YOUR SECRET CELL PHONE PASSCODE MAY NOT BE A SECRET FOR LONG: THE UNCERTAINTY OF COMPELLED PASSWORD PRODUCTION

Michael Seager*

I. INTRODUCTION

Imagine that police arrive at your door and hand you a valid search warrant. Officers enter your home and start grabbing documents, hard drives, computers, and your beloved smart phone. Officers request your cell phone passcode, and you refuse to give it. Depending on the state or jurisdiction you live in, not only would you have to hand over your phone, but you could also be ordered by a judge to provide your phone passcode, essentially assisting the government in your own prosecution.

The compelled disclosure of a cell phone passcode violates an individual's Fifth Amendment right against self-incrimination. In the criminal law context, modern technological advancements have vastly outpaced obsolete laws and procedures. Without clear guidance from the United States Supreme Court on the critical constitutional issue of whether the government can compel a criminal defendant to unlock his phone, lower courts have been left holding the bag and are divided on the issue.[1]

* J.D. Candidate 2023; Lead Article Editor of the Southwestern Law Review, 2022-2023. Thank you to my wife, Nahal, and my two daughters, Olivia and Isabella, who inspire me every day. Without their love and support, this Note would not have been possible. Thank you to my father, Edward Seager, for showing me that that a law career is possible with enough hard work and tenacity. Lastly, thank you to the Southwestern Law Review Professors, Executive Board, and Staff members for their tireless efforts in refining this Note.

1. *See generally* Greg S. Sergienko, *Self Incrimination and Cryptographic Keys*, 2 RICH. J.L. & TECH. 1 (1996); Michael S. Mahoney, *Compelling the Production of Passwords: Government's Ability to Compel the Production of Passwords Necessary to the Discovery of Encrypted Evidence in Criminal Proceedings, Merely a Choice of Words*, 6 T.M. COOLEY J. PRAC. & CLINICAL L. 83 (2003). *Compare* State v. Andrews, 234 A.3d 1254, 1273, 1275 (N.J. 2020) (finding that the act of unlocking a cell phone is a testimonial act which ordinarily receives protection under the Fifth Amendment of the U.S. Constitution (which the court later nullified by applying an exception)),

In *State v. Andrews*, the New Jersey Supreme Court held that "neither federal nor state protections against compelled disclosure shield" a defendant's passcodes.[2] The court correctly acknowledged that entering a passcode into a cell phone requires communication from the owner's mind and is, therefore, a "testimonial act" as defined by the Fifth Amendment.[3] However, as a result of the court's erroneous decision that the "foregone conclusion" exception to the Fifth Amendment is applicable, a defendant's constitutional protections are nullified.[4]

Part II of this Note provides a background and examines the Fifth Amendment, its exceptions, and issues that arise in the context of compelled cell phone passcode disclosure. Part III discusses the reasons for and against compelled disclosure based on various interpretations of lower courts. Particular attention is paid on the Fifth Amendment's foregone conclusion exception. Part IV examines the catastrophic consequences of the erroneously decided cases and the troubling precedent that has been established. Finally, Part V proposes a clear, easily applicable standard for courts to apply that is consistent with modern technology and societal norms.

II. BACKGROUND

A. Why Cell Phones Matter in Modern Society

Today, smartphones are incredibly prevalent. Ninety-seven percent of adults in the United States use cell phones, and eighty-five percent of those are smartphones.[5] With phone calls, text messages, emails, photos, social media, GPS locations, banking information, and various third-party applications, it is not surprising that a person's phone can store evidence of a crime. In many instances, a cell phone is the most important, or only tool

---

and State v. Pittman, 479 P.3d 1028, 1051 (Or. 2021) (holding that in order to compel a defendant to unlock their cell phone, the state must already know the information that doing so would produce), *and* Commonwealth v. Davis, 220 A.3d 534, 551 (Pa. 2019) (holding that the act of unlocking a cell phone is a testimonial act which is protected by the Fifth Amendment of the U.S. Constitution), *and* Eunjoo Seo v. State, 148 N.E.3d 952, 962 (Ind. 2020) (finding that the state cannot "fish" through the contents of a cell phone without knowing that the files they are looking for on the phone exist or that they are possessed by the defendant), *with* People v. Sneed, 187 N.E.3d 801, 819 (Ill. App. Ct. 2021) (finding that the act of unlocking a cell phone itself is a nontestimonial act and is not protected by the Fifth Amendment of the U.S. Constitution).

