PROTECTING THE FIFTH AMENDMENT: COMPELLED DECRYPTION IN INDIANA

EVAN KENNEDY*

INTRODUCTION

Is there anything containing more incriminating evidence than your cell phone? Generally, no.[1] Cell phones have numerous capabilities and could "easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[2] Even greater, modern cell phones contain thousands of texts, hundreds of pictures and videos, internet browsing history, a calendar, and so on.[3]

With this in mind, the issue becomes whether the Fifth Amendment privilege against self-incrimination protects criminal defendants from court orders requiring them to unlock their cell phones.[4] Potential constitutional problems arise when a court orders a criminal defendant to provide his or her passcode in an investigation.[5] One view is that the defendant, by providing his passcode, only implicitly testifies that "I know the password."[6] A differing perspective is that entering the passcode communicates: "Everything on the phone exists to my knowledge, is authentic, and in my control."[7] Adopting the latter leads to a self-incrimination violation.[8] The former, however, approves of the government forcing a defendant to unlock his phone and obtaining access to all files on the phone via the foregone conclusion doctrine.[9]

The Fifth Amendment's Self-Incrimination Clause states that no person "shall be compelled in any criminal case to be a witness against himself."[10] Taking the stand is the traditional mechanism triggering the Self-Incrimination Clause; nevertheless:

> the act of producing subpoenaed documents may have a compelled testimonial aspect. That act, as well as a custodian's compelled testimony about whether he has produced everything demanded, may certainly communicate information about the documents' existence, custody, and

---

* J.D. Candidate, 2021, Indiana University Robert H. McKinney School of Law; B.S. 2018, Purdue University – West Lafayette, Indiana.

1. Riley v. California, 573 U.S. 373, 393-94 (2014).
2. *Id.* at 393.
3. *Id.*
4. *See generally* Commonwealth v. Jones, 117 N.E.3d 702, 707-08 (Mass. 2019); *see also* Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767, 769-71 (2019).
5. Seo v. State, 148 N.E.3d 952, 954-56 (Ind. 2020).
6. Kerr, *supra* note 4, at 779.
7. *See id.* at 774-75; *see also* Fisher v. United States, 425 U.S. 391, 410-12 (1976).
8. United States v. Hubbell, 530 U.S. 27, 45 (2000).
9. *See Jones*, 117 N.E.3d at 711.
10. U.S. CONST. amend. V.

> authenticity. It is also well settled that compelled testimony communicating information that may lead to incriminating evidence is privileged even if the information itself is not inculpatory.[11]

Indiana's Self-Incrimination Clause provides that "[n]o person, in any criminal prosecution, shall be compelled to testify against himself."[12] Similar to its federal counterpart, the Indiana Supreme Court addressed the act of production, stating that it is "well settled in criminal cases, that the court cannot compel the defendant to produce an instrument in writing, in his possession, to be used in evidence against him, as to do so would be to compel the defendant to furnish evidence against himself, which the law prohibits."[13] While nearly identical, "[t]he federal constitution establishes rights that the states may choose to expand."[14] Thus, the Fifth Amendment's Self-Incrimination Clause establishes the floor of protections for defendants.[15] But Article 1, Section 14 of the Indiana Constitution allows for the expansion of protections.[16]

On June 23, 2020, the Indiana Supreme Court issued a landmark decision, ultimately holding that the government must know—not merely infer—that the evidence it seeks exists on a defendant's smartphone, is under his or her control, and is authentic in order to overcome the Fifth Amendment protection.[17] Particularly, the government cannot compel a suspect to enter their passcode merely by showing that the defendant knows the passcode to the phone.[18] In rejecting that line of thinking, the Indiana Supreme Court noted that law enforcement could simply fish for "incriminating evidence," that is, "scour the device for incriminating information."[19] Put differently, the foregone conclusion exception applies only when the government shows, with sufficient particularity, the documents or files it seeks.[20] This is the proper scope of the protection provided by the Self-Incrimination Clause. Even more, the Indiana Supreme Court expressed concerns with extending the foregone conclusion exception to the compelled production of an unlocked smartphone.[21]

Meanwhile, the Massachusetts Supreme Court paved a simpler route for the government by holding that the defendant must unlock his cell phone if the prosecution can establish the defendant's knowledge of the passcode beyond a

---

11. *Hubbell*, 530 U.S. at 28.

12. IND. CONST. art. 1, § 14.

13. Sprague v. State, 181 N.E. 507, 510 (Ind. 1932) (quoting McGinnis v. State, 24 Ind. 500, 503 (1865)).

14. Edwards v. State, 902 N.E.2d 821, 829 (Ind. 2009).

15. *See* Ajabu v. State, 693 N.E.2d 921, 932 (Ind. 1998).

16. *Id.*

17. Seo v. State, 148 N.E.3d 952, 957-58 (Ind. 2020).

18. *Id.* at 958.

19. *Id.*

20. *Id.*

21. *Id.* at 958-62.

reasonable doubt.[22] This case provided the government access to a defendant's decrypted cell phone with a minimal showing that the defendant knew the passcode, thereby allowing access to all files on the cell phone.[23] Further, the opinion acknowledged that other witnesses knew the passcode, yet failed to hold that the government should explore those options before compelling a criminal defendant to unlock his cell phone.[24]

This Note argues that the foregone conclusion exception to the act-of-production doctrine should only apply to the files or documents on the phone, and not to the testimonial aspect of knowing the phone's passcode. In other words, the government needs to show with reasonable particularity the files sought rather than merely showing that the defendant knows the passcode to the phone. Providing otherwise would swallow up any Fifth Amendment protections against self-incrimination. This Note further argues that the Indiana Supreme Court adopted the proper framework in *Seo v. State*, despite the inevitability of the United States Supreme Court weighing in. If and when the highest court issues a decision in the compelled decryption realm, the Indiana Constitution can nevertheless provide a higher ceiling of protections beyond the Fifth Amendment. That is, if the United States Supreme Court adopts the *Commonwealth v. Jones* framework—where the government satisfies the foregone conclusion exception by proving the defendant knows the passcode.[25]

The Fourth Amendment analysis is beyond the scope of this Note. The Fourth Amendment protects "[t]he rights of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, ... and particularly describing the place to be searched, and the persons or things to be seized."[26] It is important to keep the Fourth and Fifth Amendments separate, as conflating the two in this situation would swallow up any Fifth Amendment protections with the evolution of technology.

Part I of the Note explains encryption and decryption. This Part compares the readability of cell phone data when the phone is locked and unlocked. Part II examines where federal law currently stands. This Part explains the act-of-production doctrine and foregone conclusion exception and analyzes precedent in light of technological advances. Part III explores both sides of the coin—that is, both arguments in this arena. Part IV explains Indiana's groundbreaking decision in *Seo v. State*. This Part provides a thorough explanation of the facts, holding, and ramifications of this decision. Part V explains how and why Indiana got it right and provides the suggested framework when a criminal defendant receives a court order to unlock his phone. Lastly, this Part explores additional protections under the Indiana Constitution for if and when the United States

---

22. Commonwealth v. Jones, 117 N.E.3d 702, 717-18 (Mass. 2019) (noting that "proof of ownership or exclusive control of the LG phone would certainly further support the Commonwealth's argument").

23. *Id.*

24. *Id.* at 717.

25. *See id.* at 717-18.

26. U.S. CONST. amend. IV.

Supreme Court weighs in.

I. OVERVIEW OF ENCRYPTION AND DECRYPTION

In the United States, 77% of citizens are smartphone users.[27] On average, people check their phones 150 times a day, send 763 texts per month, and have possession of these devices 16 hours a day.[28] Cell phones are "minicomputers" that also have the capacity to be used as telephones.[29] These store our photos, texts, where we've been, emails, contacts, and financial information.[30] Because of the immense storage capacity, cell phones require more protection from intrusion than other property.[31]

Yet some may ask, "Why not have Apple write software that decrypts phones in certain situations?"[32] Security experts assert that "personal and financial data" will "gradually become more accessible to hackers based both in the United States and abroad."[33] However, if these companies cannot be compelled to undercut encryption, clues in some criminal investigations may never be discovered.[34]

On the other hand, the "storage capacity of cell phones has several interrelated consequences for privacy."[35] First, cell phones accumulate a wealth of unique information, such as personal notes, bank statements, videos, and addresses, which "reveal much more in combination than any isolated record."[36] Second, a cell phone paints a picture of a person's life.[37] For example, cell phone photos include "dates, locations, and descriptions; the same cannot be said of a photograph . . . of loved ones tucked into a wallet."[38] Additionally:

> an element of pervasiveness . . . characterizes cell phones but not

---

27. *How Many Phones are in the World?*, BANKMYCELL, https://www.bankmycell.com/blog/how-ma ny-phones-are-in-the-world (last visited Mar. 4, 2021) [https://perma.cc/U2GW-LSWP].

