CONFLICTING COMMON LAW: APPLICATION OF THE SELF-INCRIMINATION CLAUSE AS APPLIED TO SMARTPHONE TECHNOLOGY

Andrew Meena[*]

The Self-Incrimination Clause of the Fifth Amendment of the United States Constitution protects individuals from being compelled to submit evidence or provide testimony against themselves in relation to the crimes for which they are charged. The text of the clause reads "[no person] shall be compelled in any criminal case to be a witness against himself."[1] In the modern era, the judicial application of this clause had once been relatively clear, with judges taking an originalist approach. For instance, in *Hoffman v. United States,* the Supreme Court held that a witness may "refuse to answer questions as to whether he had seen, talked to, or knew the whereabouts of a certain person" following the issuing of a subpoena "on the ground that his answers might incriminate him of a federal offense."[2] In *Griffin v. California,* the Supreme Court struck down a California state rule of evidence that allowed a jury to consider it tantamount to a showing of guilt if a defendant did not testify in criminal proceedings.[3] In a third case, *Fisher v. United States,* the Supreme Court held that the Self-Incrimination Clause protects individuals from "compelled self-incrimination," such as testimony, but does not extend to privately disclosed information, such as privately disclosed tax-related documents that hold pertinent information.[4] While each of these examples supply a clear application of the Self-Incrimination Clause, applying the Fifth

[*]Andrew Meena is an expected 2024 J.D. candidate at The University of Akron School of Law and a Fellow for The Center for Constitutional Law at Akron. Professionally, Mr. Meena is an educator in the Cleveland Metropolitan School District, teaching both World and American History at the secondary education level. The author extends a profound thanks and appreciation to Michael Gentithes, Associate Dean of Academic Affairs, for his counsel and support as well as Tracy Thomas, Director, The Center for Constitutional Law, for her encouragement and editing support.

1. NATIONAL ARCHIVES, *The Constitution: Amendments 11–27,* https://www.archives.gov/founding-docs/amendments-11-27 (last visited June 25, 2022).

2. 341 U.S. 479, 481 (1951).

3. 380 U.S. 609 (1965).

4. 425 U.S. 391, 401 (1976).

Amendment has become murkier and substantially more difficult as technology has advanced to include password-protected files, passcode-protected devices, and biometric decryption technologies like facial ID, thumbprints, and more.

Part of this murkiness has come from the Supreme Court's denial of two recent and relevant writs of certiorari that would have provided greater clarity toward the application of the Self-Incrimination Clause as it relates to modern technology.[5] The first, *Commonwealth v. Jones,* would have asked the Court to address how the foregone conclusion rule, the rule that testimony is compelled and considered an act of surrender when it "adds little or nothing to the sum total of" information gathered by government officials,[6] should be applied when a defendant is compelled to unlock a password-encrypted device.[7] The Supreme Judicial Court of Massachusetts held that mere knowledge of a password is not itself incriminating.[8] The second case, *State v. Andrews,* addressed whether mere knowledge of a passcode is relevant when government officials are seeking access to files and information that are passcode protected, and to what evidentiary extent passcodes themselves have on the criminal proceedings.[9] Both of these cases cited the holding in *Fisher* as precedent when discussing self-incrimination to posit a modern understanding, a case that was decided nearly fifty years prior.

Legitimate or not, the perceived hesitancy by the Supreme Court has led state and lower federal courts to apply the Self-Incrimination Clause to these types of technological issues with conflicting results. In the same year that *Commonwealth v. Jones* was decided, another case, *Seo v. State,* saw the Supreme Court of Indiana hold that in addition to mere knowledge of a password, the government must also show evidence that the input of the password will unlock specific evidence: the government must know what significant evidence exists on the device in order to compel a defendant to input the password.[10] Thus, there are competing applications across two different states. In one case, *Commonwealth v. Jones,* the defendant was required to submit a password because knowledge of that

5. *ACLU, EFF Urge Supreme Court to Protect Against Forced Disclosure of Phone Passwords to Law Enforcement* AMERICAN CIVIL LIBERTIES UNION (Jan. 8, 2021), https://www.aclu.org/press-releases/aclu-eff-urge-supreme-court-protect-against-forced-disclosure-phone-passwords-law.

6. 425 U.S. at 411.

7. 117 N.E.3d 702 (Mass. 2019).

8. *Id.*

9. 234 A.3d 1254 (N.J. 2020). The case is discussed further *infra*.

10. 148 N.E.3d 952 (2020).

password was not self-incriminating;[11] in another, *Seo v. State,* there had to be more than mere knowledge of the password.[12] One case required preliminary knowledge, another required authorities to know with certainty the information sought existed on the device.

This type of judicial confusion and apparent hesitancy by the Supreme Court is certainly not without logic considering the perceived pace at which technology is advancing and will continue to do so.[13] The prospects of updating a common law approach to the application of the Self-Incrimination Clause on ever-changing technology would appear to be a constantly moving target. While in recent years the Court has provided more clarity on the application of the Fourth Amendment Search and Seizure Clause,[14] the Self-Incrimination Clause has yet to receive the same treatment.

This essay will discuss the pros and cons of a judicial solution to these conflicting results against a legislative solution. Rather than through regulation or statutory reform, the focus will be on the need for a contemporary judicial interpretation of the Self-Incrimination Clause in furtherance of the common law tradition that spawned the first understandings of the Fifth Amendment. Ultimately, this examination will call upon the Supreme Court to craft a modern application of the Self-Incrimination Clause by holding that (1) the foregone conclusion rule should not apply merely to unlocking a person's smartphone, and (2) that the particularity requirement of search warrants should include with specificity which applications and what information law enforcement is seeking.