2. *Andrews*, 234 A.3d at 1277.

3. *Id.* at 1273.

4. *Id.* at 1275.

5. *Mobile Fact Sheet*, PEW RESEARCH CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/ [https://perma.cc/896C-MET3].

for law enforcement and prosecutors to obtain the incriminating evidence needed to charge and convict a defendant.[6]

Under Fourth Amendment jurisprudence, law enforcement officers may confiscate an item, such as a cell phone, if they believe it contains evidence of a crime, even if a warrant has not yet been obtained. However, they may not conduct a search of the item until a warrant is issued.[7] When police seize a cell phone and the owner refuses to unlock it or provide the passcode, complications arise. In this scenario, the prosecutor would file a motion to compel, allowing the judge to compel the defendant to disclose their cell phone passcode or face contempt of court.

For purposes of this Note, law enforcement is deemed to have a lawful search warrant if they seize a suspect's cell phone because they believe it contains incriminating evidence. While there is considerable debate on whether the government can successfully break into a locked smartphone, even if they occasionally can, it is certainly not commonplace.[8] In high-priority cases, the Federal Bureau of Investigation (FBI) has successfully broken into a suspect's phone, but only after investing significant time and resources.[9]

In response to this government action, major smartphone retailers, such as Apple (which manufactures the highly popular iPhone device), have strengthened the privacy protections on the devices they manufacture.[10] Apple has gone so far as to claim that its more recent operating systems are designed to be impenetrable.[11]

Since it is evident that the government has difficulty accessing a suspect's passcode-protected cell phone, the question becomes whether the government can compel an individual to unlock their phone by disclosing the

---

6. Ajay Krishnan, *The Cellphone: Most Crucial Piece of Evidence in Criminal Investigations*, MEDIUM (Nov. 18, 2019), https://medium.com/@ajaykrishnan25/the-cellphone-most-crucial-piece-of-evidence-in-criminal-investigations-97baba6b1d02 [https://perma.cc/YUQ3-6Q6B].

7. *See* Riley v. California, 573 U.S. 373, 401-03 (2014).

8. Riana Pfefferkorn, *The FBI is Mad Because it Keeps Getting Into Locked iPhones Without Apple's Help*, TECHCRUNCH (May 22, 2020, 2:33 PM), https://techcrunch.com/2020/05/22/the-fbi-is-mad-because-it-keeps-getting-into-locked-iphones-without-apples-help/ [https://perma.cc/EBD6-JX7Z].

9. *See* Attorney General William P. Barr Announces Updates to the Findings of the Investigation into the December 2019 Shooting at Pensacola Naval Air Station, U.S. DEP'T OF JUST. (May 18, 2020), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-updates-findings-investigation-december-2019 [https://perma.cc/P36K-4DMA].

10. *See* Craig Timberg, *Apple Will No Longer Unlock Most iPhones, iPads for Police, Even with Search Warrants,* WASH. POST (Sept. 18, 2014), https://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html [https://perma.cc/TL56-TCKG].

11. *See id.*

passcode. This raises critical issues under the Fifth Amendment's constitutional protection of an individual's right against self-incrimination.

B. The Fifth Amendment Self-Incrimination Clause

In accordance with the Fifth Amendment self-incrimination clause, "[n]o person . . . shall be compelled in any criminal case to be a witness against himself."[12] The privilege can be asserted in any civil or criminal proceeding or investigation to protect information that a person "reasonably believes could be used in a criminal prosecution or could lead to other evidence that might be so used."[13] Importantly, the U.S. Supreme Court has held that the Fifth Amendment privilege "protects the innocent as well as the guilty."[14] In other words, there is no requirement that the defendant must be guilty or have something to hide, to assert their Fifth Amendment privilege. Instead, the accused may assert the privilege for any information he believes could be used against him or lead to evidence that might be used against him in a criminal proceeding.[15]

The government bears the burden to produce evidence against an accused rather than compelling the individual to provide it.[16] The consequence of the Fifth Amendment, according to the Supreme Court, is that if the state "proposes to convict and punish an individual [it must] produce the evidence against him by the independent labor of its officers, not by the simple, cruel expedient of forcing it from his own lips."[17]