28. *8 Surprising Cell Phone Statistics*, MOBILE COACH, https://mobilecoach.com/8-surprising-cell-phone-statistics/ (last visited Mar. 4, 2021) [https://perma.cc/YS3U-95XB].

29. Riley v. California, 573 U.S. 373, 393 (2014).

30. Erik Sofge, *What Personal Data Stays on a Phone?*, CONSUMER REPS. (Mar. 23, 2016), https://www.consumerreports.org/cell-phones-services/what-personal-data-stays-on-your-phone-[https://perma.cc/BS8E-WGW6].

31. *Riley*, 573 U.S. at 393-94.

32. *See* Alina Selyukh, *A Year After San Bernardino and Apple-FBI, Where Are We on Encryption?*, NPR (Dec. 3, 2016), https://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption [https://perma.cc/4L5C-JMHD].

33. Sofge, *supra* note 30.

34. *Id.*

35. *Riley*, 573 U.S. at 394.

36. *Id.*

37. *Id.*

38. *Id.*

> physical records. Prior to the digital age, people did not . . . carry . . . sensitive personal information with them [throughout the] day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception.[39]

The tension between personal privacy and liberty versus the government's interest in crime detection and public safety underlies the compelled decryption problem.

Device encryption scrambles stored data to make it unreadable to others.[40] The process of encryption converts personal data from "normal message ([P]laintext) into meaningless message (Ciphertext)."[41] When a smartphone is locked, the device is encrypted.[42] The only way to make the data readable is by putting in your passcode—known as decryption.[43] The process of decryption converts the personal data from the "meaningless message (Ciphertext) into its original form (Plaintext)."[44] The data in encrypted form is "an unintelligible kind that's undecipherable unless decrypted."[45] Effectively, a passcode is the decryption key to unlock the data and make it readable and accessible.[46]

Additionally, encryption is essential to personal privacy: if your data is not encrypted, anyone who happens across your phone or laptop can gain access to readable data.[47] This includes a wealth of information: contacts, browsing history, text messages, call history, photos, etc.[48] Additionally, encryption prevents hackers from stealing a user's information and locks the smartphone after numerous failed attempts entering a passcode.[49]

Androids and iPhones, by default, encrypt data when a phone is passcode-protected.[50] Smartphone companies do not provide a "backdoor" for law

---

39. *Id.* at 395.

40. Mike Brown, *Here's How Cell Phone Encryption Works*, INVERSE (Nov. 23, 2017), https://www.inverse.com/article/38639-cell-phone-encryption-how-it-works [https://perma.cc/EZ3K-9KEB].

41. *Difference Between Encryption and Decryption*, GEEKSFORGEEKS (Mar. 31, 2020), https://www.geeksforgeeks.org/difference-between-encryption-and-decryption/ [https://perma.cc/292T-UWBH].

42. Brown, *supra* note 40.

43. *Id.*

44. *Difference Between Encryption and Decryption*, *supra* note 41.

45. *Id.*

46. Michael Price & Zach Simonetti, *Defending Device Decryption Cases*, CHAMPION, July 2019, at 42, 42-43.

47. David Nield, *Why You Should Be Encrypting Your Devices and How to Easily Do It*, GIZMODO (Sept. 4, 2017), https://gizmodo.com/why-you-should-be-encrypting-your-devices-and-how-to-ea-1798698901 [https://perma.cc/VVD5-8WHQ].

48. *Id.*

49. Brown, *supra* note 40.

50. *How to: Encrypt Your iPhone*, SURVEILLANCE SELF-DEF. (Mar. 26, 2018), https://ssd.eff.org/en/module/how-encrypt-your-iphone [https://perma.cc/QQH8-JSM8].

enforcement; if the phone is locked, gaining access requires entering the passcode.[51] However, nothing prevents the government from decrypting through third-parties—the phone company itself, a witness who may know the passcode, etc.[52] Compelled decryption raises questions about whether providing a passcode—producing a decrypted cell phone—violates the Fifth Amendment privilege against self-incrimination.[53]

II. WHERE FEDERAL LAW STANDS

A. The Fifth Amendment to the U.S. Constitution

The Fifth Amendment to the U.S. Constitution states that no person "shall be compelled in any criminal case to be a witness against himself."[54] Its purpose is to protect the accused "from having to reveal, directly or indirectly, his knowledge of facts relating him to the offense or from having to share his thoughts and beliefs with the Government."[55] The Supreme Court recognized that "the Amendment must be accorded *liberal construction* in favor of the right it was intended to secure"—namely, the protection against self-incrimination.[56]

The self-incrimination privilege to the Fifth Amendment requires that a communication be (1) incriminating, (2) compelled, and (3) testimonial.[57] A defendant satisfies the incrimination prong by "[p]roviding information that is inculpatory, or that could lead to the discovery of inculpatory evidence."[58] A defendant satisfies the compelled prong when a court order, warrant, or subpoena requires involuntary compliance.[59] Thus, compelled decryption fulfills the incrimination and compulsion prongs because the government generally obtains a search warrant or subpoena ordering the defendant to produce a decrypted phone (compulsion), which could lead to the discovery of inculpatory evidence (incriminating).[60]

When a criminal defendant must unlock a smartphone, the "testimonial" prong is at issue. Testimonial is "the attempt to force [the defendant] to disclose the contents of his own mind that implicates the Self-Incrimination Clause."[61]

---

51. Brown, *supra* note 40.

52. *Id.*

53. Nathaniel Sobel, *The Massachusetts High Court Rules That State Can Compel Password Decryption in* Commonwealth v. Jones, LAWFARE (Apr. 24, 2019), https:// www. lawfareblog.com/ massachusetts-high-court-rules-state-can-compel-password-decryption-commonwealth-v-jones [https://perma.cc/TRR5-SYKW].

54. U.S. CONST. amend. V.

55. Doe v. United States, 487 U.S. 201, 213 (1988).

56. Hoffman v. United States, 341 U.S. 479, 486 (1951) (emphasis added).

57. United States v. Hubbell, 530 U.S. 27, 34-38 (2000).

58. Price & Simonetti, *supra* note 46, at 43.

59. *See In re* Search of [Redacted] Wash., D.C., 317 F. Supp. 3d 523, 534 (D.D.C. 2018).

60. Price & Simonetti, *supra* note 46, at 43.

61. Doe v. United States, 487 U.S. 201, 211 (1988) (quoting Curcio v. United States, 354

However, the Supreme Court unclearly defined the difference between testimonial and non-testimonial: being forced to surrender a key to a strongbox containing incriminating documents does not constitute "testimonial," but revealing the combination to a wall safe does.[62] While this analogy does not provide a clear cut answer, it does lay the foundation for a Fifth Amendment analysis.[63]

In 1966, the Supreme Court provided a clear illustration of a nontestimonial act. In *Schmerber v. California*, a criminal defendant raised his Fifth Amendment privilege against self-incrimination concerning the introduction of his blood sample as evidence to prove that he was drinking and driving.[64] The Court held that blood sampling evidence, like fingerprints, photographs, or measurements, did not violate the Fifth Amendment because the privilege "is a bar against compelling 'communications' or 'testimony,' but that compulsion which makes a suspect or accused the source of 'real or physical evidence' does not violate it."[65] So, the Court held that providing a blood sample did not require that the defendant communicate certain facts, otherwise not obtainable, to the government.[66]

Nevertheless, giving in-court testimony is not the only way to satisfy the testimonial prong. Producing documents implicitly relays facts that can give rise to the self-incrimination protection.[67] Notably, the "Cyber Age has vast potential both to expand and restrict individual freedoms in dimensions not contemplated in earlier times."[68] The Supreme Court acknowledged the vast potential of modern technology in shaping how people think and express themselves, which requires courts to be conscious of their rulings today, as those rulings might be obsolete tomorrow.[69]

B. The Act of Production & Foregone Conclusion Doctrines

The traditional thought is that the Fifth Amendment privilege against self-incrimination applies to oral testimony; however, a defendant's compelled action may satisfy the testimonial prong.[70] The act-of-production doctrine is a branch of the Fifth Amendment privilege that applies to the compelled production of

---

U.S. 118, 128 (1957)) (internal quotation marks omitted).