I. HISTORICAL BACKGROUND

For much of the history of the Fifth Amendment Self-Incrimination Clause, the Supreme Court, state courts, and lower federal courts have

11. 117 N.E.3d at 706.

12. 148 N.E.3d 952 (2020).

13. Sam Baker & Ashley Gold, *Big Tech's Future is Up to a Supreme Court That Doesn't Understand It,* AXIOS, https://www.axios.com/2023/02/20/supreme-court-section-230-google-twitter-tech (last visited Mar. 12, 2023); UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, *The Impact of Rapid Technological Change on Sustainable Development,* https://unctad.org/publication/impact-rapid-technological-change-sustainable-development (last visited Mar. 12, 2023) ("[R]apid technological change poses new challenges for policymaking. It can outpace the capacity of Governments and society to adapt to the changes that new technologies bring about.").

14. *Catch Me If You Scan: Constitutionality of Compelled Decryption Divides the Courts* CONGRESSIONAL RESEARCH SERVICE, (Mar. 6, 2020), https://crsreports.congress.gov/product/pdf/LSB/LSB10416.

applied an originalist understanding that begins with the seminal case *United States v. Burr*.[15] This was the first case in post-colonial America that established the right against self-incrimination, and has been subsequently applied to any communications that are testimonial, incriminating, and to those which are compelled.[16] For the right against self-incrimination to apply, that which the government is compelling must be considered "testimonial" in nature, meaning that the information must come from the contents of the defendant's own mind in order to be communicated.[17] For example, requiring a criminal defendant to disclose the combination of a lock is considered by the courts of various jurisdictions to be "testimony" and the "contents of one's own mind," which is thus protected by the Fifth Amendment. On the other hand, being forced to surrender a key to a locked desk is not testimonial in nature and does not receive the same protection.[18]

This right can also sometimes be applied to the production of physical documents when compelled by a subpoena, as the act itself may likewise be testimonial in nature.[19] Additionally, the privilege against self-incrimination includes such testimony that is considered to be "a link in the chain of evidence needed to prosecute" for a crime.[20] An important exception to this fundamental right is the "foregone conclusion" rule: if the government can show that it is already aware the suspect possesses the relevant documents or information at issue, then the act of production is no longer protected as "testimony" but is rather considered to be an act of "surrender" and receives no Fifth Amendment protection.[21] For the foregone conclusion rule to apply, the relevant information cannot provide any new links in the chain of evidence against a defendant or a witness, and government officials "must establish that it *already knows the testimony* that is implicit in the act of production."[22]

A. Legal History of the Self-Incrimination Clause

The history of the Self-Incrimination Clause does not begin with the enumeration of the Fifth Amendment but rather with a continuation of the

15. Nicole Hager, *SCOTUS Asked If 5th Amendment Bars Compelling Defendants to Unlock Electronic Devices,* FEDSOC BLOG (June 2, 2022), https://fedsoc.org/commentary/fedsoc-blog/scotus-asked-if-5th-amendment-bars-compelling-defendants-to-unlock-electronic-devices.

16. *Catch Me if You Scan, supra* note 14.

17. *Id.*

18. *Id. See U.S. v. Hubbell*, 530 U.S. 27, 41 (2000).

19. *Id.*

20. *Hoffman*, 341 U.S. at 486.

21. *Id.*

22. *Commonwealth,* 117 N.E.3d at 710.

English Common Law upon early American jurisprudence. The clause itself was understood at the time to be a mere extension, perhaps even a recitation, of a common law understanding dating back as far as the 17th century and in written form as far back as the 18th century.[23] As a result, preeminent legal scholars of early America held the privilege against self-incrimination as merely "the English Common Law brought to a new shore," a standard that was nationally and juridically held at the time to be authoritative.[24] The privilege against self-incrimination, according to this legal standard, states that "[A] witness shall not be asked any question, the answering to which might oblige him to accuse himself of a crime."[25] This understanding of the privilege against self-incrimination would be applied in the first American case to invoke the right in 1807: *United States v. Burr.*

Following his term as Vice President of the United States, Burr had fallen out of favor with his own party, the Democratic-Republicans, for running against the standard bearer, Thomas Jefferson, in the 1800 presidential election.[26] After his term ended, Burr sought better fortunes in the untamed West through military conquests in the Louisiana and Mexico territories (modern-day Texas).[27] Left unclear to the Jefferson administration, however, were Burr's intentions once he had acquired this new land west of the Mississippi River.[28] Accordingly, President Jefferson had Burr arrested and charged with treason and with violating the Neutrality Act of 1794.[29] Part of the evidence brought against Burr was a letter he had sent to one of his supposed co-conspirators, known as the "Wilbourn Letter."[30] The contents of this letter were encrypted by the use of a cipher, a commonly used tool during that era for concealing the

23. Orin S. Kerr, *Decryption Originalism: The Lessons of Burr*, 134 HARV. L. REV. 905, 925 (2021). *See* WILLIAM HAWKINS, A TREATISE OF THE PLEAS OF THE CROWN 609 (6th ed. 1788).