The suspect's ability to invoke the privilege depends on the nature of the statement and the likelihood of the statement to expose the suspect.[18] In *Schmerber v. California*, the Supreme Court held that the Fifth Amendment only protects an accused against testimonial or communicative compulsion.[19] To assert Fifth Amendment privilege, the communication must be testimonial, incriminating, and compelled.[20]

When a suspect is subpoenaed, or the court grants a motion to compel, the suspect's subsequent testimony is clearly compelled. Therefore, "compelled" testimony is generally not an issue in Fifth Amendment cases. Regarding the "incriminating" prong, the Court has stated that the Fifth

12. U.S. CONST. amend. V.
13. Kastigar v. United States, 406 U.S. 441, 444-45 (1972).
14. Ohio v. Reiner, 532 U.S. 17, 18 (2001).
15. *Kastigar*, 406 U.S. at 444.
16. Miranda v. Arizona, 384 U.S. 436, 460 (1966).
17. Estelle v. Smith, 451 U.S. 454, 462 (1981).
18. *Id.*
19. 384 U.S. 757, 761 (1966).
20. Hiibel v. Sixth Jud. Dist. Ct. of Nev., Humboldt Cnty., 542 U.S. 177, 189 (2004).

Amendment protects testimony that "would furnish a link in the chain of evidence needed to prosecute."[21] Therefore, the privilege protects any compelled testimony, even if not inherently incriminating itself, but could lead to incriminating evidence against an individual.[22]

In many Fifth Amendment cases, the issue is whether the defendant's communication or act is a "testimonial communication," and thus qualifies for protection. Cases involving the supplying of a cell phone passcode are not an exception and can hinge on whether the disclosure of the passcode qualifies as a "testimonial communication."

1. Testimonial Communications

The Supreme Court has struggled to clearly define what qualifies as testimonial communication, but it has offered some guidance: "in order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a 'witness' against himself."[23]

To qualify as testimonial communication, an individual must disclose the contents of his own mind.[24] Further, "'[t]he vast majority of verbal statements thus will be testimonial'" because a verbal statement will usually convey information or assert facts.[25] The statement is testimonial when a suspect is compelled to communicate an express or implied assertion of fact or belief.[26] The goal is to avoid putting a suspect in the "cruel trilemma" of having to communicate either a truth, falsity, or silence.[27]

While the accused's communications are clearly protected,[28] compelled physical evidence is considered nontestimonial and therefore unprotected. For example, physical evidence such as blood testing, fingerprinting, or standing in a photo lineup, is not testimonial evidence because these acts do not communicate the individual's subjective thoughts.[29]

2. Foregone Conclusion Doctrine

In addition to verbal and written communications, the privilege against self-incrimination has also been held to apply to the production of documents

21. Hoffman v. United States, 341 U.S. 479, 486 (1951).
22. United States. v. Hubbell, 530 U.S. 27, 38 (2000).
23. Doe v. United States, 487 U.S. 201, 210 (1988).
24. *Id.* at 211.
25. Pennsylvania v. Muniz, 496 U.S. 582, 597 (1990) (quoting *Doe*, 487 U.S. at 213).
26. *Id.*
27. *Id.*
28. Schmerber v. California, 384 U.S. 757, 763-64 (1966).
29. *Id.* at 764.

in response to a government subpoena because the act of producing the records itself could be incriminating.[30] Some courts have applied the act of production and "foregone conclusion doctrine" in cases involving compelled passcode disclosure, while others have not.[31] The foregone conclusion doctrine is a limited exception to the Fifth Amendment privilege against self-incrimination. When the existence, location, and authenticity of a document is a foregone conclusion that "adds little or nothing to the sum total of the Government's information," the Fifth Amendment does not protect the act of evidence production.[32] The government must show with "reasonable particularity" that the evidence was sought, that they had knowledge of its existence, that the evidence was in the defendant's possession and control, and that the evidence is authentic.[33]