62. *Id.* at 210 n.9.

63. *Id.*

64. Schmerber v. California, 384 U.S. 757, 758-59 (1966).

65. *Id.* at 764; *see also* United States v. Patane, 542 U.S. 630, 638 (2004) (noting that "[t]he Fifth Amendment prohibits use by the prosecution in its case in chief only of *compelled* testimony" (quoting Oregon v. Elstad, 470 U.S. 298, 306-07 (1985) (emphasis in original))).

66. *Schmerber*, 384 U.S. at 761.

67. *See* United States v. Hubbell, 530 U.S. 27, 33 (2000).

68. Carpenter v. United States, 138 S. Ct. 2206, 2224 (2018) (Kennedy, J., dissenting).

69. Packingham v. North Carolina, 137 S. Ct. 1730, 1736 (2017).

70. *See Hubbell*, 530 U.S. at 33.

documents by a defendant.[71] Cases succinctly point out that "the very act of producing documents in response to a subpoena may have a compelled testimonial aspect in and of itself."[72] Also, "[t]he 'compelled testimony' that is relevant . . . is not to be found in the *contents* of the documents produced in response to the subpoena."[73] Instead, "the testimony *inherent in the act of producing those documents*" governs the analysis.[74]

It is important to conceptually understand what the Fifth Amendment protects and when the act-of-production doctrine applies:

> while the *contents* of pre-existing documents are never subject to a claim of Fifth Amendment privilege (because their creation was not "compelled"), the compelled act of *producing* them in response to a subpoena . . . can itself be testimonial on the . . . existence, his possession, and the authenticity of the documents or other materials that the subpoena calls for, as well as the respondent's belief that the documents he would be producing are responsive to the subpoena.[75]

In other words, the Fifth Amendment does not protect the words on the document or the content of the files. Instead, it protects a suspect from producing the documents and files, which implicitly communicates that the files exist, the files are authentic, and the files are in the control and custody of the defendant.[76]

The fact that producing records implicitly communicates information does not end the analysis. The foregone conclusion doctrine is an exception to the act-of-production doctrine.[77] So, "when any potentially testimonial component of the act of production—such as the existence, custody, and authenticity of evidence—is a 'foregone conclusion' that 'adds little or nothing to the sum total of the Government's information,'" the Fifth Amendment protection against self-incrimination does not apply.[78] But, the foregone conclusion doctrine only applies when the government can show with reasonable particularity that it knows of the materials, making any testimonial aspect in the act of production a *foregone conclusion* adding little prosecutorial value.[79] Thus, the government proving the exact files it seeks will bar Fifth Amendment protections because the government already knows of their existence and is not relying on the defendant to use his

---

71. James G. Thomas, *The Act of Production Doctrine*, NEAL & HARWELL, PLC (Feb. 14, 2017), https://www.nealharwell.com/the-act-of-production-doctrine/ [https://perma.cc/RE3F-6HSE].

72. Commonwealth v. Davis, 220 A.3d 534, 546 (Pa. 2019); *see also Hubbell*, 530 U.S. at 40.

73. *Hubbell*, 530 U.S. at 40 (emphasis added).

74. *Id.* (emphasis added).

75. Thomas, *supra* note 71.

76. Fisher v. United States, 425 U.S. 391, 410-12 (1976).

77. United States v. Apple Mac Pro Comput., 851 F.3d 238, 247 (3d Cir. 2017).

78. *Id.* (quoting *Fisher*, 425 U.S. at 411).

79. *In re* Grand Jury Subpoena Duces Tecum, 670 F.3d 1335, 1345-46 (11th Cir. 2012).

mental processes to produce otherwise unobtainable information.[80]

Two seminal cases apply the act-of-production and foregone conclusion doctrines. The first is *Fisher v. United States*. There, the Court ordered a defendant's attorney to produce the defendant's tax records.[81] The defendant asserted his Fifth Amendment privilege against self-incrimination because the documents belonged to him.[82] The Court held that the documents were not "compelled" because the documents were in the lawyer's possession.[83] In order for the privilege to exist, the Court reasoned, the compulsion must be directed at the defendant, not a third party.[84] However, the Court stated that "[t]he 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."[85]

That is, producing tax records implicitly communicates that: (1) the documents *existed*; (2) the documents were in his *possession or control*; and (3) the documents were *authentic*.[86] In particular, "[w]hether the constitutional privilege protects the answers to such questions, or protects the act of production itself, is a question that is distinct from the question whether the unprotected contents of the documents themselves are incriminating."[87] The Court in *Fisher* explained that the defendant's implicit admission to the existence and possession of the documents through third-party production does not rise to the level of testimony within the protection of the Fifth Amendment.[88]

In *Fisher*, even if the taxpayer (and not the attorney) was the one to respond to the subpoena, the act of production would not be testimonial because the existence and location of the documents were a "foregone conclusion," and the testimony added "little or nothing to the sum total of the Government's information by conceding that he in fact ha[d] the papers."[89] The government knew that these tax documents existed through the accountants who created them.[90] If the government, for example, had not been able to point to the exact documents sought and instead just subpoenaed all relevant documents in the defendant's possession, then the foregone conclusion doctrine would not apply.[91] The defendant in that situation would have to use his mental processes in determining whether the documents were relevant, and by producing them, would

---

80. *See* United States v. Hubbell, 530 U.S. 27, 42 (2000).
81. *Fisher*, 425 U.S. at 394.
82. *Id.* at 395-96.
83. *Id.* at 397.
84. *Id.* at 396-97.
85. *Id.* at 410.
86. *Id.* at 410-12.
87. United States v. Hubbell, 530 U.S. 27, 37 (2000).
88. *Fisher*, 425 U.S. at 411-12.
89. *Id.* at 411.
90. *Id.* at 411-13.
91. *See Hubbell*, 530 U.S. at 44-45.

implicitly testify that the records in fact existed, were in his possession, and were authentic.[92]

The Supreme Court again applied the act-of-production doctrine to business records in 2000. In *United States v. Hubbell*, the defendant, Hubbell, received a subpoena to produce business records from eleven broad categories.[93] Hubbell invoked his Fifth Amendment right against self-incrimination but instead received immunity "to the extent allowed by law."[94] Hubbell then produced over 13,000 pages of documents, followed by an indictment, even after he was granted immunity.[95]

The Court held that the compelled act of production provided the necessary linkage for the indictment.[96] Producing the documents proved their existence, authenticity, and custody.[97] The fact that the government did not intend to use the documents as evidence at criminal trial did not matter; the "derivative use" of the testimonial aspect to get an indictment, even after granting immunity, violated the Fifth Amendment.[98]

The Court in *Hubbell* further explained that the foregone conclusion doctrine did not apply because the government could not meet the "reasonable particularity standard."[99] For the foregone conclusion doctrine to apply, the government must show with "reasonable particularity" the documents it seeks.[100] Unlike in *Fisher*, where the government knew that the documents were in the attorney's possession and could independently confirm their existence and authenticity through the accountant, the government in *Hubbell* did not show that it had prior knowledge about the existence or whereabouts regarding the 13,120 pages of documents.[101] Complying with the subpoena would require the suspect to take mental and physical steps to provide the prosecution with many sources of potentially incriminating evidence.[102] Thus, the defendant would have to use his mental capacity to produce these documents, which invariably communicates facts to the government that are not otherwise known.[103]

In sum, "*Hubbell* stands for the proposition that the government cannot prosecute an individual based on evidence obtained by means of a 'fishing expedition' subpoena duces tecum, even when the individual's act of production has been fully immunized."[104] To the contrary, the defendant's possession of the

---

92. *See generally id*.
93. *Id*. at 42.
94. *Id*. at 38.
95. *Id*. at 41-43.
96. *Id*. at 42.
97. *Id*. at 41.
98. *Id*.
99. *Id*. at 30.
100. *Id*. at 28.
101. *Id*. at 33.
102. *Id*. at 42.
103. *Id*. at 42-43.
104. Thomas, *supra* note 71.

specific documents must be a "foregone conclusion."[105]

III. BOTH SIDES OF THE COIN: DOES THE FOREGONE CONCLUSION DOCTRINE APPLY TO THE ACT OF PUTTING IN THE PASSCODE OR THE FILES IN WHICH THE GOVERNMENT SEEKS?