24. Kerr, *supra* note 23, at 925.

25. *Id.* at 926. *Cf* LEONARD MACNALLY, THE RULES OF EVIDENCE ON PLEAS OF THE CROWN (1802).

26. Scott Bomboy, *Aaron Burr's Trial and the Constitution's Treason Clause*, CONSTITUTION DAILY (Sept. 1, 2021), https://constitutioncenter.org/blog/the-great-trial-that-tested-the-constitutions-treason-clause. In addition to becoming a political enemy of Thomas Jefferson and the Democratic-Republicans, Burr had also made himself an enemy of the Federalists after fatally wounding Alexander Hamilton in their famous duel in 1804. Short of options on the east coast, Burr recruited a small army and led them into the American frontier. However, this newly formed band of fortune-seekers caused Jefferson to believe that Burr was planning to start a war against the United States as part of an effort to create a new, separatist state.

27. *Id.*

28. Kerr, *supra* note 23, at 915.

29. *Id.*

30. *Id.* at 918.

contents of important correspondence due to the insecurity of early 19th century postal services.[31]

While it was asserted that Burr indeed wrote the letter, the prosecution also charged that the letter had been copied prior to being sent by Burr's secretary, Charles Willie.[32] Mr. Willie was brought before the court and asked whether he copied the letter and if he understood the contents therein.[33] Burr's counsel then argued that it was improper for the prosecution to ask Willie if he understood the letter, for if the letter contained anything treasonous, it would show that Willie knowingly concealed treasonous acts,[34] making Willie himself guilty of treason.[35] Thus, the question before the court was whether it would be self-incriminating for Charles Willie to answer this question, and if so, whether he would be granted the privilege enumerated in the Fifth Amendment.

Ultimately, Willie was made to answer the question, though he was exonerated for his part in the supposed plot with former Vice President Burr. As part of Chief Justice Marshall's reasoning for exonerating Burr, it was noted that Willie was asked only "whether he currently understood the contents of the letter; his "*present* knowledge of the cipher would not prove his *past* knowledge of it," leaving Willie free from incrimination as a result.[36] Applying it to modern usage, Chief Justice Marshall's reasoning shows that a suspect can be compelled to testify where the government is merely asking whether the person *knows* the current password, or in the case of Charles Willie, a cipher.[37] Mere knowledge of the password (or cipher) is not itself incriminating and is thus not a protected privilege under the Fifth Amendment.

While Charles Willie was made to testify, and an arguably legally nuanced application of the Self-Incrimination Clause was applied, the application followed a tradition set forth in the English common law. Thus, there is a clear precedential timeline of the privilege against self-incrimination starting from the 17th and extending into the 19th century.

---

31. *Id.* at 917.
32. *Id.* at 921.
33. *Id.* at 923.
34. *Id.* at 923-24.
35. Treason and Sedition Acts of 1795, 18 U.S.C. § 2382 (West). "Whoever, owing allegiance to the United States and *having knowledge* of the commission of any treason against them, conceals and does not, as soon as may be, disclose and make known the same . . . is guilty of misprision of treason. . . ." (emphasis added)
36. Kerr, *supra* note 23, at 944 (emphasis added).
37. *Id.* at 952.

B. Self-Incrimination in the Modern Era

As discussed, the Supreme Court has yet to consider the application of the Self-Incrimination Clause on modern technology, specifically whether it is a form of self-incrimination for one to be compelled to input their password. This has left state and lower federal courts to determine independently how self-incrimination should be applied to current technology.[38] An example of this is the case, *State v. Andrews*.

In that case, a former county sheriff's officer was charged with aiding the target of a state narcotics investigation.[39] The state acquired a search warrant for the officer's two iPhones, both of which were password protected.[40] The state then moved to compel the officer to unlock the two phones.[41] The court ruled that this was not "incriminating" because the passwords "were not an element of any crime with which the defendant was charged,"[42] and thus were not testimonial in nature. Without specifically invoking the forgone conclusion rule but heavily implying its application, the court also stated that since the prosecution had already established the phones belonged to the officer, the passwords held very little "evidentiary significance" that bore any weight on whether a crime had been committed.[43]

On the surface, the ruling in this case may appear to be analogous to Chief Justice Marshall's rationale in *Burr,* that present knowledge of a password is not itself incriminating. The difference in *Andrews* is the invocation, or the perception, of the "foregone conclusion" rule. Here, the State was able to show that "the cellphones' contents are passcode-protected," that "the cellphones were in Andrews's possession . . . and that he owned and operated the cellphones, establishing [present] knowledge of the passcodes."[44] Thus, the foregone conclusion rule applied even though it was not expressly invoked.