The foregone conclusion doctrine arises out of the unique facts of *Fisher v. United States* where the government sought to obtain the defendant's tax records.[34] The records were obtained from the defendant's accountant, who prepared the records, and provided them to his lawyers.[35] Citing the Fifth Amendment privilege, the defendant's lawyers refused to turn over the records to the law enforcement.[36] The Court found that the existence and location of the paper records were a foregone conclusion, and the defendant's admission that he possessed those records added little to no information to the government's evidence.[37] Under those circumstances, the Court reasoned that there was no violation of the Fifth Amendment and that the issue was the surrender of the documents themselves, not testimony.[38]

The Supreme Court has rarely addressed the foregone conclusion doctrine since *Fisher*. In *United States v. Hubbell*, the government subpoenaed the defendant's tax-related documents.[39] The Court held that the act of production (supplying the documents) required the defendant to use the contents of his mind, qualifying it as a testimonial act.[40] The focus there

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

31. *See* State v. Andrews, 234 A.3d 1254, 1273, 1275 (N.J. 2020) (applying the foregone conclusion doctrine); *see also* State v. Stahl, 206 So. 3d 124, 135-37 (Fla. Dist. Ct. App. 2016) (applying the foregone conclusion doctrine). *But see* G.A.Q.L. v. State, 257 So. 3d 1058, 1066 (Fla. Dist. Ct. App. 2018) (refusing to apply the foregone conclusion exception).

32. *Fisher*, 425 U.S. at 411.

33. United States v. Hubbell, 530 U.S. 27, 32-33 (2000).

34. *Fisher*, 425 U.S. at 391.

35. *Id.*

36. *Id.* at 393-95.

37. *Id.* at 411.

38. *Id.*

39. 530 U.S. 27, 31 (2000).

40. *Id.* at 43.

was that the act of document production—while clearly not pure verbal testimony—qualified as testimonial since it was for documents unknown to the government. The foregone conclusion exception does not apply if the defendant is compelled to produce information that reveals the existence, possession or control, and authenticity of evidence. The defendant in *Hubbell*, therefore, was able to assert his Fifth Amendment privilege and the foregone conclusion exception failed.[41] Referring to *Doe v. United States*, the Court in *Hubbell* noted that producing the documents was akin to revealing "the combination to a wall safe" rather than "being forced to surrender the key to a strongbox."[42] Notably, the Court criticized the foregone conclusion exception for being vague, stating that "[w]hatever the scope of this 'foregone conclusion' rationale, the facts of this case plainly fall outside of it."[43] The court went on to state that "[w]hile in *Fisher* the government already knew that the documents were in the attorneys' possession and could independently confirm their existence and authenticity through the accountants who created them, here the government has not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent."[44]

3. What happened in *State v. Andrews*?

In *Andrews*, the defendant was a deputy sheriff who was charged by the state of New Jersey with allegedly providing a suspect in a narcotics investigation, Quincey Lowery, with information that allowed him to avoid police surveillance.[45] Lowery, who met the defendant through a motorcycle club, told detectives that the defendant was calling, texting, and sending him photographs, to help Lowery avoid surveillance and a tracking device inside his vehicle.[46] The state obtained a warrant for the defendant's arrest and a search warrant to search his two iPhones.[47] The police seized the phones but the defendant refused to disclose the passcodes, invoking his Fifth Amendment right against self-incrimination.[48] The trial court held that the defendant was not entitled to Fifth Amendment protection because the act of

41. *Id.* at 43-44.
42. *Id.* at 43 (citing Doe v. United States, 487 U.S. 201, 210 (1988)).
43. Id. at 44.
44. *Id.* at 44-45.
45. State v. Andrews, 234 A.3d 1254, 1273, 1259 (N.J. 2020).
46. *Id.* at 1260.
47. *Id.* at 1261.
48. *Id.*

being compelled to turn over the phone passcode was not testimonial.[49] The appellate division affirmed, reasoning that although the act of producing information may be testimonial, the Fifth Amendment affords no protection to a defendant when the act of producing that evidence is a foregone conclusion.[50] The court held that the state had proven that the defendant owned, possessed, and controlled the evidence, satisfying the foregone conclusion exception.[51] The New Jersey Supreme Court affirmed and held that the act of producing the iPhone passcodes was testimonial because compelling its disclosure implied an assertion of fact, but the foregone conclusion exception applied.[52] Therefore, the defendant was not entitled to assert the Fifth Amendment privilege.