One way to think about compelled decryption is to imagine requiring a witness to take the stand and translate a secret language into English.[106] While one can argue that physically taking the stand and translating a language is unlike unlocking a cell phone,[107] does it not produce the same result? Both require using mental processes to relay facts that are unknown to the prosecution. Both take unreadable, undecipherable data and make it understandable for the prosecution.[108] Producing a key, on the other hand, does not require the same mental process that makes entering a passcode a testimonial act.[109] This is the same distinction *Doe v. United States* (*Doe II*) made with the key and a wall safe.[110]

Virtually all commentators agree that providing a passcode—or providing a decrypted smartphone—is testimonial. As evidence that unlocking something is testimonial, in *United States v. Green*, the Fifth Circuit held that the act of a criminal defendant opening combination locks to briefcases and a safe was testimonial in nature.[111] The "compelled acts disclosed [defendant's] knowledge of the presence of firearms in these cases and of the means of opening these cases."[112] The act of producing a password requires more mental process than producing the blood samples in *Schmerber*.[113] Knowing that the act-of-production doctrine applies, the next step in the analysis becomes whether the foregone conclusion exception applies—whether the specificity of the government's knowledge extends to (A) the testimonial act of entering the passcode,[114] or (B) the actual files and documents the government seeks.[115]

Effectively, the analysis boils down to the facts conveyed by entering the passcode: (1) only that the person knows the passcode, or (2) implicit testimony about the possession, authenticity, and custody of the files on the phone. More simply, is compelled decryption the digital equivalent of turning over the key or giving a combination to a safe as depicted in *Doe II*?

---

105. *Id.*

106. Kerr, *supra* note 4, at 782.

107. *Id.*

108. *Difference Between Encryption and Decryption*, *supra* note 41.

109. Doe v. United States, 487 U.S. 201, 202, 209-10 n.9 (1988).

110. *Id.*

111. United States v. Green, 272 F.3d 748, 753-54 (5th Cir. 2001); *see also* United States v. Kirschner, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010).

112. *Green*, 272 F.3d at 753.

113. *See supra* Section II.A.

114. *See generally* Commonwealth v. Jones, 117 N.E.3d 702 (Mass. 2019).

115. *See generally* Seo v. State, 148 N.E.3d 952 (Ind. 2020).

A. The Foregone Conclusion Exception Applies to the Testimonial Aspect of Putting in the Passcode

One side of the argument believes that entering a passcode relays minimal information: the only fact conveyed by entering numbers to open the phone is "I know the password" and can therefore access the device.[116] The premise is that "[b]ecause the password is entered without revealing it to the government, any communicative content that its characters might contain (such as a hypothetical passcode, 'ISELLDRUGS')" would not be revealed to the government.[117] Massachusetts adopted this view, arguably eliminating any Fifth Amendment protections in compelled decryption cases.[118] In *Commonwealth v. Jones*, the lower court ordered the defendant, against his assertion of Fifth Amendment protections, to unlock a cell phone obtained in a sex trafficking investigation.[119] The prosecutor argued that compelling a defendant to enter the passcode did not force him to incriminate himself; the act of putting in the passcode would not reveal any information the State did not already know—i.e., proof that the cell phone belonged to the defendant.[120]

The Massachusetts Supreme Court held that the foregone conclusion exception applied to the passcode itself.[121] The Commonwealth was "only required to establish the defendant's knowledge of the password beyond a reasonable doubt" [standard of proof under Massachusetts's constitution]—and not even exclusive control of the cell phone—to compel a defendant to enter a passcode and produce a decrypted device.[122] The court adopted the view that the only fact implicitly testified by entering a passcode is "I know the password"; therefore, the foregone conclusion exception applies when the government shows the individual knows the passcode because such information "adds little or nothing to the sum total of the Government's information."[123] Put differently, any Fifth Amendment protections are eliminated in Massachusetts when the government satisfies the minor obstacle of proving that the suspect knows the passcode—which may be established by showing that the smartphone belongs to him or that he simply had possession of the phone.[124]

The Third Circuit applied the foregone conclusion doctrine to producing decrypted hard drives. In *United States v. Apple Mac Pro Computer*, a defendant

---

116. *Jones*, 117 N.E.3d at 710.

117. Kerr, *supra* note 4, at 779 (footnote omitted).

118. *See Jones*, 117 N.E.3d at 717-18.

119. *Id.* at 702-04.

120. *Id.* at 708.

121. *Id.* at 710.

122. *Id.* at 717.

123. *Id.* at 710 (quoting Fisher v. United States, 425 U.S. 391, 411 (1976)).

124. *Id.* at 717-18 (noting that proof of ownership or exclusive control of the phone would further support the argument that the defendant knows the passcode).

was charged with possession of child pornography.[125] The defendant voluntarily unlocked his iPhone but would not decrypt his external hard drives, which the government believed to contain the child pornography.[126] The defendant was held in civil contempt until he complied with the court order.[127]

The court held that any testimonial aspects relayed by producing a decrypted hard drive were a foregone conclusion.[128] The government provided evidence that the files existed, and that the defendant could decrypt the hard drives.[129] The government also proved the files existed via affidavits from forensic analysts and because the cell phone had 2,015 videos and photographs.[130] Thus, the court found that any testimonial aspect in producing the decrypted device added little or nothing to the information already obtained by the government.[131]

Significantly, the evidence provided in *Apple*, unlike in *Jones*, showed that the government had a strong foundation in its belief that the hard drive contained incriminating evidence.[132] While the court in *Apple* held that the defendant had to produce a decrypted hard drive because the government showed he had the capability to do so (applying the *Jones* framework), at least substantial evidence corroborated the prosecution's belief that the hard drive contained the incriminating evidence.[133] Arguably, the government still could have satisfied the proper foregone conclusion analysis.[134]

Regardless, proponents of this view believe that the Fourth Amendment governs the particularity requirement that the government must satisfy before searching for evidence.[135] However, if the Fourth Amendment governs the particularity requirement, what Fifth Amendment protections would remain?

B. Foregone Conclusion Exception Applies to the Documents the Government Seeks

The more accurate view is that entering a passcode implicitly relays facts about the authenticity, custody, and existence of the files and documents on the cell phone. This is the proper approach that aligns with precedent and the fundamental right guaranteed to criminal defendants by the Fifth Amendment: the privilege against self-incrimination.[136]

The Supreme Court has applied the foregone conclusion doctrine once—only

---

125. United States v. Apple Mac Pro Comput., 851 F.3d 238, 242 (3d Cir. 2017).
126. *Id.* at 242.
127. *Id.* at 242-43.
128. *Id.* at 248.
129. *Id.* at 249.
130. *Id.* at 248.
131. *Id.*
132. *Id.* at 247-48.
133. *Id.* at 248.
134. *See infra* Part V.
135. Kerr, *supra* note 4, at 787-88.
136. United States v. Verdugo-Urquidez, 494 U.S. 259, 264 (1990).

in *Fisher v. United States*.[137] The Court originally created this doctrine to protect criminal defendants from producing business documents.[138] Expanding this exception goes beyond precedent, against its purpose, and would swallow up the Fifth Amendment because courts would solely rely on the Fourth Amendment on evidentiary rulings.[139]

For instance, unlike in *Doe II* where the government ordered the defendant to sign a consent form to obtain foreign bank records,[140] ordering defendants to unlock a smartphone requires them to "disclose the contents of [their] mind."[141] Signing the bank disclosure form was more similar to "surrender[ing] a key to a strongbox" instead of "reveal[ing] the combination to [petitioner's] wall safe."[142] Producing a decrypted cell phone requires more mental processes and communicates far more than signing a consent form. Signing a consent form is much like producing a blood sample—both do not express any facts unknown to the government. But giving a passcode and producing an unlocked cellphone communicates loads of information and translates the data into readable evidence for law enforcement.[143]

Even more, the Eleventh Circuit found contrary to *Apple* on very similar facts, ordering the defendant in *In re Grand Jury Subpoena Duces Tecum* to decrypt a hard drive in a child pornography case.[144] The Eleventh Circuit held that "(1) [the defendant's] decryption and production of the contents of the drives would be testimonial, not merely a physical act; and (2) the explicit and implicit factual communications associated with the decryption and production are not foregone conclusions."[145] The opinion continued:

> this case is far closer to the *Hubbell* end of the spectrum than it is to the *Fisher* end.[146] As in *Hubbell*, "the Government has not shown that it had any prior knowledge of either the existence or the whereabouts of the [files]" that it seeks to compel Doe to produce."[147]

Courts and commentators remain split on the issue of how much information a defendant discloses by producing a decrypted device and whether the Fifth Amendment provides protection.