The circuit court's holding in *Andrews* references two additional cases that create a conflicting framework when applying the Self-Incrimination Clause to modern technology: *Fisher v. United States.* and *Seo v. State*. From *Fisher,* the *Andrews* case bases its inferred application of the foregone conclusion rule to apply to passcode-protected cellphones. However, the holding and usage of the foregone conclusion rule in *Fisher*

38. Hager, *supra* note 15.
39. *Andrews*, 234 A.3d. at 1259.
40. *Id.*
41. *Id.*
42. *Id.* at 1276.
43. *Id.*
44. *Id.* at 1275.

was applied to a very narrow set of facts, as argued by the litigants for the petitioner, Robert Andrews.[45]

In *Fisher,* which was two separate district court cases heard together, the Supreme Court held that privileges granted by the Fifth Amendment were "not violated by enforcement of documentary summons . . . for production of accountant's documents . . . which were not [petitioner's] 'private papers.'"[46] Both cases stemmed from two Internal Revenue Service (IRS) investigations into possible violations of United States tax laws. Prior to being interviewed by the IRS, in which they would have been required to personally produce certain tax documents, both petitioners sent their respective tax documents to their attorneys.[47] The IRS was thus seeking to compel the petitioners' attorneys to produce said tax documents, while petitioners claimed such a request was a violation of the Fifth Amendment. Application of the foregone conclusion rule arose from the Government's knowledge of the tax papers' existence. According to the court, "[t]he existence and location of the papers [were] 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."[48] The Court furthermore concluded that this did not amount to an act of testimony protected by the Fifth Amendment, but rather was an act of surrender.[49] Here, the relevant authorities were aware of the existence of those documents, and compelling the petitioners to forfeit them was not an act of self-incrimination because the production of the documents added nothing to the totality of the evidence against them.

On its own, the foregone conclusion rule is simple enough to understand when applied to physical documents: the relevant authorities have concrete knowledge of the existence of pertinent documentation and compelling the forfeiture of such documentation does not provide any new links in the chain of evidence against a defendant. Applying the same conclusion, however, to modern technology creates a standard that is less clear. The *Fisher* standard, when applied to cellphones, would open to law

45. Petition for Certiorari at 3, Andrews, v. New Jersey, 2021 WL 135207 (2021).

46. *Fisher*, 425 U.S. at 414.

47. *Id*. at 394.

48. *Id.* at 411.

49. *Id.* This recalls the "lock and key" analogy described above. Turning over the tax documents was a physical act of surrender akin to providing a key to a lock. Physical acts of production such as this are not considered to be testimonial in nature or a revelation of the contents of one's own mind. Thus, the defendants in *Fisher* did not receive Fifth Amendment protections and the foregone conclusion rule was established.

enforcement unlimited access to a wealth of personal information that may be stored on such devices.[50]

In *Seo v. State,* this very problem faced the Supreme Court of Indiana. In that case, the defendant refused to grant local police access to her phone during a stalking investigation in which the defendant had accused a third party of stalking her.[51] Here, the court ruled that the foregone conclusion rule did not apply because the state was unsure that the information they were seeking was definitively on Seo's locked cellphone:

> [C]ompelling Seo to unlock her iPhone would implicitly communicate certain facts to the State. And for those communicative aspects to be rendered nontestimonial, the State must establish that it already knows those facts. Even if we assume the State has shown that Seo knows the password to her smartphone, the State has failed to demonstrate that any particular files on the device exist or that she possessed those files.[52]

For the *Seo* court, it was not enough that the relevant authorities were able to establish that the cellphone belonged to Seo, that she was caught in possession of it, or that she undoubtedly would have knowledge of the password and the contents therein. Furthermore, the State needed to establish that they had knowledge of what they were trying to access and that they had knowledge that the information they were trying to access was stored on Seo's phone.[53]

The difference in applying the foregone conclusion rule to modern technology can be seen no clearer than in the cases of *Seo* and *Andrews.* In *Seo,* and for all those residing (or committing crimes) in the State of Indiana, relevant authorities need to show they are aware that pertinent information is currently housed on a device in order for the foregone conclusion rule to apply. Otherwise, compelling a defendant to input their passcode is a violation of the Fifth Amendment Self-Incrimination Clause. In *Andrews,* and for all those residing in the State of New Jersey, relevant authorities are not required to show such knowledge. In that state, merely showing that a phone belongs to a given defendant is enough for the foregone conclusion rule to apply and for said defendant to receive no protection under the Fifth Amendment.

Making these two cases distinct from a case like *Burr,* or even *Fisher,* is the technology itself. Cellphones now house an incredible

50. *Catch Me If You Scan, supra* note 14.
51. *Seo*, 148 N.E.3d 952.
52. *Id.* at 958.
53. *Id.*

amount of personal information.[54] In *Burr,* compelling Charles Willie to confirm his knowledge of a letter is relevant *only* to that letter; compelling the submission of tax documents is relevant *only* to the information contained in those documents. Thus, with the advent of modern technology, the precedents set in *Burr* and *Fisher* have not been applied in the same, analogous way across all judicial jurisdictions, causing citizens in one state to receive certain protections that those in another do not.

II. THE NEED FOR A JUDICIAL SOLUTION

From the holding in *Fisher* to the holdings in *Seo* and *Andrews,* a contradictory framework has emerged when applying the Self-Incrimination Clause to modern technology. Since the highest court has yet to do so, and indeed seems to be actively avoiding it, it would seem as though legislative measures are needed at the federal level to address the conflicting application of the self-incrimination clause. However, the most proficient solution is still through the judicial process. In 1807, the litigants in *United States v. Burr* understood that the Self-Incrimination Clause reflected the English Common Law standards.[55] Ultimately, a judicial solution is the most proficient one available because it will follow the same common law tradition established two centuries ago in *Burr,* not create wholly new standards that would likely develop from a regulatory committee or agency. The litigants in *Burr* understood that the privilege against self-incrimination was a fundamental right connected with the English common law,[56] and it is from the common law again that a solution to this dilemma must emerge.