C. Cases that Applied the Foregone Conclusion Doctrine

Andrews is not the only case that applied the foregone conclusion doctrine to analyze the compelled disclosure of a cell phone passcode. In *State v. Stahl*, the defendant was charged with video voyeurism.[53] The police seized the defendant's cell phone pursuant to a valid search warrant to obtain the alleged video footage.[54] The authorities could not access the cell phone data since it was password-protected.[55] The state filed a motion to compel production of the passcode,[56] arguing that the production was not testimonial communication because the evidence was a foregone conclusion, or alternatively, because the production did not require use of the defendant's mind.[57] The trial court denied the state's motion and held that the disclosure of a passcode was testimonial evidence and therefore protected by the Fifth Amendment privilege against self-incrimination.[58] The Florida District Court of Appeal reversed, holding that the disclosure of the passcode lacked sufficient testimonial significance and that its production was a foregone conclusion; hence the Fifth Amendment protection did not apply.[59]

---

49. *Id.* at 1261-62.

50. Defendant's Brief in Support of His Interlocutory Appeal of the Appellate Division's Decision Compelling Defendant to Disclose His Cell Phone Passwords in Violation of His Right Against Self-Incrimination at 6, *Andrews* 234 A.3d 1254 (N.J. 2020) (No. A-000291-17).

51. *Andrews*, 243 A.3d at 1275.

52. *Id.* at 1274.

53. 206 So. 3d 124, 127 (Fla. Dist. Ct. App. 2016).

54. *Id.* at 128.

55. *Id.*

56. *Id.*

57. Initial Brief of Appellant at 2, *Stahl*, 206 So.3d 124 (Fla. Dist. Ct. App. 2016) (No. 2D14-4283).

58. *Stahl*, 206 So.3d at 128.

59. *Id.* at 134, 136.

However, other courts have reached different conclusions. In *G.A.Q.L. v. State*, decided two years after *Stahl* in a different Florida appellate district, the court held that the compelled disclosure of a cellphone passcode is a testimonial communication.[60] The court reasoned that the foregone conclusion doctrine was not satisfied because the state could not show with "reasonable particularity" anything beyond the fact that the passcode existed.[61] The court found that the state "incorrectly focused on the passcode as the target of the foregone conclusion exception rather than the data shielded by the passcode." The Fourth District stated that the Second District's analysis in *Stahl*, which focused on the passcode, was flawed.[62]

In *People v. Spicer*, the police found cocaine in the defendant's vehicle after they pulled over the vehicle he was traveling in.[63] The police seized the defendant's phone, and the court issued a search warrant.[64] The cell phone was inaccessible to law enforcement, and the defendant refused to provide the passcode.[65] The defendant successfully relied on *G.A.Q.L.* and the court denied the government's motion to compel because the phone's contents were not a foregone conclusion.[66]

III. LOWER COURTS MISAPPLIED BINDING PRECEDENT AND ERODED CONSTITUTIONAL PRIVACY RIGHTS BY COMPELLING PASSCODE DISCLOSURE

A. State v. Andrews *Missed the Mark*

Andrews was wrongly decided. The New Jersey Supreme Court correctly found that compelling the defendant to reveal his phone passcode constituted a testimonial act, but erroneously held that the foregone conclusion exception to the Fifth Amendment applied.[67] To justify the result, the court incorrectly focused on the act of producing the passcode itself, as was done in *Stahl*, rather than on the actual contents of the defendant's phone.[68] Clearly, the state does not care what the actual numerical passcode is; the state is interested in the phone's contents (text messages, emails, etc.). Even under the forgone conclusion analysis, the state has not met its burden

60. 257 So. 3d 1058, 1061-62 (Fla. Dist. Ct. App. 2018).
61. *Id.* at 1064.
62. *Id.* at 1063-64.
63. People v. Spicer, 125 N.E.3d 1286, 1288 (Ill. App. Ct. 2019).
64. *Id.*
65. *Id.* at 1288-89.
66. *Id.* at 1289.
67. State v. Andrews, 234 A.3d 1254, 1273-74 (N.J. 2020).
68. *See id.* at 1294.

because it could not prove authenticity of the passcode, which is precisely why the state compelled the defendant to provide it. Despite this, the court allowed the state to bypass this requirement under the theory that a valid passcode will unlock the phone, and thus, self-authenticated it.[69] The court stretched the foregone conclusion doctrine to destroy the constitutional protections the defendant was entitled to when it accepted as true the uncorroborated word of a witness regarding what was on the defendant's phone and held that forcing passcode disclosure would self-authenticate the defendant's control of the data sought. The court missed the point that, at the very least, the analysis should have focused on the evidence sought, namely the phone contents, rather than the phone passcode itself.

