the act conveys potentially self-incriminating information, such as ownership.[31] In conjunction with her commentary on the Fifth Amendment, Westmore justified her decision by arguing that the law has failed to keep pace with technology's fast-paced evolution.[32] The "broad array of private information" that a single smartphone can contain today is like nothing the legal sphere has seen previously.[33] In sum, Jamie Williams, an EFF Staff Attorney, "recognized that given the sheer amount of data on modern day cell phones, the government simply cannot anticipate the full contents of someone's phone, and any order compelling someone to unlock their phone — whether via a numeric passcode or a fingerprint scan — violates the Fifth Amendment privilege against self-incrimination."[34] Using the opportunity created by the novel technology of biometric and facial-recognition passwords, Westmore set the stage for state courts across the nation to substantiate or invalidate her position on the Fifth Amendment's relationship to the smartphone.[35]

---

27 *Id.*

28 Morrison, *supra* note 7.

29 *See generally* Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 FORDHAM L. REV. 203 (2018).

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

31 *Id.* at 1015–16.

32 *Id.* at 1014.

33 *Id.* at 1017.

34 Kraus, *supra* note 15.

35 *Oakland*, 354 F. Supp. 3d at 1017.

In the summer of 2020, two state courts were faced with similar cases involving search warrants, smartphone passcodes, and the Fifth Amendment.[36] On August 10, 2020, the Supreme Court of New Jersey, held that law enforcement officers were able to compel production of an individual's smartphone passcode without violating the Fifth Amendment.[37] While the court remarked on the inconsistencies in the legal treatment of biometric and facial-recognition passcodes versus alphanumeric passcodes, they came to the conclusion that a heightened Fifth Amendment protection for both types of security protocols did not exist, and their unlocking instead fell within an exception to the amendment, namely, the foregone conclusion doctrine.[38] Further, they explained that, unlike Westmore, they arrived at this conclusion by focusing solely on the passcodes themselves and not in conjunction with the contents of a smartphone.[39] Thus, New Jersey analyzed facts similar to those presented in the search warrant Westmore ruled on and arrived at the opposite conclusion regarding both alphanumeric and biometric passcodes alike.[40] Not all state courts were so quick to push back on Westmore's assessments, however.[41]

The Indiana Supreme Court arrived at the same conclusion as Westmore just two months before the New Jersey decision, holding that the Fifth Amendment barred such a warrant for the unlocking of smartphones.[42] The Court remarked that such a compelled production would amount to a "fishing expedition"[43] whereby law enforcement could "scour [a] device for incriminating information."[44] They worried that as technology continues to evolve at breakneck speed, "to hold otherwise would sound 'the death knell for a constitutional protection against compelled self-incrimination in the digital age.'"[45] The court disagreed with the idea of ignoring what they referred to as the "unique ubiquity and capacity" of smartphones to hold vast amounts of data, much of it personal.[46] Similar to the New Jersey decision, the Indiana court treats alphanumeric, biometric, and facial recognition security protocols as one and the same, except in this instance they are all extended protection under the Fifth

---

36 Ikeda, *supra* note 10.

37 State v. Andrews, 234 A.3d 1254, 1274 (N.J. 2020).

38 *Id.* (The foregone conclusion doctrine will be discussed further in more detail in the next section of the article).

39 *Id.* at 1275 (discussing that even if they considered the phones' contents, they would have arrived at the same conclusion given what the State already knew was on the phones).

40 *Id.* at 1274.

41 Seo v. State, 148 N.E.3d 952, 958 (Ind. 2020).

42 *Id.* at 955.

43 Ikeda, *supra* note 10.

44 *Seo*, 148 N.E.3d at 958.

45 *Id.*

46 *Id.* at 959.

Amendment.[47] Most importantly, the Indiana decision expanded on Westmore's rationalization that using the Fifth Amendment to shield the smartphone from compelled unlocking required viewing the smartphone passcode in conjunction with the vast amount of information it protects from prying eyes.[48]

So, what has accounted for the differences in interpretation between New Jersey and Indiana on Westmore's theorization of Fifth Amendment protection for smartphone passcodes and the smartphone itself? It all comes down to the application of different doctrines and exceptions under the Fifth Amendment and how the courts apply them to smartphones—particularly the foregone conclusion doctrine.[49] Resolution of this disagreement across state courts will only be achieved with Supreme Court interpretation, but a coherent legal framework that extends heightened Fifth Amendment protection to smartphones and their passcodes is necessary to ensure the rights guaranteed by the amendment remain effectual in the digital age. In order to demonstrate what this framework should look like and what standards the Supreme Court should adopt concerning the way in which smartphones are to be legally analyzed, a synthesized history of Fifth Amendment doctrine is necessary.

## II. BACKGROUND

### A. The Act of Production Doctrine

The Fifth Amendment protection against self-incrimination involves three prongs relating to the communication of information.[50] A close reading is necessary to understand what the prongs and subject-matter of the amendment entail. The Fifth Amendment states the following:

> No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without

---

47 *See generally id.* (referring to all forms of smartphone security by the arbitrary terminology of "password" and "passcode").

48 *Id.* at 959–60.

49 *Compare* State v. Andrews, 234 A.3d 1254, 1274 (N.J. 2020) (contending that the foregone conclusion doctrine can be expanded into cases dealing with smartphones and likewise applies here), *with Seo*, 148 N.E.3d at 958 (cautioning against the expansion of the foregone conclusion doctrine into cases dealing with smartphones and likewise holding that it does not apply here).