A. The Difficulties of a Legislative Solution

A counterargument or counterproposal to a judicial solution is to create a federal regulatory committee or agency, subject to legislative oversight. However, such a solution is unlikely to address the lack of clarity surrounding modern technology because of constantly changing political winds, a characteristic unlikely to be altered in the coming election cycles, and because of the role that such agencies provide. Three examples that embody the political uncertainty of federal agencies are the Federal Communications Commission (FCC) and the policy of Net

54. *Catch Me If You Scan*, *supra* note 14.
55. Kerr, *supra* note 23, at 949.
56. *Id.* at 925.

Neutrality, the Federal Election Commission (FEC) and their role and force on national elections, and the Environmental Protection Agency (EPA) and its regulations of environmental policies.

Since 2015, the position of the FCC's stance on net neutrality has changed three different times—2015, 2018, and 2021. Net neutrality "is the principle that Internet Service Providers (ISP) must . . . offer equal access to all internet content to all without charging for faster or higher-quality delivery" speeds.[57] Following the ruling in *Verizon Communications Inc. v. FCC* (2014), the FCC issued the Open Internet Order in 2015, "which reclassified ISPs as common carriers subject to FCC regulation."[58] In 2018, under a different presidential administration, broadband companies were removed from the regulatory umbrella of the Open Internet Order, effectively nullifying all regulatory effect the Open Internet Order had on those companies.[59] Most recently in 2021, under yet another presidential administration, Executive Order 14036 restored the net neutrality rules that had only three years previously been done away with.[60] In sum, six years of federal oversight changed under three different presidential administrations, producing three different policies for regulating a crucial aspect of modern American information access.

The FEC and the EPA are no different. The FEC's decline into relative obsolescence began in 2010 following the decision in *Citizens United v. FEC*, which removed long-held campaign finance restrictions, enabling "corporations and other outside groups to spend unlimited funds on elections."[61] However, even prior to that, the FEC had been "long dysfunctional thanks to partisan gridlock."[62] Meanwhile, the EPA has been a partisan political issue since the 1980s, seeing its federal funding cut or increased depending on whichever political wind is blowing in a given year.[63]

Furthermore, a legislative solution is not likely to work because what is required is an updated *interpretation* of the Self-Incrimination Clause,

57. Lexi Hudson, *The Save the Internet Act: The Hero America Needs, But We Deserve Much Better,* 53 UIC L. REV. 607, 608 (2019).

58. *Id.* at 613.

59. *Id.* at 615.

60. Executive Order on Promoting Competition in the American Economy, July 9, 2021, at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/.

61. *Citizens United Explained,* BRENNAN CENTER FOR JUSTICE, https://www.brennancenter.org/our-work/research-reports/citizens-united-explained (last visited June 24, 2022).

62. *Id.*

63. *How the EPA Became a Victim of its Own Success,* NPR, https://www.npr.org/2017/02/17/515748401/how-the-epa-became-a-victim-of-its-own-success (last accessed June 24, 2022).

a task that is wholly unique to, and the primary function of, the judicial branch. The role of federal regulatory agencies is to *enforce* laws that are already interpreted and understood, setting certain standards to be followed by the public as well as law enforcement officers. An argument could also be made that it is through statutory law that this issue should be addressed. Such a solution would potentially give adequate notice of the rule and provide uniform application thereof. An argument could also be made that it is through statutory law that this issue should be addressed. Such a solution would potentially give adequate notice of the rule and provide uniform application thereof. However, given the breadth of knowledge exposed when a cellphone is unlocked, the inherent difficulty of writing a perfectly crafted, unambiguous statute to deal with this precise issue and as many future contingencies as possible seems unlikely, invoking the Courts to step in.[64] For these reasons, a federal regulatory agency will not resolve the issues plaguing modern application of the Self-Incrimination Clause. For these reasons, a federal regulatory agency will not resolve the issues plaguing modern application of the Self-Incrimination Clause.

B. The Need for a Modern Judicial Interpretation of the Self-Incrimination Clause

Rather than a legislative solution, what is required is a contemporary interpretation of the Fifth Amendment Self-Incrimination Clause that more consistently applies to the modern age of technology. As evident in *Andrews,* what has occurred in recent years is a judicial inconsistency among state and lower federal courts that has led the citizens of some states to be protected by the Fifth Amendment and citizens of other states left wanting, "The current split among federal and state courts . . . affords some people the benefit of the protection against self-incrimination and leaves others with no protection at all."[65] What has been created as a result is a set of conflicting opinions and a lack of judicial predictability.

64. Deborah Beth Meadows, *A Beginner's Guide to Legislative Drafting,* HARV. LAW SCHOOL J. LEGISLATION (Oct. 24, 2016), https://harvardjol.com/2016/10/24/a-beginners-guide-to-legislative-drafting/ ("[A] lack of precision can result in litigation that even involves the Supreme Court and can affect millions of individuals.") The broader debate of a regulatory solution versus a judicial one is beyond the scope of this essay. However, a judicial solution would be preferable because statutes subsequently require both enforcement and interpretation; they require interpretation of what the language means. This, in turn, could lead law enforcement into the same problems the judiciary is experiencing, as this essay examines. Such a statutory regulation would likely require Supreme Court interpretation at some point, but such a path would very likely also affect an indeterminate number of Americans in the meantime.