---

137. *See generally* Fisher v. United States, 425 U.S. 391, 411 (1976).

138. United States v. Hubbell, 530 U.S. 27, 44 (2000).

139. Oral Argument at 25:30, Seo v. State, 148 N.E.3d 952 (Ind. 2020), https://mycourts.in.gov/arguments/default.aspx?&id=2328&view=detail&yr=&when=&page=1&court=&search=Eunjoo&direction=%20ASC&future=True&sort=&judge=&county=&admin=False&pageSize=20 [https://perma.cc/BW4B-RU7P] .

140. Doe v. United States, 487 U.S. 201, 202, 205 (1988).

141. *See* Curcio v. United States, 354 U.S. 118, 128 (1957).

142. *Doe*, 487 U.S. at 210 n.9 (citation and internal quotation marks omitted).

143. *Difference Between Encryption and Decryption*, *supra* note 41.

144. *In re* Grand Jury Subpoena Duces Tecum, 670 F.3d 1335, 1339 (11th Cir. 2012).

145. *Id.* at 1346.

146. *Id.* at 1347.

147. *Id.* (quoting United States v. Hubbell, 530 U.S. 27, 45 (2000)).

Above all, the analysis needs to account for the fact that "[s]martphones are everywhere and contain everything."[148] They have become "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[149] Therefore, courts need to be reluctant in applying the foregone conclusion doctrine in light of technological advances.

IV. JUNE 23, 2020: WHERE INDIANA LAW STANDS

On August 21, 2018, the Indiana Court of Appeals held that the government must know, and not merely infer, that the evidence they seek exists on a defendant's cell phone, is under his control, and is authentic in order to overcome the Fifth Amendment protection.[150] However, the Indiana Supreme Court granted transfer on *Seo v. State*, vacating the opinion and leaving much uncertainty as to the protections criminal defendants have when faced with an order to unlock their cell phones.[151] Nevertheless, on June 23, 2020, Indiana's highest court issued a landmark decision with lasting impact, at least until the United States Supreme Court enters this realm.[152]

A. Background: Seo v. Indiana

Katelin Seo contacted the local sheriff's department to report that she had been sexually assaulted by D.S.[153] With Seo's consent, officers completed a forensic download of her iPhone and returned it.[154] After examining the content on her cell phone, officers shifted their focus from D.S. to Seo, believing that Seo harassed and stalked D.S. with spoofed calls and texts.[155] The ensuing investigations confirmed that belief, and Seo was arrested and charged with felony stalking.[156]

Subsequent to her arrest, Seo refused to unlock the iPhone.[157] So officers obtained two search warrants: one authorizing a forensic download of Seo's iPhone, and the other compelling Seo to unlock the cell phone.[158] Once again, Seo refused to unlock the iPhone—this time asserting her Fifth Amendment privilege.[159]

---

148. Seo v. State, 148 N.E.3d 952, 959 (Ind. 2020).

149. Riley v. California, 573 U.S. 373, 385 (2014).

150. *See* Seo v. State, 109 N.E.3d 418, 432, 433, 436 (Ind. Ct. App. 2018), *vacated*, 148 N.E.3d 952.

151. *Seo*, 148 N.E.3d at 954.

152. *See id.*

153. *Id.* at 953.

154. *Id.*

155. *Id.*

156. *Id.* at 953-54.

157. *Id.* at 954.

158. *Id.*

159. *Id.*

The trial court disagreed with Seo and held her in contempt, reasoning that "[t]he act of unlocking the phone does not rise to the level of testimonial self-incrimination."[160] But the Indiana Court of Appeals reversed, holding that Seo's act of using her passcode to unlock and decrypt the content on the phone was testimonial in nature and that the State did not satisfy its burden to prove that the foregone conclusion doctrine applied.[161] Indiana's highest court provided clarity.

B. Groundbreaking Holding

The Indiana Supreme Court faced two questions: First, does the act of producing an unlocked and decrypted smartphone rise to "testimonial" under the Fifth Amendment?[162] And second, if yes, does the foregone conclusion exception apply?[163]

Seo argued that being forced to unlock her iPhone for law enforcement essentially equates to Seo "assist[ing] in the prosecution of her own criminal case," therefore violating her Fifth Amendment right against self-incrimination.[164] The State asserted that "it already knows the implicit factual information Seo would convey by unlocking her iPhone—namely, that she knows the password and thus has control and use of the phone."[165]

1. Does Producing a Decrypted Smartphone Rise to "Testimonial" Under the Fifth Amendment?—The Indiana Supreme Court answered in the affirmative and held that forcing criminal defendants to unlock and decrypt their cell phones violates their Fifth Amendment right against self-incrimination.[166] The court explained that producing an unlocked cell phone "communicates to the State, at a minimum, that (1) the suspect knows the password; (2) the files on the device exist; and (3) the suspect possesses those files."[167] The breadth of factual information relayed by producing an unlocked cell phone triggers Fifth Amendment protection.[168] Otherwise, the compelled act will communicate information the State previously did not know—"precisely what the privilege against self-incrimination is designed to prevent."[169]

In reaching this conclusion, Indiana's highest court turned to the same federal precedent discussed in Part II.[170] First, the court analyzed *Fisher v. United States*—the case involving subpoenaing taxpayers' documents in their attorneys'

160. *Id.* (internal citation omitted).
161. Seo v. State, 109 N.E.3d 418, 436 (Ind. Ct. App. 2018), *vacated*, 148 N.E.3d 952.
162. *Seo*, 148 N.E.3d at 955-58.
163. *Id.* at 958.
164. *Id.* at 955.
165. *Id.* (internal quotation marks omitted).
166. *Id.*
167. *Id.*
168. *Id.*
169. *Id.* at 958 (citing Couch v. United States, 409 U.S. 322, 328 (1973)).
170. *See supra* Part II.

possession—which created the act-of-production doctrine.[171] Recall that the United States Supreme Court provided that producing documents in response to a subpoena can be testimonial if the act concedes the existence, possession, or authenticity of the documents ultimately produced.[172]

However, *Fisher* went on to hold that when the government can show that it already knows this information, then the testimonial aspects are a "foregone conclusion," and complying with the subpoena becomes a question "not of testimony but of surrender."[173] And, because the government proved the possession of the tax documents and their authenticity through the accountants who prepared them, the case did not implicate incriminating testimony.[174] Accordingly, the foregone conclusion exception applied—the first and only time it has been used by the Supreme Court.[175]

The *Seo* decision went on to analyze two other cases where the government failed to sufficiently show that the foregone conclusion doctrine applied.[176] First, in *United States v. Doe* (*Doe I*), a business owner refused to comply with five subpoenas to produce certain documents.[177] Second, in *Hubbell*, the defendant actually produced 13,120 documents in response to government subpoenas.[178] In both cases, the United States Supreme Court held that the government violated the defendants' Fifth Amendment privilege because the "physical act [of producing documents], nontestimonial in nature, cannot be 'entirely divorced from its "implicit" testimonial aspect.'"[179]

In sum, "the act of production doctrine links the physical act to the documents ultimately produced. And the foregone conclusion exception relies on this link by asking whether the government can show it already knows the documents exist, are in the suspect's possession, and are authentic."[180] Accordingly, a criminal defendant is protected vis-à-vis the Fifth Amendment from producing an unlocked cell phone with files that the government cannot independently verify.[181]

2. Does the Foregone Conclusion Exception Apply in Seo's Case?—Because the Indiana Supreme Court found that compelling Seo to unlock her iPhone would implicitly communicate facts to the State, the next inquiry involved whether the State met its burden in proving that the foregone conclusion exception applied: Did the State show that (1) Seo knew the passcode to her

---

171. *See* Fisher v. United States, 425 U.S. 391, 394-96 (1976).