50 Hiibel v. Sixth Judicial Dist. Court, 542 U.S. 177, 189 (2004).

> due process of law; nor shall private property be taken for public use, without just compensation.[51]

The three-part test for whether a communication falls within the protection of the amendment is as follows: the communication must be "testimonial, incriminating, and compelled."[52] A testimonial communication is where "an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information."[53] An incriminating communication refers to disclosures, information, or "testimony which could be used to convict him of a crime in another jurisdiction."[54] A compelled communication is one that does not "allow a citizen to remain silent when asked a question requiring an incriminatory answer."[55] These prongs, and the test for whether a communication is self-incriminatory as a whole, are relatively clear as to what communicative phrases or statements need to be included in order to be protected.[56] What this standard does not address, however, is how communicative acts may fit within this schema of protection.[57] Thumbprint and facial scans are not testimony on their face, and even alphanumeric passcodes have been regarded as holding "minimal testimonial value."[58]

While engaging in a physical act may have the effect of producing self-incriminating information, this does not make the act of producing the information incriminating as well.[59] The Supreme Court in *United States v. Hubbell* discussed the differences between using compulsion to gain information from an individual and compelling that person to act.[60] In short, "the act of exhibiting such physical characteristics is not the same as a sworn communication by a witness that relates either express or implied assertions of fact or belief."[61] The Court used examples such as compelled blood samples, handwriting, and voice recordings.[62] How then could a person's thumbprint, iris, or face be any different?

The Supreme Court has not unilaterally regarded acts as one-dimensional vehicles for incriminating testimony. It is well-understood that acts have the

---

51 U.S. CONST. amend. V.
52 *Hiibel*, 542 U.S. at 189.
53 Doe v. United States, 487 U.S. 201, 209–10 (1988).
54 Kastigar v. United States, 406 U.S. 441, 456 (1972).
55 *Id.* at 461.
56 Charles Gardner Geyh, *The Testimonial Component of the Right Against Self-Incrimination*, 36 CATH. U. L. REV. 611, 642 (1987).
57 Waddell, *supra* note 12.
58 State v. Andrews, 234 A.3d 1254, 1266 (N.J. 2020).
59 United States v. Hubbell, 530 U.S. 27, 34–35 (2000).
60 *Id.*
61 *Id.* at 35.
62 *Id.*

capacity to be "communicative" in themselves.[63] In other words, an act can do more than produce incriminating evidence—it can be incriminating itself.[64] In *Fisher v. United States*, the Supreme Court outlined a doctrine under the Fifth Amendment that has since been denoted as the "act of production" doctrine.[65] In the context of subpoenas, the Court in *Fisher* drew a distinction between the information contained within produced evidence and the act of production of that evidence itself:

> The act of producing evidence in response to a subpoena nevertheless has communicative aspects of its own, wholly aside from the contents of the papers produced. Compliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer. It also would indicate the taxpayer's belief that the papers are those described in the subpoena.[66]

The act of production doctrine effectively states that the act of "compelled production" of information may itself incriminate the individual disclosing the information by showing that the information exists, is in the person's control, and is authentic.[67] This is in addition to the incriminatory nature of the produced information itself.[68] In the context of smartphone passcodes, this would equate to the act of unlocking the phone conveying the fact that the phone contains information (exists), is within the owner's control, and is the phone in question that law enforcement is seeking. At its simplest, it seems as though the act of production doctrine's application to smartphones would provide unfettered protection to devices, as any unlocking would convey these three potentially incriminating bits of information (existence, control or ownership, and authenticity). However, the Court in *Fisher* did not extend such an uninhibited right.[69] When the government chooses to compel production of potential evidence from a suspect, the suspect's act of producing the evidence and the evidence itself may violate their "fifth amendment rights, but the two must be evaluated separately."[70]

In *Fisher*, "[t]he end sought—the document itself—was testimonial and incriminating, but not compelled. The means on the other hand—the act of producing the document—was compelled. The ends and the means, however,

---

63 Fisher v. United States, 425 U.S. 391, 410 (1976).

64 *Id.*

65 United States v. O'Shea, 662 F. Supp. 2d 535, 544 (S.D.W. Va. 2009).

66 *Fisher*, 425 U.S. at 410.

67 Peter Thomson, *The Fifth Amendment's Act of Production Doctrine: An Overlooked Shield Against Grand Jury Subpoenas Duces Tecum*, 20 FED. SOC'Y REV. 4, 6 (2019).

68 *Fisher*, 425 U.S. at 410.

69 *Id.* at 410–411.

70 Geyh, *supra* note 56, at 639.

could not be combined to form a single Fifth Amendment violation."[71] The act of production in that case was compelled by the government, and even testimonial because it conveyed the existence, control, and authenticity of the documents in question.[72] However, the communicative act that conveyed this testimonial information was not incriminating—it was a foregone conclusion of the government that the documents existed, were in control of the defendant, and were authentic.[73] This put the act within another exception to Fifth Amendment protection, one that the New Jersey Supreme Court has already utilized in conjunction with smartphone passcodes: the foregone conclusion doctrine.[74]

### B. The Foregone Conclusion Doctrine

In *Fisher*, the Supreme Court noted that "[t]he existence and location of the papers are a foregone conclusion, and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers."[75] This is what has come to be known as the foregone conclusion doctrine.[76] Stated plainly, the government was already aware of the content and existence of the documents it compelled the defendant to produce, eliminating the ability for that information to be incriminating.[77] If the government already knows of the existence and location of the information it is seeking from an individual, the information communicated by the act is a "foregone conclusion"—the disclosure by the individual "adds little" to the government's case and is not self-incriminating.[78] The information itself that an act can produce is not barred under the act of production doctrine if that content was derived by the government from an independent source other than what the act would deliver.[79] This was the argument that carried the day for the New Jersey Supreme Court in their estimation of whether the compelled unlocking of a smartphone violated the Fifth Amendment; it was a foregone conclusion that the passcodes in question existed, were possessed by the suspects, and were authentic.[80]