1. Compelled Cellphone Passcode Disclosure Qualifies for Fifth Amendment Protection

Being forced to disclose a cell phone passcode qualifies for Fifth Amendment protection because it is incriminating, compelled, and testimonial. As mentioned above, for purposes of this Note, the defendant's passcode is presumed seized pursuant to a lawful warrant, the defendant has refused to disclose the passcode, and the state is attempting to compel disclosure (typically by a motion to compel). In this context, the defendant is compelled to provide the passcode.

Next, disclosure of a passcode is incriminating. Typically, consisting of a simple four- or six-digit numerical sequence, a passcode does not by itself generate incriminating information. There is nothing inherently incriminating by releasing those numbers. Nonetheless, the Supreme Court has made it abundantly clear that the actual disclosure itself need not be incriminating.[70] The testimonial communication should merely convey implicit incrimination or serve as a "link in the chain" of evidence that can be used to criminally prosecute a defendant.[71] In other words, disclosing the passcode itself may not be incriminating, but the vast contents of a cell phone may be.

Finally, and as acknowledged even by the *Andrews* Court, revealing a smartphone passcode is clearly a testimonial communication. As opposed to a physical act, verbal or written communication is the purest form of testimony because verbalizing a passcode requires a person to "use the contents of one's own mind" and memory. This communication relates a

69. *Id.* at 1272.

70. United States v. Hubbell, 530 U.S. 27, 37-38 (2000).

71. Hoffman v. United States, 341 U.S. 479, 486 (1951).

factual assertion and discloses information, such as the fact that the code is 1-2-3-4.

Disclosing a cell phone passcode is like revealing "the combination to [a] wall safe"[72]—not like being "forced to surrender a key to a strongbox."[73] Handing over a key has clear physical characteristics, and as such has been found by the Court to be afforded less protection. Physically handing over a key does not compel a defendant to disclose the contents of her mind. However, verbal disclosure of a cell phone passcode is the purest form of testimony and is akin to providing the combination to a wall safe. Therefore, because the disclosure of a cell phone passcode is testimonial, incriminating, and compelled, it is entitled to full protection under the Fifth Amendment.

2. The Foregone Conclusion Exception Does Not Apply to Passcode Production Cases

The compelled disclosure of a cell phone passcode simply does not trigger the outdated *Fisher* foregone conclusion exception. In *Fisher*, the government compelled the defendant to produce physical documentation, which triggered the "act of production" analysis, where Fifth Amendment protection is afforded to the act of document production has testimonial aspects. The forgone conclusion doctrine is an exception to the act of production if it is a "foregone conclusion" as to the existence, possession, and authenticity of the documents in question. This exception does not apply in a password disclosure case when the government compels pure testimony (a passcode) coming directly from the defendant. When the government seeks new information from the defendant to get access to the cell phone's contents, it does so to build a criminal case against that defendant. The government is not simply asking the defendant to produce known pre-existing documents, which was a crucial factor in *Fisher*.[74] Therefore, the act of production and the foregone conclusion exception are inapplicable in passcode disclosure cases.

In passcode production cases, the applicable law pertains to physical documents (i.e., the tax documents in *Fisher*). Forcing a defendant to produce physical documents is one thing. Granting the law enforcement or the prosecutor access to a person's smartphone is quite another. Given the wealth of information about a person and their activities that is contained within a handheld device, giving unfettered access to a cell phone could

72. *See* Doe v. United States, 487 U.S. 201, 219 (1988) (Stevens, J., dissenting).