172. *Id.* at 412-13.

173. *Id.* at 411 (quoting *In re* Harris, 211 U.S. 274, 279 (1911)).

174. *Id.* at 414.

175. *Id.* at 411; *see also* Seo v. State, 148 N.E.3d 952, 956 (Ind. 2020).

176. *Seo*, 148 N.E.3d at 956-57.

177. *See* United States v. Doe, 465 U.S. 605 (1984).

178. *See* United States v. Hubbell, 530 U.S. 27, 31 (2000).

179. *Seo*, 148 N.E.3d at 957 (quoting *Hubbell*, 530 U.S. at 43).

180. *Id.* (citing Laurent Sacharoff, *What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr*, 97 TEX. L. REV. 63, 68 (2019)).

181. *Id.* at 957-58.

iPhone; (2) the files on the device existed; and (3) she possessed those files?[182] The State needed to prove its knowledge of each of these facts to render Seo's communicative aspects nontestimonial.

Indiana's highest court rejected the State's argument that it could invoke the foregone conclusion exception by merely showing that Seo knew her passcode.[183] Why? Because forcing a criminal defendant under these circumstances would allow the State to "fish for incriminating evidence" without any knowledge of what was on the phone.[184] "[T]o hold otherwise would sound 'the death knell for a constitutional protection against compelled self-incrimination in the digital age.'"[185] The State also failed to show that the particular files existed and that Seo indeed possessed those files.[186]

3. Belt and Suspenders: Can the Foregone Conclusion Doctrine Ever Apply in the Compelled Decryption Context?—Ultimately, the Indiana Supreme Court noted that the foregone conclusion doctrine is a "narrow exception" that may be unsuitable in the compelled decryption context.[187]Although determining that the foregone conclusion doctrine did not apply in Seo's case, the court did not stop here. In a belt-and-suspenders approach, it provided a lengthy explanation that extending the foregone conclusion exception should likely never apply in compelled decryption cases for three separate reasons.[188]

First, the court reasoned that the foregone conclusion exception "fails to account for the unique ubiquity and capacity of smartphones."[189] In other words, *Fisher*, *Doe I*, and *Hubbell* could not have anticipated that smartphones would become so prevalent, so ubiquitous, and so advanced.[190] In fact, in 2019, 81% of Americans owned a smartphone—a dramatic increase from the mere 35% in 2011.[191] Even more compelling, in *Fisher*, *Doe I*, and *Hubbell*, the subpoena nevertheless limited the information implicated by the compelled production.[192] An unlocked smartphone, to the contrary, could not have the same limitation because of the breadth and depth of information the government could contain.[193] Therefore, analogizing with decade-old cases is inappropriate.[194]

Second, the court explained that the foregone conclusion exception "may

182. *Id.* at 958.

183. *Id.*

184. *Id.* at 962.

185. *Id.* (quoting Commonwealth v. Jones, 117 N.E.3d 702, 724 (Mass. 2019) (Lenk, J., concurring)).

186. *Id.*

187. *Id.*

188. *See id.* at 958-59.

189. *Id.* at 959.

190. *Id.*

191. *Id.*

192. *Id.*

193. *Id.* at 960.

194. *See id.*

prove unworkable" in the compelled decryption realm.[195] That is, smartphones contain the "combined footprint of what has been occurring socially, economically, personally, psychologically, spiritually and sometimes even sexually, in the owner's life."[196] As such, complications would arise barring the application of this exception. For instance, "if officers searching a suspect's smartphone encounter an application or website protected by another password, will they need a separate motion to compel the suspect to unlock that application or website?"[197] Or, equipped with this information, could officers then invoke the foregone conclusion doctrine?[198] Given the uncertainties, "it seems imprudent" to extend the foregone conclusion exception to smartphones.[199]

Lastly, the court elucidated that the foregone conclusion exception "runs counter to U.S. Supreme Court precedent."[200] Stated differently, "[t]he Supreme Court has hesitated to apply [other] doctrines to novel dilemmas."[201] For example, the Court in *Riley v. California* declined to extend the search-incident-to-arrest exception to a cell phone on an arrestee.[202] And in *Carpenter v. United States*, the Court determined that the third-party doctrine did not extend to cellular site location information.[203] What do these cases all have in common? Well, the Indiana Supreme Court and the United States Supreme Court crafted these exceptions in a vastly different context, much like the foregone conclusion doctrine.[204]

In sum, the Indiana Supreme Court correctly based its holding on one key fact: smartphones simply contain too much of our personal lives to enable the government free and total access.[205]

V. SUGGESTED FRAMEWORK TO PROTECT THE PRIVILEGE AGAINST SELF-INCRIMINATION

A. The Government Should Show with Reasonable Particularity the Files It Seeks

Indiana hit the nail on the head in its *Seo v. State* decision as to smartphones being inapposite to physical documents. But this novel issue will continue to evolve in other jurisdictions, and in all likelihood, with the United States Supreme Court eventually weighing in. The government should first have to show by a

195. *Id.*
196. *Id.* (quoting United States. v. Djibo, 151 F. Supp. 3d 297, 310 (E.D.N.Y. 2015)).
197. *Id.*
198. *Id.* at 960-61.
199. *Id.* at 961.
200. *Id.* at 959.
201. *Id.* at 961.
202. *See* Riley v. California, 573 U.S. 373, 401-02 (2014).
203. *See* Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018).
204. *Seo*, 148 N.E.3d at 961-62.
205. *See id.* at 959.

preponderance of the evidence that it took all reasonable steps to explore third-party methods to decrypt the cell phone. While the Fifth Amendment does not protect the physical documents, it does protect the *compulsion* of documents.[206] A significant flaw in *Commonwealth v. Jones* was when the court stated, "That multiple people may have used the LG phone and therefore may know its password does not disprove the defendant's knowledge of the password; *exclusive control of the phone is not required*."[207] This should not be the case; if the government knows other witnesses, and other people know or possibly know the passcode, the government should have to seek those alternatives.

Furthermore, the government can turn to phone companies and potentially obtain the information needed. For example, Apple, similar to many phone companies, publishes guidelines for law enforcement and generally complies with subpoenas and court orders when they are "as narrow and specific as possible."[208] Although Apple cannot produce a passcode or decrypt messages, they can provide emails, iTunes data, Find My iPhone data, etc.[209]

Law enforcement has previously used a third-party vendor to unlock a criminal's cell phone, illustrating different avenues prosecutors could pursue. In 2015, after the San Bernardino mass shooting, the FBI looked for leads on the terrorist's iPhone.[210] The phone, however, had a four-digit passcode.[211] A court required Apple to "write special software to thwart security measures that otherwise threatened to erase its content if muscled through."[212] Apple refused to cooperate due to concerns for consumer privacy and it "not [being] technically feasible for the company to unlock passcodes . . . warrant or no warrant."[213] Regardless, police were able to unlock the iPhone with the help of a third party, showing the feasibility of decrypting a cell phone without a suspect's mental process.[214]

If the government takes all reasonable steps to obtain the passcode information from third parties and is still unable to unlock the phone, then the government must show with reasonable particularity the files, texts, photos, or data needed in order to constitutionally require a defendant to unlock his phone.[215] In each of the act of production cases, the government did not have to prove that the defendant, for example, knew the passcode to the safe, and therefore must unlock the safe.[216] Instead, the government needed to show with reasonable

---

206. Doe v. United States, 487 U.S. 201, 205, 210 n.9 (1988).

207. Commonwealth v. Jones, 117 N.E.3d 702, 717 (Mass. 2019) (emphasis added).

208. *Legal Process Guidelines*, APPLE, https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf (last visited Mar. 18, 2021) [https://perma.cc/LN9K-NRR2].