Extending the foregone conclusion doctrine to smartphone passcodes

---

71 *Id.*
72 *Id.*
73 *Id.*
74 State v. Andrews, 234 A.3d 1254, 1274–75 (N.J. 2020); *see also* Ikeda, *supra* note 10.
75 Fisher v. United States, 425 U.S. 391, 411 (1976).
76 United States v. O'Shea, 662 F. Supp. 2d 535, 544 (S.D.W. Va. 2009).
77 *Fisher*, 425 U.S. at 411.
78 *Id.*
79 Thomson, *supra* note 67.
80 State v. Andrews, 234 A.3d 1254, 1274–75 (N.J. 2020).

effectively removes smartphones from the breadth of Fifth Amendment protection simply because of their technological advancement. In all cases, if the Supreme Court were to adopt the construction of the New Jersey Supreme Court, the existence, control, and authenticity of a smartphone passcode is a foregone conclusion for the government; the phone is passcode protected (existence), found within the suspect's possession or owned by them (control), and provides access to the phone upon entry of the passcode ("self-authentication").[81] This embodies the Indiana Supreme Court's worst fears concerning smartphone privacy and only emphasizes the incongruity and lag in legal protection on which Westmore commented.[82] But such a blunt application of the foregone conclusion doctrine fails to take into account what the doctrine is being applied to, namely, the technological miracle that is today's smartphones. Treating technologically advanced personal items like the business documents in the *Fisher* decision would be a blatant oversimplification of this type of item and would ignore recent Supreme Court precedent.[83] To protect the "unique ubiquity" of the smartphone, the extension of a legal doctrine from more than a century ago may provide the answer.[84]

### C. Private Papers

In the *Fisher* opinion, the Supreme Court briefly made mention of "private papers," as the defendant taxpayer argued that because the documents in question were his private papers, they were barred from compelled production under the Fifth Amendment.[85] This argument finds precedent in the 1886 decision by the Supreme Court in *Boyd v. United States*, which held that the compelled production of "private papers" was barred under the Fifth Amendment.[86] The *Boyd* decision clarified that private papers are "goods and chattels" and one's "dearest property."[87] Because of their personal nature, the Court held that "they will hardly bear an inspection," placing them firmly within the Fifth Amendment's protection.[88] This is easier to understand when thinking about private papers within the context of the act of production doctrine—without their compelled production, it is in doubt whether the government would

---

81 *Id.* at 1274–1275.

82 Seo v. State, 148 N.E.3d 952, 958 (Ind. 2020); *see also In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1014–15 (N.D. Cal. 2019).

83 *Seo*, 148 N.E.3d at 959–61 (discussing the *Riley* decision's discussion of smartphones and their profound capabilities).

84 *Id.* at 958–59.

85 Fisher v. United States, 425 U.S. 391, 409 (1976).

86 Boyd v. United States, 116 U.S. 616, 628 (1886).

87 *Id.* at 627–28.

88 *Id.* at 628.

know of the papers' existence, their control, and their authenticity. These three factors would be far from a foregone conclusion for the government.

There is no agreed-upon definition of what comprises "private papers," but the non-exhaustive list includes diaries, journals, and other personal effects.[89] This protection also seemingly extends to personal letters, which in turn lends itself to an added protection for personal communications in the modern context.[90] These documents separate themselves from things such as business records in that their existence depends on the owner's whim; private papers are voluntarily self-created, whereas business records are either required by law or anticipatory given common business practices.[91] If we extrapolate the doctrine of private papers to the Indiana Supreme Court's discussion of smartphones, it is clear that the devices would fall under the doctrine's protection: they contain text messages, photos, emails, location histories, web browsing histories, and so much more of one's own voluntary creation.[92] The Supreme Court's decision in *Fisher* however eliminated protection of private papers under the Fifth Amendment. The opinion in *Fisher* states:

> To the extent, however, that the rule against compelling production of private papers rested on the proposition that seizures of or subpoenas for "mere evidence," including documents, violated the Fourth Amendment and therefore also transgressed the Fifth, the foundations for the rule have been washed away. In consequence, the prohibition against forcing the production of private papers has long been a rule searching for a rationale consistent with the proscriptions of the Fifth Amendment against compelling a person to give "testimony" that incriminates him.[93]

*Fisher* effectively barred protection of private documents under the Fifth Amendment; the Court reasoned that because private papers were voluntarily created, this put them outside of being "compelled" within the Fifth Amendment's meaning.[94] Here, the discussion of being "compelled" seems to be in reference to the creation of the private papers themselves. If one were to write something incriminating in their own diary, for example, that would undoubtedly be a testimonial statement that was also incriminating. But, the act

---

89 James A. McKenna, *The Constitutional Protection of Private Papers: The Role of a Hierarchical Fourth Amendment*, 53 IND. L. J. 55, 55 (1977).

90 Fisher v. United States, 425 U.S. 391, 427 (1976) (Brennan, J., concurring).

91 Lance Cole, *The Fifth Amendment and Compelled Production of Personal Documents after United States v. Hubbell – New Protection for Private Papers*, 29 AM. J. CRIM. L. 123, 126 (2002).

92 *See* Seo v. State, 148 N.E.3d 952, 955–57 (2020).

93 *Fisher*, 425 U.S. at 409.