65. Petition for Certiorari at 18, *Andrews, supra* note 45.

Furthermore, the advancement of biometric technology has made application of the Fifth Amendment even more difficult and inconsistent, with lower courts obligated to decipher "obsolete Supreme Court precedent" to determine if it applies to the modern technological landscape.[66]

Organizations on both sides of the political spectrum have made note of this confusion and variance in judicial application. From the American Civil Liberties Union (ACLU) to the Federalist Society, calls have been made for the Supreme Court to take up this issue.[67] The ACLU goes so far as to recommend that the Court extend Fifth Amendment protections to password-protected cellphones and computers, "urging the U.S. Supreme Court to ensure the Fifth Amendment protection against self-incrimination extends to the digital age by prohibiting law enforcement from forcing individuals to disclose their phone and computer passcodes."[68]

Calls for the Court to specifically hear the *Andrews* case were also made by legal scholars, including Laurent Sacharoff.[69] It is Professor Sacharoff's belief that the currently used standard from *Fisher* does not apply to cellphones because *Fisher* was a compelled production of *pre-existing* documents, whereas cases like *Andrews* are not.[70] "When a Court orders a person to *state* her password, it has not ordered her to produce pre-existing documents; rather, it has ordered her to create, afresh, testimony. This Court could clarify that *Fisher*—and the foregone conclusion exception—do not apply because the premise triggering *Fisher* does not exist."[71] The advocates for Andrews go so far as to state that "*Fisher's* forty-five-year-old, narrow holding was not intended to be expanded beyond its factual setting of tax records, particularly not into the digital age."[72] A judicial solution to the issue is therefore necessary because the current standard is both outdated and inapplicable to the realities of today's technological landscape.

Furthermore, a modernized application of the Self-Incrimination Clause would be a continuation of the same judicial principles set forth in

66. Brittany A. Carnes, *Face ID and Fingerprints: Modernizing Fifth Amendment Protections for Cell Phones,* 66 LOY. L. REV. 183, 199-200 (2020).

67. Hager, *supra* note 15; ACLU, *supra* note 5.

68. ACLU, *supra* note 5.

69. Brief of Laurent Sacharoff as Amicus Curiae Supporting Petition for Certiorari at 4, Andrews v. New Jersey, 2021 WL 723113 (2021). Further discussion of Professor Sacharoff's interpretation is made in Section D of this essay.

70. *Id.*

71. *Id.*

72. Petition for Certiorari, *supra* note 45.

the English common law as it was applied to *Burr* two centuries ago: a common law interpretation for a common law dilemma. The Supreme Court thus needs to begin by determining whether compelled input of a passcode is a protected privilege in the modern age of technology, and how the foregone conclusion rule applies to such devices. An updated interpretation would not only clarify application of the foregone conclusion rule but also determine whether compelling the input of a cellphone password is analogous to an admission of knowledge or an act of compelled production.[73] As things currently stand, there are different approaches and standards across the United States. A legislative approach cannot make these same determinations for the reasons discussed above. Furthermore, any standards set by federal regulatory agencies would likely be challenged in court, continuing a dizzying and unending cycle of unclear and inconsistent fundamental rights.

C. Why a Judicial Solution Provides More Stability

Ultimately, a judicial solution to the dilemma is more appropriate because of the interpretive stability such a solution would provide. Conversely, a cursory glance at the stature of the federal courts would indicate that they, like the legislative branch and federal agencies, are equally subject to shifting political winds. One need only look to the varying ways in which the Supreme Court has interpreted the Commerce Clause of the U.S. Constitution throughout the Court's various eras or the Court's majority opinion in *Dobbs v. Jackson Women's Health Organization* to see these shifts in action.[74] One issue in which the Court has remained consistent in the modern era, however, is its interpretation of the fundamental right to privacy as it relates to Fourth Amendment protections and the "plain view doctrine."

1. The Plain View Doctrine

Federal courts have consistently held that privacy is at the very heart of Fourth Amendment principles, including warrantless searches and the plain view doctrine. In *Torres v. Madrid*, the Supreme Court held that privacy is of the very "essence" of Fourth Amendment precedent.[75] The Fifth Circuit Court of Appeals recently held similarly, stating that the basic purpose of the Fourth Amendment "is to safeguard individuals

73. Kerr, *supra* note 23, at 913.
74. 142 S.Ct. 2228 (2022).
75. 141 S.Ct. 989 (2021).

against arbitrary invasions of property by government officials."[76] With regard to warrantless searches by government officials, the Seventh Circuit recently reaffirmed that they "are per se unreasonable under the Fourth Amendment, subject only" to a few specific and well-established exceptions.[77]

The plain view doctrine is perhaps the most relevant rule associated with the Fourth Amendment that can also be readily applied to an analysis of the Fifth Amendment. This doctrine "permits the warrantless seizure of an item if the officer is lawfully present, in a position from which the item is clearly visible, there is probable cause to seize the item, and the officer has a lawful right of access to the item itself."[78] If one considers a smartphone as fundamentally similar to a place of residence, then the judiciary's interpretation of the plain view doctrine can be used to support an argument for judicial interpretation as being a more able resolution to the Fifth Amendment quandary laid forth above. The interpretive longevity that exists with the Court's understanding of the plain view doctrine would ultimately support the view that a modern judicial interpretation is preferable to a legislative solution despite the court's own subjectivity to political shifts.