73. *Id.*

74. Brief of Laurent Sacharoff, Professor of Law at the University of Arkansas, As Amicus Curiae In Support of Petition for Certiorari at 12, Andrews v. New Jersey, 141 S. Ct. 2623 (2021) (No. 20-937).

easily lead to the discovery of material evidence that far exceeds the scope of a search warrant. This will lead to law enforcement conducting fishing expeditions while violating an individual's privacy rights. Moreover, a court order compelling a defendant to produce his past tax returns cannot be reasonably compared to an order to disclose his smartphone passcode so that law enforcement can rummage through its contents—texts, emails, call logs, GPS history, perhaps even access to an application that provides access to 10 years' worth of tax return documents. Does the plain view doctrine come into play here (which allows officers to seize evidence found in plain view of where they are allowed to be)?[75] If police stumble upon evidence of criminal activity that has nothing to do with the original investigation or the scope of the warrant, can they use this evidence to file new charges against the defendant? Do we believe or even expect police to not go beyond their search parameters and who would monitor this process to prevent violations?

Some courts may attempt to limit the scope of the warrant to specific evidence such as text messages or photographs. However, the government still receives substantially more information than it would in a regular case involving the request for production of physical documents. For police to retrieve the information they seek from a cell phone, they will certainly have to sift through huge volumes of text messages, images, or other data. This likely scenario is patently unfair to a criminal defendant.

B. How Cell Phone Passcodes Should Be Handled

As discussed above, the courts have handled cases involving compelled disclosure of cell phone passwords differently. Many courts seek to analyze such cases using obscure and outdated doctrines, such as the foregone conclusion exception. Some courts focus their foregone conclusion analysis on the passcode itself, while others focus on the evidence on the device, which is what the government wants. None of the rulings are straightforward, most likely because the doctrine is fact-specific and intended solely for the production of physical documents, not for access to digital devices such as cell phones. Courts have attempted to fit a round peg in a square hole. Sadly, what we are left with is a dramatic split amongst lower courts.[76] Depending on the jurisdiction in which a person resides, this fact alone may determine their constitutional right of whether they must disclose

75. *See* Coolidge v. New Hampshire, 403 U.S. 443, 472 (1971).

76. Robert J. Anello & Richard F. Albert, *Hey SIRI, Does the Fifth Amendment Protect My Passcode?*, N.Y.L.J. (June 9, 2021, 12:30 PM), https://www.law.com/newyorklawjournal/2021/06/09/hey-siri-does-the-fifth-amendment-protect-my-passcode/ [https://perma.cc/BL2J-9K8W].

a passcode or not. To ensure uniformity, courts must not overcomplicate the issue. Since prosecutors and law enforcement are seeking evidence that is compelled, incriminating, and testimonial, the Fifth Amendment clearly affords an individual protection from this type of government overreach and a suspect cannot be compelled to furnish evidence that can be used against him in a criminal prosecution.

The burden must remain with the government to keep up with technological advances when executing search warrants. The government's inability to gather independent evidence is insufficient to justify the trampling of constitutional rights. Whether or not the government has the potential to break into a locked phone is unknown and remains in flux. The challenge here is the attempting to define constitutional protections in today's technologically advanced society. The government's objectives must be balanced with individual privacy and liberty. This is not a simple task, especially without clear guidance from the Supreme Court. However, when in doubt, judicial interpretation must err on the side of protecting an individual's constitutional rights.

IV. CONCLUSION

It is of the utmost importance to allow law enforcement and prosecutors to effectively investigate and prosecute crimes. Hindering their efforts to do their job would effectively impede the administration of justice. However, this interest must be balanced against the equally important individual rights. While certainly not as easy undertaking, courts cannot justify stretching outdated law to the point of absurdity and clear lines must be drawn. This is especially true in cases involving cell phone password disclosure, where some lower courts have significantly been restricting individual constitutional rights. Law enforcement and prosecutors have alternatives besides violating constitution rights. If the state wants a defendant's email correspondence, it can subpoena Google. If it wants a defendant's call log, it can subpoena Verizon. Unless the Supreme Court states otherwise, the existing case law should be properly followed. The Fifth Amendment protects individuals from being compelled to provide the government with incriminating testimonial evidence that could assist in their criminal prosecution. Therefore, no individual should be compelled to disclose the passcode to their cell phone. The burden is on the government to keep up or develop new technology to execute their search warrants. The convenience of government investigations should not come at the cost of eroding constitutional rights and liberties.