94 Cole, *supra* note 91.

of confessing incriminating information to one's diary is voluntary—the individual is not being compelled to write the damning evidence into their personal effects. The *Fisher* decision effectively removed the doctrine surrounding private papers for decades and reoriented the focus of the Fifth Amendment's application to compelled production around the foregone conclusion doctrine.[95] The foregone conclusion doctrine, however, could not exclude private papers indefinitely.[96]

In 2000, the Supreme Court decided *United States v. Hubbell*, a case where the government was seeking to compel the production of more than 13,000 of documents from the defendant in question.[97] There, the government guaranteed the defendant "act of production immunity", whereby the government would act as if the sought-after documents were delivered to them anonymously.[98] The government was asking the defendant to produce documents related to eleven broad categories listed in a subpoena, and argued that their existence, control, and authenticity were a foregone conclusion allowing for production.[99] However, the Court held the act of producing numerous documents, even after granted an act of production immunity, holds a great amount of testimonial value and the foregone conclusion doctrine does not apply.[100] The Court stated that the government was unable to ascertain that the records in question existed, that the defendant controlled them, or that they were authentic unless the defendant organized them according to the subpoena in question and produced them.[101] The Court held that the "critical inquiry" for the application of the foregone conclusion doctrine rests on the government's prior knowledge of the documents sought.[102] If the government grants "act of production" immunity to the production of documents it believes are likely to exist, it cannot then say that the contents of those produced documents were a foregone conclusion.[103] This reorients the focus away from private papers' voluntary self-creation and towards the inquiry on the government's knowledge of those documents.[104] It effectively provides an opportunity for private papers to be protected under the Fifth Amendment in the future and gives the doctrine of private papers a chance

---

95 *Id.*

96 United States v. Hubbell, 530 U.S. 27, 45 (2000).

97 *Id.* at 42.

98 Cole, *supra* note 91.

99 *Hubbell*, 530 U.S. at 41.

100 *Id.* at 44–45.

101 *Id.*

102 Cole, *supra* note 91, at 168.

103 *See* United States v. Hubbell, 530 U.S. 27, 45 (2000) ("The Government cannot cure this deficiency through the overbroad argument that a businessman such as respondent will always possess general business and tax records that fall within the broad categories described in this subpoena"); *see also* Cole, *supra* note 91, at 168.

104 Cole, *supra* note 91, at 170.

to expand just as the Supreme Court is looking to be more technologically savvy with their jurisprudence.

## III. A MODERN LEGAL FRAMEWORK FOR SMARTPHONE PROTECTION

### A. The Supreme Court Set Their Own Stage

With the tools of the act of production doctrine, the foregone conclusion doctrine, post-*Hubbell*, and the doctrine of private papers, one can see a way forward for Fifth Amendment protection for smartphone passcodes and thus for smartphones themselves. Judge Westmore's opinion sparked the initial controversy as to the legal differences between alphanumeric, biometric, and facial-recognition passcodes, in terms of the application of the Fifth Amendment.[105] However, the Supreme Court's decision in *Riley v. California* and its commentary on privacy considerations under the Fourth Amendment concerning smartphones may be a stronger sign of the need (and enthusiasm) for a Fifth Amendment legal framework covering the devices.[106]

In *Riley*, two separate petitioners claimed that law enforcement's access of their smartphones without a search warrant – both of which produced incriminating evidence – violated their Fourth Amendment rights.[107] While the Court inevitably ruled for petitioners and held that search warrants are usually required before law enforcement can seize and search through someone's smartphone, they also rejected a number of smaller arguments by the government that attempted to analogize smartphone searches to other simple activities.[108] None was more emphatic than the Court's rejection of the notion that a search of all the data on a cell phone was somehow analogous to searching someone's pockets, relying heavily on the enormity of the data contained within the phone and the uniqueness of the contents.[109] The Court went on to describe the "quantitative and qualitative" differences in smartphones from "physical items."[110] They noted that there is an inherent "pervasiveness" in cell phone data not present in physical records in that they contain an enormous "cache of sensitive personal information."[111] Further, the Court established an important premise: "It is no exaggeration to say that many of the more than 90% of

---

105 *In re* Search of a Residence in Oakland, 354 F.Supp.3d 1010, 1013, 1015–16 (N.D. Cal. 2019).
106 *See* Riley v. California, 573 U.S. 373, 385, 387, 393 (2014).
107 *Id.* at 379–81.
108 *Id.* at 393–95.
109 *Id.* at 393, 395.
110 *Id.* at 393–95.
111 *Id.* at 395.

American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."[112]

While the Court went almost out of their way to establish the special place of smartphones in society today while outlining a Fourth Amendment framework for their protection in *Riley*, they went further in another decision to emphasize the importance of the law keeping up with technology as it continues to evolve at a quicker pace. Chief Justice Roberts, in *Carpenter v. United States*, argued in dicta for increased awareness of the legal world's inability to keep up with the digital world.[113] The consequences of a failure of the legal sphere to evolve as technology evolves could lead to serious confusion, as ambiguity does more harm than good.[114] In terms of the digital privacy context, Chief Justice Roberts forcefully noted that privacy from the government is a necessity of sorts, and a mechanical approach to the Fourth Amendment does not suffice a society of ever-evolving technology.[115] The same should hold true for an archaic Fifth Amendment, and prompt expansion of the doctrines of act of production, foregone conclusion, and private papers into a modern framework of smartphone protection. *Carpenter* further opens the door to establishing a more robust protection for smartphones via the Fifth Amendment, protection that should acknowledge the technological advancement of smartphones and the way in which they order our public and especially our private lives.[116]

### B. Smartphones as Private Papers

The stage is set for the Supreme Court to firmly denote smartphones as an amalgamation of private papers. In the sense that private papers are comprised of diaries, personal letters, and the most intimate thoughts of the individual creating them,[117] smartphones are perhaps the ultimate form that private papers can take since their legal inception. The *Hubbell* decision allows for the reintroduction and build-out of the private papers framework in that it shifts focus back to the government's prior knowledge of documents' existence, control, and authenticity under the foregone conclusion doctrine and away from the "voluntary self-creation" rationale offered by *Fisher*.[118]

---

112 *Id.*

113 Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).