The plain view doctrine was first established in 1971 with the case *Coolidge v. New Hampshire.* That case established three factors for application: (1) the officer must be present in the place where the evidence is viewed; (2) the officer must have probable cause to believe the item is evidence of a crime; and (3) the evidence must be viewed inadvertently (unintentionally) by the officer.[79] Fifty-years later, the plain view doctrine was invoked again to deny certiorari where local game wardens had tested the limits of the doctrine.[80] In that case, state officials had entered private property and began searching the property owner's garage via an open window without the owner's consent or knowledge. In a separate opinion, Justice Gorsuch, joined by Justice Sotomayor and Justice Kagan, stated that the plain view doctrine does not apply where officials do not have legal authority to be present on private property. "No one, after all, thinks an officer can unlawfully break into a home, witness illegal activity, and then claim the benefit of the plain view doctrine."[81] This interpretation

76. *United States v. Johnlouis*, 44 F.4th 331, 336 (5th Cir. 2022).

77. *United States v. Tuggle*, 4 F.4th 505, 512 (7th Cir. 2021) (quoting *United States v. Edwards*, 769 F.3d 509, 513 (7th Cir. 2014)).

78. *United States v. Casellas*, 149 F. Supp. 3d 222, 237 (D.N.H. 2016) (quoting *United States v. Gamache*, 792 F.3d 194, 199 (1st Cir. 2015).

79. 403 U.S. 443 (1971).

80. *Bovat v. Vermont*, 141 S.Ct. 22 (2020).

81. *Id.* at 23.

has also been applied in recent years by lower federal courts, such as *United States v. Casellas,* to further show that probable cause is an important element of the plain view doctrine. In that case, where an item was warrantlessly seized during a legal search, the court stated that "probable cause exists when the incriminating character of an object is immediately apparent to the police."[82] Under this context, incriminating evidence that is outside the scope of a warrant is not inherently or "immediately apparent" unless it occurs within the natural course of a search.

2. The Plain View Doctrine as an Analogy

The plain view doctrine is a compelling analogy that can be applied to smartphone technology and simultaneously show why a judicial solution is ultimately the preferable option. First, the nature and breadth of personal content that resides on a smartphone is adequately comparable to that of a house or of some other real property. The way in which content is stored on a smartphone is functionally similar to the way in which items are stored in a place of residence. A place of residence has several rooms, drawers, and closets that are used by its residents to house everyday items and long-forgotten items alike. Often one of these rooms will have a desk or a bureau that will include a drawer that is locked, only to be opened by use of a key. Many homeowners also use a safe to store sensitive and/or valuable materials. In each of these cases, a search warrant must explicitly identify them as a notable place to be searched by government officials.[83] A smartphone functions in a very similar way: the home screen passcode acts as the front door, while each application acts as a separate room, drawer, or closet containing unique and personal information specific to its owner. An application may even have its own unique passcode to input before it can be accessed.

Second, application of the plain view doctrine shows the longevity of judicial precedence when a question of actual privacy–an invasion of personal liberty by government officials—is at hand. The cases above show a common law tradition that has continued throughout several generations of judicial interpretation. These cases also show that a judicial approach is preferable to a legislative solution to the issue of self-

82. 149 F. Supp.3d 222, 237 (2016).

83. WAYNE LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 4.5 (6th ed. 2022). "When a description is insufficient in this sense, then the search warrant is invalid and, under the traditional view, it would as a consequence be necessary to suppress any evidence obtained in reliance upon that warrant."

incrimination as it pertains to smartphone technology because they show a common law tradition at various levels of the judiciary preventing overreach by government officials. The issue most pertinent to the plain view doctrine is government officials overstepping the boundaries of a search warrant or the application of probable cause. Allowing government officials carte blanch access to a witness's smartphone is akin to removing these boundaries that protect them from searches of their residence.

D. What the Supreme Court Should Ultimately Determine

The question at hand regards the information that is held on the phone or device, and which lies behind the encryption or biometric ID, not the passcode or the phone itself. How does a prosecutorial team ensure it gets the relevant answers it seeks without simultaneously abridging a witness's Fifth Amendment protections? Furthermore, how does the court protect an individual from *subsequent* prosecution because of what is found on that individual's phone during compelled testimony?

While use and derivative use immunity are two available options, the power to grant immunity is not inherently with the judiciary.[84] The Federal Rules of Evidence can also limit the scope of evidence, but those rules only apply to current proceedings and not subsequent use.[85] While the executive branch or a prosecutorial team may, on its own, grant use or derivative use immunity for such testimony, such a privilege cannot be court-ordered for fear of an overreach of judicial power. Because of these realities, the court should incorporate the standard set in *Seo v. State* and rule that mere knowledge of a passcode is not enough to compel testimony. Determining that mere knowledge of a passcode is sufficient, like in *Commonwealth v. Jones,* is too broad of a power to be given to the executive branch of government particularly as it relates to modern technology.