209. *Id.*

210. Selyukh, *supra* note 32.

211. *Id.*

212. *Id.*

213. *Id.*

214. *Id.*

215. *See* Seo v. State, 148 N.E.3d 952, 960 (Ind. 2020).

216. *See* Doe v. United States, 487 U.S. 201 (1988).

particularity that the documents existed, were in the control and custody of the defendant, and were authentic.[217] With a sufficient showing, and only with that, should the foregone conclusion doctrine apply.

In the one and only United States Supreme Court case where the foregone conclusion doctrine did in fact apply (*Fisher*), the government still could show with reasonable particularity that the requested tax documents existed, were in the defendant's control, and were authentic.[218] The government did not merely have to show that the defendant knew the passcode to the file cabinet, and therefore had to unlock the entire cabinet, surrendering all of the documents as evidence.[219]

Further, "[w]hen confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents."[220] Extending the foregone conclusion doctrine does precisely this. With the advancement of encryption and decryption, the Supreme Court should not extend the foregone conclusion doctrine beyond its original scope—to business files that the government could show with reasonable particularity.[221]

Emergencies will provide exceptions to the suggested framework in extraordinary circumstances.[222] As this area of law continues to expand, solutions to *bona fide* emergencies will become more evident, such as the need to unlock a cell phone to uncover plans to seriously harm others. However, no hard and fast rule will completely alleviate potential problems between balancing the government's need to unlock a cell phone and individual privacy.[223]

B. If the Government Cannot Meet that Standard, It Must Subpoena the Files, and the Fisher *Analysis Governs*

If the government cannot show with reasonable particularity the files it seeks, the fact that the government possesses the cell phone should not be dispositive. In other words, like advocated in *Seo v. State*, the government should give the phone back to the criminal defendant and go through the *Fisher* and *Hubbell* analysis.[224] This gives the government more time to investigate, gather information, and find sufficient evidence for the specific texts, photos, or files sought rather than immediately jumping to the conclusion that a defendant should surrender his self-incrimination privilege.

Stated succinctly, the precedent establishes that the foregone conclusion doctrine applies to business records; thus, applying the exception to passwords

---

217. United States v. Hubbell, 530 U.S. 27, 30 (2000); *see also* Fisher v. United States, 425 U.S. 391, 410 (1976).

218. *Fisher*, 425 U.S. at 413.

219. *See generally id*.

220. Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018).

221. Oral Argument, *supra* note 139, at 28:22.

222. Seo v. State, 109 N.E.3d 418, 432 (Ind. Ct. App. 2018), *vacated*, 148 N.E.3d 952 (Ind. 2020).

223. *Id.* at 439-40.

224. *Fisher*, 425 U.S. at 411; *see also* United States v. Hubbell, 530 U.S. 27, 41-45 (2000).

is clearly beyond its original scope. The foregone conclusion doctrine in *Fisher* applied if a third party held the documents—not if the government could show the documents existed in a file.[225] Using similar reasoning, the foregone conclusion doctrine should not apply merely because the government can show the files exist on the suspect's phone. This would greatly expand an exception that the Supreme Court did not intend.[226] Importantly, the Fifth Amendment does not protect the contents of the documents—rather, it protects the *compulsion of the documents*.[227] The United States Supreme Court has sought to "assure [ ] preservation of that degree of privacy against [the] government."[228] With this in mind, an exclusionary rule would not be appropriate concerning evidence collected in violation of the U.S. Constitution.

C. An Exclusionary Rule is Not Appropriate

At oral argument in *Seo v. State*, Indiana Supreme Court Justice Mark Massa raised the question: "Could we cure any potential violations with an exclusionary rule that would exclude evidence of this act of production and yet would still allow the state access ultimately to the evidence itself?"[229] An exclusionary rule is a "judicially created remedy" applicable in cases in which evidence is collected under unconstitutional circumstances.[230] When evidence is obtained in violation of the person's rights, "the government will generally be prohibited from using that evidence in a criminal prosecution against that person."[231] Although this may seem like the common-sense solution, this solution is tailored more towards the Fourth Amendment and assumes the exact premise of this Note—a constitutional violation in fact occurred.

An exclusionary rule here presupposes the heart of the compelled decryption argument—evidence obtained by unconstitutional conduct. In other words, for an exclusionary rule to be in place, we must assume that compelling a suspect to unlock their phone is a Fifth Amendment violation. And if we presuppose that a constitutional violation occurs when compelling a suspect to enter their passcode, then no need for an exclusionary rule exists because the exclusionary rule applies to the Fourth Amendment already, thereby creating a circular argument.

But even if a "judicially created" exclusionary rule applied, the government would still need to show with reasonable particularity the exact documents or texts it seeks. Allowing the government access to all documents on a cell phone

---

225. *See Fisher*, 425 U.S. at 411.

226. Oral Argument, *supra* note 139, at 28:47.

227. Doe v. United States, 487 U.S. 201, 204 (1988).

228. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

229. Oral Argument, *supra* note 139, at 21:47.

230. United States v. Riley, 920 F.3d 200, 205 (4th Cir. 2019) (quoting Davis v. United States, 564 U.S. 229, 238 (2011)).

231. United States v. Streett, 363 F. Supp. 3d 1212, 1283 (D.N.M. 2018).

opens the door for potential abuse and other avenues for prosecution.[232] Additionally, the *Hubbell* decision rejected this exact "fishing expedition."[233] The documents in *Hubbell* would not have "magically appeared in the prosecutor's office like 'manna from heaven.'"[234] Rather, the documents only appeared after granting Hubbell immunity and taking "mental and physical steps necessary to provide the prosecutor with an accurate inventory of the many sources of potentially incriminating evidence sought by the subpoena."[235] The Supreme Court rejected the broad subpoenas as a "fishing expedition" that allowed the government to derivatively use the produced documents to get an indictment against Hubbell, something that the Fifth Amendment protects.[236]

D. Potential Protection Under the Indiana Constitution

If the United States Supreme Court issues a decision contrary to that of the Indiana Supreme Court, the Indiana Constitution may provide additional protections. Indiana's Self-Incrimination Clause provides that "[n]o person, in any criminal prosecution, shall be compelled to testify against himself."[237] The protection "must be balanced against the government's legitimate demands to compel citizens to testify so that, in order to effect justice, the truth surrounding the criminal incident may be discovered."[238] The similarity between the Indiana and U.S. Constitutions and their parallel judicial history "support *but do not compel* the conclusion that the framers of the Indiana Constitution and the authors of the Fifth Amendment had the same objectives."[239]

The Indiana Supreme Court explained, but rejected, a defendant's argument about how a state can expand upon any federal constitutional right by interpreting its constitutional language based on precedent. In *Edwards v. State*, the trial court determined that the defendant had a severe mental illness, thereby denying the defendant's request to act pro se.[240] The defendant argued that while the Sixth Amendment of the U.S. Constitution allows a defendant to act pro se, the Indiana Constitution provides broader protections from (1) Indiana precedent, and (2) Indiana's constitution explicitly guaranteeing the right "to be heard by 'himself.'"[241] The court rejected the defendant's argument because "[Indiana's]

---

232. *See, e.g.*, Andresen v. Maryland, 427 U.S. 463, 482-83 (1976) (allowing the prosecution to introduce evidence in connection with other crimes that were not mentioned in the search warrant).

233. United States v. Hubbell, 530 U.S. 27, 42 (2000).

234. *Id.*

235. *Id.*

236. *Id.* at 42-43.

237. IND. CONST. art. 1, § 14.

238. Tunis v. State, 129 N.E.3d 258, 263 (Ind. Ct. App. 2019) (quoting *In re* Caito, 459 N.E.2d 1179, 1182 (Ind. 1984)).