114 Heidi Kuffel et al., *"Face ID is Unavailable. Try Again Later"— Can Law Enforcement Force a Suspect to Unlock Their Phone by Face ID or Fingerprint?*, A.B.A. (Feb. 13, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/cyberspace/2019/201902/fa_1/.

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

116 *Id.* at 2220.

117 McKenna, *supra* note 89.

118 Cole, *supra* note 91, at 168–69.

One criticism of the *Boyd* rationale for private papers is its "conflation of the Fourth and Fifth Amendments."[119] The *Hubbell* case itself was a dispute about responding to a subpoena and the production of documents via that method of legal compulsion; it was not a decision about search warrants, and legal scholars have cautioned against denoting a subpoena's compelled production as the "equivalent of a search and seizure."[120] In the context of smartphones however, Judge Westmore and the Indiana Supreme Court have already done the job of taking positions that more closely resemble such a conflation, while keeping in place the foregone conclusion doctrine.[121] Smartphone storage capacities are far more vast than the over 13,000 pages sought in the *Hubbell* case;[122] our stored personal communications with family members, friends, and employers alone are enough private documents to eclipse that number, which pales in comparison after adding in thousands of photos, location-tracking information, and web browser history to the total document count

The Supreme Court has already indicated a shift toward construing the doctrine of private papers broadly to include smartphones. In *Riley*, the Court noted that "one of the most notable distinguishing features of modern cell phones is their immense storage capacity."[123] The Court even describes the "pervasiveness" of such a search throughout the opinion and details the way in which all the information available to one who has access to the phone could be used to "reconstruct" someone's personal life.[124] All of this discussion of the private nature of the smartphone, the immensity of the data it can contain, and the ways in which smartphones have transformed the way in which we live out and protect our personal lives is the framework for labeling smartphones as private papers. The Supreme Court has subtly already done the job of outlining a possible definition; now it must expressly embrace that definition.[125]

### C. Smartphone Passcodes, the Act of Production Doctrine, and the Foregone Conclusion Doctrine

In that same context, the act of production doctrine can and should be extended to smartphone passcodes, thereby entitling such an unlocking to the

---

119 *Id.* at 169.
120 *Id.* at 170.
121 *See In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1017 (N.D. Cal. 2019); *see also* Seo v. State, 148 N.E.3d 952, 958 (Ind. 2020).
122 United States v. Hubbell, 530 U.S. 27, 42 (2000).
123 Riley v. California, 573 U.S. 373, 393 (2014).
124 *Id.* at 394–95.
125 *Id.* at 394 (explaining how cell phones can store "millions of pages of text, thousands of pictures, or hundreds of videos," which creates "interrelated privacy consequences").

protections the Fifth Amendment. While the differences between biometric or facial-recognition passcodes and alphanumeric passwords sparked the initial legal debate as to whether the smartphone's production violated the Fifth Amendment, an adoption of the *Seo* and Westmore position, coupled with a focus on what the smartphone contains as opposed to how it's protected, is the most workable legal framework. The Indiana Supreme Court noted firmly that the "act of producing an unlocked smartphone communicates a breadth of factual information."[126] This eliminates the distinctions between using one's biological features and a written password to unlock the device, a conclusion that logically follows from the main premise of the act of production doctrine: such an act demonstrates existence, control, and authenticity of the information in question.[127] Westmore also advocates for an understanding of the smartphone not from the manner of its protection, but from its potential to contain self-incriminating information.[128]

It necessarily follows that the foregone conclusion doctrine becomes a harder bar for the government to surpass in reference to smartphones. In terms of specific documents, especially in the contexts of banking, taxes, and business records, the government was able to outline an effective argument that they knew such records existed and what they necessarily contained, either because the individual in question was legally required to keep them or they were a common business practice.[129] With private papers however, especially in reference to smartphones, it is impossible to know if such papers even exist, let alone the subject matter of what they contain.[130] The Supreme Court outlined in *Riley* the storage capacity of the smartphone, which further demonstrates the government's inability to anticipate all that could be contained on the device.[131] This, in turn, puts smartphones relatively beyond the reach of the government, unless they can ascertain that they know specific information on the phone from independent sources, such as cellular providers or other tech service providers.[132] Again, the act of production doctrine protects the unlocking of the phone itself under the Fifth Amendment as an incriminating act—it is not that the information on the phone itself is necessarily barred as self-incriminating,

---

126 *Seo*, 148 N.E.3d at 955.

127 Thomson, *supra* note 67 (explaining that the "witness' act of producing" documents could "communicate information that the government" does not have, "such as the existence, possession, and authenticity" of subpoenaed documents).

128 *In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1016 (N.D. Cal. 2019).

129 *See* Fisher v. United States, 425 U.S. 391, 410 (1976) (explaining that the documents in question had to exist, were controlled by the taxpayer, and were their authentic versions) (citing *Curcio v. United States*, 354 U.S. 118, 125 (1957)).

130 Kraus, *supra* note 15.

131 Riley v. California, 573 U.S. 373, 393–94 (2014).

132 Kraus, *supra* note 15.

but that the unlocking proves existence, control, and authenticity of the phone and its contents.[133] How would the Supreme Court go about creating such a protection scheme, one that would allow greater security for the smartphone without completely compromising law enforcement's ability to search the device?