This conclusion was drawn by the Supreme Court of Indiana in the *Seo* case, which highlighted the fact that authorities "failed to demonstrate that any particular files on the device exist or that [Seo] possessed those files."[86] That court also made note of three concerns associated with extending the foregone conclusion rule established in *Fisher* to the compelled production of unlocking a smartphone. First, while smartphones contain substantially more private information than an individual's tax returns, "there is no limiter like a documentary subpoena

84. *State v. Quigley*, 883 N.W.2d 139, 150 (Wis. App. 2016).
85. FED. R. EVID. 105.
86. *Seo*, 148 N.E.3d at 958.

for specific files."[87] Secondly, by the very nature of smartphones, it is extremely difficult to restrict access to law enforcement's search for information once the phone is unlocked, thereby giving complete access to every piece of data so located.[88] Thirdly, the precedent established in *Fisher,* the same one used in the *Andrews* case, would "mean expanding a decades-old and narrowly defined legal exception (the foregone conclusion rule) to dynamically developing technology that was in its infancy just decades ago."[89] Ultimately, the court determined that far better avenues are available to government authorities, such as the Stored Communications Act or a grant of derivative use immunity, that would avoid these Fifth Amendment questions of carte blanche access to any and all information stored on a witness's smartphone.[90]

Chief Justice Roberts espoused similar difficulties in the majority opinion in *Riley v. California* six years prior to the ruling in *Seo.*[91] In this opinion, the Chief Justice used the two-pronged test established in *Chimel v. California*.[92] Where there is a custodial arrest, two risks are identified when a search of an arrestee is made and evidence is potentially found on their person: harm to the arresting officer(s) and the potential destruction of evidence.[93] Even where those risks are not apparent, an officer is free from Fourth Amendment constraints and is able to search through those items if the search is reasonable and based upon probable cause.[94] However, for the Chief Justice, this type of analogy is insufficient when applied to modern cellphone technology, which differs from other physical items both quantitatively and qualitatively.[95] The storage capacity alone of a modern smartphone holds several interrelated consequences that have the ability to summarize and reconstruct an individual's private life through access of dozens of gigabytes of information. The same cannot be said for physical evidence; it is not feasible for someone to carry thousands of physical photos like they do their digital counterparts on a smartphone. Allowing an arresting officer to scrutinize such information as part of routine searches subsequent to an arrest is fundamentally different than searching one to two personal items

87. *Id.* at 959.
88. *Id.* at 960.
89. *Id.* at 962.
90. *Id.*
91. 573 U.S. 373 (2014).
92. 395 U.S. 752 (1969).
93. *Riley,* 573 U.S. at 386.
94. *Id.* at 383.
95. *Id.* at 393.

an arrestee may have on their person at the time of an arrest.[96] The Chief Justice concludes by stating that while smartphones are not immune from searches altogether, "a warrant is generally required before such a search" is initiated because of the vast amounts of stored personal information an individual typically has on their smartphone.[97]

In *Andrews,* the question was whether the defendant's Fifth Amendment protections were violated when he was compelled to unlock his two smartphones by way of a search warrant. The issue is not that a warrant was issued or that Andrews was compelled to unlock his smartphones. It is that the warrant was overly broad in its scope and did not specifically identify what evidence law enforcement officials definitively knew would be stored on those smartphones. Generally, search warrants must state with particularity what information or evidence law enforcement officials intend to search and seize; Chief Justice Roberts's opinion extends this requirement to smartphones under the fundamental rights guaranteed by the Fourth Amendment.

The decision in *Andrews* effectively permits law enforcement officials to claim that the foregone conclusion rule waives this requirement where it can be unquestionably established that a witness or defendant owns a particular piece of technology. As has been discussed, however, this waiver is not consistently granted across every state. Taking this into consideration, the Supreme Court should update the application of the Self-Incrimination Clause by reaching two related holdings: (1) that the foregone conclusion rule should not apply merely to the unlocking of a person's smartphone; and (2) that the particularity requirement of search warrants should be extended to require law enforcement officials to specifically identify which applications and what information from those applications it is seeking.

The standard in *Riley* established that modern smartphone technology houses information far too great to allow law enforcement officials open access to any and all files stored on it. The *Seo* court understood this reality and applied the foregone conclusion rule accordingly, holding that law enforcement officials must state with particularity what information it is seeking and what applications it wishes to search. That court went on to state that allowing such unfettered access would be the death of Fifth Amendment protections in America.[98] Both of those courts realized the implications of allowing such access, causing

96. *Id.* at 395.
97. *Id.* at 401.
98. *Seo*, 148 N.E.3d 952 (quoting *Commonwealth v. Jones*, 117 N.E.3d 702 (Mass. 2019)).

both to reason that law enforcement needs to state with particularity, even where a search warrant is involved, the information they are seeking and specifically where on the smartphone they wish to search.

III. CONCLUSION

Given the ubiquitous nature of modern smartphone technology, application of the law and of fundamental rights needs to be updated accordingly. The way in which the Self-Incrimination Clause of the Fifth Amendment has been understood as it applies to this technology has been inconsistent across the state court level, granting some a fundamental protection against self-incrimination and not granting it for others. The issue is not that the *Andrews* court held differently from the *Seo* court but that there are different standards for citizens residing in different states. A modern, judicial interpretation of the Fifth Amendment Self-Incrimination Clause is therefore required to provide clarity where none currently exists. Such a solution is preferable to a legislative one even though appearances would lend one to believe that the judicial branch is just as subject to political winds as the legislative branch. While interpretation of certain rights and government powers have shifted over time and over the course of judicial eras, certain rights and liberties have remained absolute despite these changes. Where this is seen to be the truest is in regard to the individual right to privacy in cases of government intrusion. Applying the foregone conclusion rule to hold that mere knowledge of a passcode is sufficient to compel production thereof is a form of government intrusion because of the mountains of personal information a smartphone typically carries. As is seen with the plain view doctrine of the Fourth Amendment, the Supreme Court has historically favored the individual in these cases and should continue that historical application in a modern interpretation of the Self-Incrimination Clause.