239. Ajabu v. State, 693 N.E.2d 921, 932 (Ind. 1998) (emphasis added).

240. Edwards v. State, 902 N.E.2d 821, 823 (Ind. 2009).

241. *Id.* at 828.

precedents respecting self-representation have tracked federal standards," and nothing in the State's precedent says otherwise.[242]

Meanwhile, in *Malinksi v. State*, the Indiana Supreme Court interpreted the State's constitution to allow the right to counsel at an earlier point than the U.S. Constitution.[243] The U.S. Constitution does not require that police inform a custodial suspect about an attorney's efforts to contact him.[244] Nevertheless, the court held that under Indiana's constitution, "an incarcerated suspect has a right under section 13 to be informed that an attorney hired by his family to represent him is present at the station and wishes to speak to him,"[245] thereby broadening the federal constitutional protections via the Indiana Constitution. The court's reasoning was found in light of Indiana's history of an expansive state right to counsel.[246]

The *Edwards* decision demonstrates how the Indiana Supreme Court can broadly interpret Article 1, Section 14's language, "[n]o person, in any criminal prosecution, *shall be compelled to testify against himself*."[247] The *Malinski* holding corroborates this: a suspect was given more protection and allowed a more expansive timing regarding the right to counsel.[248] Both decisions were based primarily on Indiana precedent and an acknowledgment that Indiana's constitution "affords [its] citizens greater protection than its federal counterpart."[249] Our court should look at precedent to determine whether Article 1, Section 14 provides broader protection than the Fifth Amendment. After doing so, the reasonable conclusion is that the Indiana Constitution does afford more extensive protection for suspects.

If the United States Supreme Court holds contrary to the *Seo* decision by adopting the view that the foregone conclusion doctrine applies when the government can prove with reasonable particularity that the criminal defendant knows the passcode, then Indiana precedent nevertheless affords stronger protections for suspects. First, in *Alldredge v. State*, the Indiana Supreme Court conceded that evidence of a defendant refusing to produce documents, books, or papers, which involve testimonial aspects, is not admissible.[250] Further, Indiana does not allow a criminal defendant's refusal to comply with such an order as evidence.[251]

Alldredge illustrates a possible expansion of criminal defendants' protections under the Indiana Constitution. Not only does the Indiana Constitution align with the U.S. Constitution on testimonial compulsion, but the Indiana Supreme Court

---

242. *Id.*
243. Malinski v. State, 794 N.E.2d 1071, 1078-79 (Ind. 2003).
244. *Id.* at 1079.
245. *Id.*
246. *Id.* at 1078-79.
247. IND. CONST. art. 1, § 14 (emphasis added).
248. *Malinski*, 794 N.E.2d at 1078-79.
249. *Id.* at 1078 (citing Ajabu v. State, 693 N.E.2d 921, 929 (Ind. 1998)).
250. Alldredge v. State, 156 N.E.2d 888, 894 (Ind. 1959).
251. *Id.*

did not allow the defendant's refusal to comply with a subpoena as evidence because that exact evidence would violate the Indiana Self-Incrimination Clause.[252]

Additionally, in *Sprague v. State*, the defendant was convicted of grand larceny and moved for a new trial.[253] The trial court admitted evidence of the defendant's noncompliance with an order to produce documents and books relating to the grand larceny charge.[254] The Indiana Supreme Court held that the trial court erred when admitting evidence of the defendant not complying with an order to produce books and documents: "The consensus of judicial opinion is that a defendant in a criminal prosecution cannot be compelled to give or furnish evidence which will incriminate him . . ."[255] The court did not see a difference between producing the documents and admitting evidence of the defendant's refusal to produce the documents; either way, the jury would make the forbidden inference that the books and documents would be favorable to the State.[256]

Another case that could provide criminal defendants protection involved a court order to produce documents. In *State v. Pence*, the defendant refused to produce prescriptions and applications to sell liquor when the defendant was charged with selling whiskey and drugs without a license.[257] The court held that the defendant did not have to produce evidence that may tend to incriminate himself; this would constitute a violation under the Indiana Constitution.[258] This constitutional protection both

> secures a person against the involuntary production of his private books and papers in response to any process or order of court addressed to him in the character of a witness, as well as against the giving of compulsory testimony in every case where the use of such documentary evidence, or such testimony, may tend to incriminate himself.[259]

Two early Indiana cases laid the foundation that shields defendants from producing documents. First, in *Armitage v. State* in 1859, a defendant charged for having a counterfeit banknote could not be compelled to produce the note as evidence against himself.[260] Second, in *McGinnis v. State* in 1865, the Indiana Supreme Court recognized the act-of-production doctrine, asserting that "[i]t is well settled in criminal cases, that the court cannot compel the defendant to produce an instrument in writing, in his possession, to be used in evidence against him, as to do so would be to compel the defendant to furnish evidence against

---

252. Seo v. State, 148 N.E.3d 952, 962 (Ind. 2020).
253. Sprague v. State, 181 N.E. 507, 508 (Ind. 1932).
254. *Id.* at 509.
255. *Id.* at 512.
256. *Id.*
257. State v. Pence, 89 N.E. 488, 488 (Ind. 1909).
258. *Id.* at 490.
259. *Id.* (citations omitted).
260. Armitage v. State, 13 Ind. 441, 443-44 (1859).

himself, which the law prohibits."[261]

The *McGinnis* court acknowledged a balance between protecting suspects' rights and preventing a fishing expedition by stating:

> The description of the instrument in the indictment must be such that it would always serve to notify the defendant of the nature of the charge against him, save him from surprise, and enable him to be prepared to produce the writing when it was his interest to produce it. But when its production would be likely to work an injury to the defendant, by aiding in his conviction, it could not be expected that he would produce it in response to the notice.[262]

These Indiana cases were mindful of the admissibility of evidence against a defendant. The defendant would have had the option of (1) refusing to produce the documents, or (2) producing the documents—both providing a jury with an inference that the evidence must have been in favor of the State, or else the defendant would have produced the documents. The Indiana Supreme Court should integrate the same reasoning from the earlier cases and not strip criminal defendants of their self-incrimination privilege. Thus, the Indiana Constitution could provide additional protection, regardless of any potential Supreme Court decisions.

The Self-Incrimination Clause under the Indiana Constitution should prevent the government from compelling the defendant to produce evidence that could *tend* to be harmful.[263] Given the split in circuits, it's inevitable that the United States Supreme Court will weigh in. If the Court's decision adopts the *Commonwealth v. Jones* framework—applying the foregone conclusion exception when the government can show that the defendant knows the passcode[264]—Indiana's constitution will likely extend protections to criminal defendants. The cases protecting criminal defendants from self-incrimination focus on the evidentiary problems and limit any potential misuse of government power. Hence, the *Seo* decision, like in *Malinski* where the Indiana Supreme Court's decision was based "[i]n light of Indiana's history of an expansive state right to counsel,"[265] is correctly based on precedent. Indiana has protected against implicit testimony by producing documents in violation of Article 1, Section 14, dating back to as early as 1865.[266]

CONCLUSION

The Indiana Supreme Court's groundbreaking decision in *Seo v. State* correctly provides criminal defendants with appropriate self-incrimination

---

261. McGinnis v. State, 24 Ind. 500, 503 (1865).

262. *Id.*

263. *See Pence*, 89 N.E. at 490; *see also* Alldredge v. State, 156 N.E.2d 888, 894 (Ind. 1959).

264. Commonwealth v. Jones, 117 N.E.3d 702, 717-18 (Mass. 2019)

265. Malinski v. State, 794 N.E.2d 1071, 1079 (Ind. 2003).

266. *See McGinnis*, 24 Ind. at 503.

protections. Ultimately, the Fifth Amendment will protect criminal defendants from producing a decrypted cell phone unless either (1) the government shows that the defendant knows the passcode, or (2) the government shows with reasonable particularity the files it seeks. Courts and commentators should keep in mind one principle when analyzing this issue: the Fifth Amendment protects the compulsion of the documents, not the documents themselves.[267]

This Note surveyed federal and Indiana law in the compelled decryption realm. Further, this Note argued that the foregone conclusion exception applies when the government shows with reasonable particularity the files it seeks,[268] as opposed to the government merely showing that the defendant knows the passcode.[269] Inevitably, the United States Supreme Court will issue a decision, either siding with Indiana's view or Massachusetts' view. Accordingly, this Note also analyzed Indiana's Self-Incrimination Clause and early case law that should supply additional security for defendants against government intrusion. In any event, this area of law will continue to develop over time, and this issue is just the first step.

---

267. Doe v. United States, 487 U.S. 201, 205-06, 210 n.9 (1988).

268. *See* Seo v. State, 109 N.E.3d 418, 420 (Ind. Ct. App. 2018), *vacated*, 148 N.E.3d 952 (Ind. 2020).

269. *See Jones*, 117 N.E.3d at 717.