### D. A Proposal for a Fifth Amendment Protection Scheme for Smartphones

Let's entertain a hypothetical. Suppose the search warrant application that Judge Westmore denied is litigated all the way to the Supreme Court, which grants certiorari. Let's recall that the search warrant application law enforcement was seeking from Westmore was in regard to two individuals suspected of extortion. They argue that given past precedent, not only is the search warrant application not overbroad for Fourth Amendment purposes, but also compelling an individual to unlock a smartphone using biometric features is not testimonial for purposes of the Fifth Amendment. In essence, they argue that someone's face or thumbprint is something they are, something that doesn't convey any information in regard to the smartphone.[134] The purported suspects argue along the lines of Westmore's written opinion, stating that not only was the search warrant in question unreasonably overbroad, but that compelling an individual to use their thumbprint or face to unlock a smartphone is testimonial because it demonstrates that they own the device.[135]

With a circuit split among the states and the dispute in need of resolution, the Court would likely first have to define smartphones using the *Boyd* definition of private papers. The Court would analogize smartphones to the "goods and chattels" and one's "dearest property" that *Boyd* described.[136] The Court would note that people confess their private thoughts to smartphones multiple times a day in text messages, emails, the photos they take, and the Google searches they make. Further, the Court would cite to previous precedent in the *Riley* decision, recalling as written above that smartphones hold a special place in how individuals order their lives, and that searching through them without proper cause is "pervasive."[137]

With smartphones designated as private papers, the Court would further

---

133 Seo v. State, 148 N.E.3d 952, 957 (Ind. 2020).

134 Kraus, *supra* note 15.

135 *In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1014–16 (N.D. Cal. 2019).

136 *Id.* at 1016.

137 Riley v. California, 573 U.S. 373, 385–90 (2014).

outline that the act of production doctrine applies to smartphone passcodes, and that using one's face or thumbprint (or even an alphanumeric pattern in this new context) demonstrates that the phone, and the information contained therein, is the authentic version in question.[138] Law enforcement would assert that because the individuals they arrested were under suspicion of extortion, the foregone conclusion doctrine applies, and the phone containing incriminating information is practically a known assertion. The Court would establish, however, that such an inference is on rather shaky foundation: there is no possible way that law enforcement would know that any information regarding extortion definitely exists on the phone, as the creation of private papers is at the whim of the creator.[139] Citing again to *Riley* as precedent, albeit in the Fourth Amendment context, given the storage capacity of the smartphone, it is impossible to know what could be contained on the device; therefore, there's no way law enforcement could know for certain that information pointing to extortion would be contained on the device.[140] If law enforcement argued that extending the Fifth Amendment to smartphones is unnecessary given their current protection under the Fourth Amendment, the Court could point to its decision in *Carpenter*, further clarifying that technology's advancement necessitates the legal sphere's continued evolution on the same front.[141] Punishing smartphones and their users by limiting their privacy rights in devices not possibly contemplated by the framers of the Constitution at the time the Fifth Amendment is unsound policy. New developments in the data privacy sector would potentially be subject to a regress in legal protection due to progress technologically.

One question that must be addressed is what law enforcement is left with after a Supreme Court decision moves smartphone passcodes within the protection of the Fifth Amendment, regardless of whether they are biometric, facial-recognition, or alphanumeric in nature. One must recall that in terms of the Act of Production doctrine, which smartphone passcodes would now be subject to, the Fifth Amendment does not protect the information on the smartphone itself as privileged; it instead denotes that the act of unlocking the smartphone using a passcode is itself incriminating, protecting the information on the device by proxy.[142] Law enforcement, as in the extortion situation the warrant on which Judge Westmore ruled, would then be unable to have smartphone owners unlock their devices during a criminal investigation. Does this effectively cut smartphones off from the purview of law enforcement? Is there any way to overcome the protection of the Fifth Amendment in the smartphone context?

---

138 Thomson, *supra* note 67.
139 Kraus, *supra* note 15.
140 *Riley*, 573 U.S. at 393.
141 Kuffel, *supra* note 114.
142 Thomson, *supra* note 67, at 4.

Recall that the information contained on the smartphone is not privileged—the passcode is the protected information under the Fifth Amendment.[143] Therefore, if an individual asserts their Fifth Amendment protection against self-incrimination and refuses to unlock their smartphone, this does not bar the police from seizing and searching the phone pursuant to a valid warrant or "specially established and well-delineated exceptions."[144] Thus, in theory, if police legally take the phone and are able to decipher the information on it without extracting the passcode from its owner, the Fifth Amendment has nothing to say. Many may recall the debacle over the iPhone device the FBI recovered in the wake of the San Bernardino attack in 2015 – a smartphone belonging to the terrorists that was also encrypted.[145] While there was no Fifth Amendment protection to assert in this situation, it demonstrates that law enforcement on both the state and federal level have other methods of extracting information from a smartphone device other than obtaining the passcode from the owner.[146] Police may seek the manufacturers help in unlocking the devices (although such a plea was denied by Apple in the circumstance above), the intervention of private cyber security firms and their hacking software, or their own tech experts.[147]

Law enforcement may also seek to obtain the information sought on the device from other databases, such as asking cloud-computing companies for access to information a user may have placed on their smartphone's hard storage or in the cloud.[148] While a warrant would likely be required in most instances (see the Court's holding in *Riley*), this would circumvent the need for a passcode to gain access to the information in question.[149] This issue would also avoid the prospect that accessing such information via the smartphone would require not only the unlocking of the device, but also other layers of passcodes and account information for cloud-stored data.

---

143 *Id*.

144 Coolidge v. New Hampshire, 403 U.S. 443, 454–55 (1971) (quoting Katz v. United States, 389 U.S. 347, 357 (1967)); G.M. Leasing Corp. v. United States, 429 U.S. 338, 353 (1977).

145 Ellen Nakashima et al., *The FBI Wanted to Unlock the San Bernardino Shooter's iPhone. It Turned to a Little-Known Australian Firm*, WASH. POST (Apr. 14, 2021), https://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/.

146 *Id*.

147 *Id*.

148 Christopher Slobogin, *Policing and the Cloud*, NAT'L CONST. CTR., (May 15, 2017), https://constitutioncenter.org/digital-privacy/policing-and-the-cloud.

149 *See* Riley v. California, 573 U.S. 373, 403 (2014).

### E. Drawbacks for Different Stakeholders: New Realities for Law Enforcement and "Big Tech"

For most of this article, I have focused almost exclusively on one set of stakeholders in the context of protecting smartphone passcodes with a Fifth Amendment framework: smartphone owners and users. As mentioned briefly in the previous section, there are several other important stakeholders that must be discussed to paint a more accurate picture of what a Fifth Amendment framework of protection for smartphone passcodes would look like in a practical application. While such a protection scheme would be a welcome boon to smartphone users and owners, it would have different, if not difficult, consequences for law enforcement and smartphone developers.

It's not hard to imagine that law enforcement would characterize a Fifth Amendment protection scheme as overly onerous on their investigative work, but in circumstances such as those outlined above, it may in fact promote more efficiency in their work while ensuring they respect proper rules of criminal procedure, constitutional rights, and the privacy considerations of those they investigate.[150] For example, the decision in *Riley* notes that heightened protection for smartphones and their contents "comes at a cost" but also is quick to reiterate that the warrant requirement for conducting searches is an important part of the investigative process, not just a consideration or obstacle to law enforcement's work.[151] Nonetheless, law enforcement would undoubtedly prefer the status quo remain unchanged: the current flux across jurisdictions creates more room for police to operate within, and the argument that submitting biometric information to unlock a device is akin to the submission of DNA or participation in a lineup is still a potent one in many states.[152] If this Fifth Amendment protection framework that I have outlined is realized by the Supreme Court, distinctions between alphanumeric and biometric passcodes could disappear altogether, requiring police in every instance to pursue other avenues of unlocking the devices using warrants.[153]

If law enforcement seeks to have a user unlock their smartphone in the absence of a warrant or probable cause, the only remaining legal justification for arguing that the police did not run afoul of either the Fourth or Fifth Amendments is the doctrine of consent.[154] While consenting to a search by law enforcement does away with the necessary prerequisites of police either obtaining a warrant or articulating probable cause, the consent itself must be

---

150 Nakashima, *supra* note 145.
151 *Riley*, 573 U.S. 373 at 401.
152 Morrison, *supra* note 7.
153 Seo v. State, 148 N.E.3d 952, 955 (Ind. 2020); Thomson, *supra* note 67.
154 Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

"voluntarily given" and not "coerced."[155] The Court has refused to equate the voluntariness requirement of consent doctrine to "proof of knowledge of the right to refuse consent" by the individual in question.[156] In the context of smartphones and the Fifth Amendment, if Fifth Amendment protection was extended to smartphones on the basis of their characterization as private papers, an owner or user would still be able to relinquish their right to be protected from self-incrimination by consenting to law enforcement's request that they unlock their smartphones, whether biometrically or through surrendering the alphanumeric code. However, given the discrepancies in how smartphone passcodes are treated across different jurisdictions, it may be important to reconsider the definition of voluntariness in the consent context when smartphones are the subject of law enforcement's search. Justice Marshall's dissent in *Schneckloth v. Bustamonte* mentions that the Fifth Amendment right to be free from being "compelled in any criminal case to be a witness against himself" deals directly with the issue of compulsion by law enforcement.[157] Justice Marshall relates consent and coercion together, believing that the majority in the case gave police a workaround to both Fourth and Fifth Amendment protections against warrantless searches and freedom from coercion respectively:

> No interests that the Court today recognizes would be damaged in such a search. Thus, all the police must do is conduct what will inevitably be a charade of asking for consent. If they display any firmness at all, a verbal expression of assent will undoubtedly be forthcoming. I cannot believe that the protections of the Constitution mean so little.[158]

Justice Marshall is thus of the opinion that voluntariness on the part of an individual looking to give consent to law enforcement to search necessitates that the individual must be aware of their right to refuse consent.[159] While the doctrine of consent is a Fourth Amendment issue in accord with warrantless searches and seizures, it helps to inform how smartphones may (or should) be treated in the Fifth Amendment context and its protections from self-incrimination. Because of the variety in legal interpretations across jurisdictions in terms of smartphone protection under the Fifth Amendment, a requirement that law enforcement have proof of knowledge that an owner or user of a device had a right to refuse to unlock their device would ensure that the constitutional

---

155 *Id.* at 233.
156 *Id.* at 232–33.
157 *Id.* at 280–81 (Marshall, J., dissenting).
158 *Id.* at 284.
159 *Id.* at 282.

right to be free from the coercion of law enforcement is protected.[160] Law enforcement benefits from the lack of clarity surrounding whether an individual can refuse to unlock their smartphone if it is requested of them; if Fifth Amendment protection is extended to smartphone passcodes, police will likely still benefit from the fact that individuals are not always aware of their rights under the Constitution.[161] Justice Douglas finds this reality troubling, and revisiting his dissent in *Schneckloth* may further ensure law enforcement cannot easily work around this new Fifth Amendment protection.[162]

As mentioned above, another important stakeholder to consider when advocating for Fifth Amendment protection of smartphone passcodes are those companies that create the devices and maintain their software.[163] It is fair to assume that their interests in such a new framework of legal protection would closely mirror those of device users and owners. The public would be more distrusting of smartphone companies who openly professed more willingness to accede to the interests of the government in intruding on the privacy of these devices than to protecting the privacy interests of their consumers. Such a stance would deter the public from purchasing smartphones after all and was likely a motivating factor behind Apple's unwillingness to create a "backdoor" into smartphones that would allow law enforcement to access the devices without the need for the owner's passcodes.[164] I discussed earlier in this article the paradox of advancements in technology leading to less constitutional protection or digital privacy. If smartphones are treated as private papers and their passcodes, whether biometric or alphanumeric, are held as testimonial in the context of disclosure to law enforcement, technology companies are assured that their innovations will not account for less legal protection for their consumers.

One drawback for these companies could be the prospect of legislation after such a Supreme Court decision that would attempt to curb the newfound privacies enjoyed by smartphone users in favor of balancing the government's interest in accessing these devices. Federal and state legislation may seek to force companies like Apple to include backdoor access and in-runs to passcode protection like that which the FBI sought Apple to create for the San Bernardino shooter's smartphone.[165] Faced with the prospect that only a sufficiently specific warrant or consent to unlock could allow law enforcement to access smartphones, the federal and state governments may seek to impose new requirements on tech companies that allow police to bypass the need to go

---

160 *Id.* at 282–83.
161 *Id.* at 283–84.
162 *Id.* at 288–90.
163 Nakashima, *supra* note 145.
164 *Id.*
165 *Id.*

through the smartphone owner to gain access to the device.[166] This would eliminate the need for law enforcement to use their own cyber hackers or hire third-party security firms, as they instead could produce a warrant that would allow them to access smartphones from the built-in backdoor the device's developer was required to implement. Still, the government's appetite to force "big tech" to deliberately compromise the privacy of the devices they produce if law enforcement deems it necessary is difficult to gauge; disrupting the already ominous reputation of companies like Meta, Apple, and Samsung by requiring them to weaken the digital privacy of their consumers may be a political death sentence.[167] Other than this consideration, the developers of these devices likely share many of the same interests in heightened smartphone passcode protection under the Fifth Amendment that their consumers do, albeit in an effort to boost the popularity and sale of their devices.

## IV. CONCLUSION

Smartphones are in desperate need of Fifth Amendment protection in a digital age where our most sensitive and private information is constantly on our person and right at our fingertips. The *Riley* decision has already done the work in the Fourth Amendment context[168], while *Carpenter* warns that the government is getting craftier in the way in which it is able to invade privacy given technology's evolution.[169] An extension of the doctrine of private papers gives the smartphone a blanket of protection seen only for the most personal of documents more than a century ago. With the devices locked away from law enforcement's purview absent the most specific search warrants and showings of prior knowledge, the Supreme Court will be able to ensure the safety and protection of the country's most unique and perhaps most powerful personal item. Such a scheme would have lasting impact on technological privacy beyond the smartphone device even; consider the way in which technology plays a role in both our professional and personal lives on a daily basis. Laptops, smart watches, smart TVs, video game consoles, even GPS tracking systems in cars all contain information that many take a presumed interest in keeping private. With smartphones protected under the Fifth Amendment, the extrapolation to include all devices capable of hoarding thousands of bytes of information under this privacy right is not an unthinkable proposition, and some courts have

---

166 Morrison, *supra* note 7.

167 *See generally* Alison Beard, *Can Big Tech Be Disrupted?*, HARVARD BUS. REV. (Jan. 2022), https://hbr.org/2022/01/can-big-tech-be-disrupted.

168 Riley v. California, 573 U.S. 373, 393–97 (2014).

169 Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).

already had to consider such a circumstance.[170] As we allocate more and more of our personal information to digital devices and the cloud, the legal schemes that protected our privacy interests in the past in more rudimentary circumstances must evolve as technology does. Smartphones should just be the beginning of such an evolution and extension.

If Chief Justice Roberts is serious about the need for the legal world to catch up to technology, then the Supreme Court should be on the lookout for cases such as Westmore's order and both New Jersey and Indiana's differing opinions on the application of the Fifth Amendment to smartphones and their passcodes.[171] By using previous precedent regarding private papers, the Supreme Court can create a new protection scheme for these devices by extending the Fifth Amendment's protection against self-incrimination while maintaining a commitment to stare decisis. The revitalization of the private papers doctrine to include smartphones as private papers is a logical outgrowth of both *Boyd* and *Hubbell* as well as an affirmation of the Court's commitment to evolving the law at a pace equal to that of technology's evolution.

It is plain to see that the law is behind technology and has been for quite some time; refusing to hear cases that can provide an opportunity to rectify this situation and the disagreement among different states' courts on tech questions such as smartphone passcodes demonstrates a lack of commitment to such an evolution. Life-changing technology, technology that has allowed for society to change the way in which its members interact with each other and protect their privacy, necessitates a rule of law that is cognizant of such wholesale changes to ways of life. Ensuring that smartphones and their passcodes are afforded the same protections as their prior art were entitled to helps society to order itself accordingly. Citizens' substantive rights in their own privacy in the context of their smartphones should not change as one crosses state lines. For a technology that is so pervasive and prevalent in our society today, the law should ensure that it is equally protected in all corners of the nation, ensuring one's cognizance as to what rights they do and do not have in their devices regardless of what jurisdiction in which they find themselves interacting with the police.

Protecting smartphone passcodes under the Fifth Amendment act of production doctrine, foregone conclusion doctrine, and private papers doctrine is a scheme that ensures the public maintains privacy and a right to protection against self-incrimination in a world where business documents are sent by e-

---

170 Nowell D. Bamberger et al., *Court Holds That 5th Amendment Self-Incrimination Privilege Precludes Compelling Fingerprint or Facial Recognition Access to Digital Devices*, CLEARY ENFORCEMENT WATCH (Jan. 23, 2019), https://www.clearyenforcementwatch.com/2019/01/court-holds-5th-amendment-self-incrimination-privilege-precludes-compelling-fingerprint-facial-recognition-access-digital-devices/ (last visited Nov. 7, 2022).

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

mail instead of telegram and diaries are kept on web applications instead of leather-bound notebooks. It is only right that the law continues to evolve as the technology it protects does.