

Spring 3-11-2021

Compelling Suspects to Unlock Their Phones: Recommendations for Prosecutors and Law Enforcement

Carissa A. Uresk

Follow this and additional works at: <https://digitalcommons.law.byu.edu/lawreview>



Part of the [Law Commons](#)

Recommended Citation

Carissa A. Uresk, *Compelling Suspects to Unlock Their Phones: Recommendations for Prosecutors and Law Enforcement*, 46 BYU L. Rev. 601 (2021).

Available at: <https://digitalcommons.law.byu.edu/lawreview/vol46/iss2/10>

This Comment is brought to you for free and open access by the Brigham Young University Law Review at BYU Law Digital Commons. It has been accepted for inclusion in BYU Law Review by an authorized editor of BYU Law Digital Commons. For more information, please contact hunterlawlibrary@byu.edu.

Compelling Suspects to Unlock Their Phones: Recommendations for Prosecutors and Law Enforcement

*Carissa A. Uresk**

CONTENTS

INTRODUCTION	602
I. TECHNOLOGY OVERVIEW.....	603
A. Phone Passcodes.....	603
B. Phone Encryption	604
C. Breaking into Locked Phones	605
1. Phones protected by PINs and alphanumeric passwords	606
2. Phones protected by biometrics.....	609
II. THE FIFTH AMENDMENT PRIVILEGE AGAINST SELF-INCRIMINATION.....	612
A. Testimonial Communications.....	612
1. The act-of-production doctrine.....	613
2. The foregone-conclusion doctrine.....	613
3. U.S. Supreme Court precedent	614
III. APPLYING THE FIFTH AMENDMENT TO COMPELLED PHONE UNLOCKS.....	618
A. Phones Protected by PINs and Alphanumeric Passwords	618
1. Is there a testimonial communication?	618
2. Does the foregone-conclusion doctrine apply?	621
B. Phones Protected by Biometrics.....	637
1. Courts that have held biometrics are not testimonial.....	638
2. Courts that have held biometrics are testimonial.....	640
3. Court that has not clearly chosen one approach	643
4. Is there a clear trend?	644
C. Additional Factors That May Influence a Court's Decision.....	645
1. Is the prosecutor offering immunity?	645
2. What was the suspect compelled to produce?.....	648
IV. RECOMMENDATIONS FOR PROSECUTORS AND LAW ENFORCEMENT	650
CONCLUSION	655

* J. Reuben Clark Law School, J.D. Candidate 2021. Westminster College in Salt Lake City, Utah, B.A. 2017. My thanks to Kelsy Young, Utah County Attorney's Office, for telling me about this issue; Professor Melinda Bowen, J. Reuben Clark Law School, for her feedback and suggestions; and BYU Law Review members for their helpful comments.

INTRODUCTION

In 2017, Katelin Seo told the Hamilton County Sheriff's Department that D.S. raped her.¹ With Seo's consent, a detective viewed and downloaded her iPhone's contents.²

Based on the phone's contents, the detective decided not to file charges against D.S. and instead began investigating Seo for stalking and harassing D.S.³ The detective spoke with D.S., who said Seo called and texted him numerous times each day, sometimes up to thirty times in one day.⁴

Later that month, Seo was arrested for stalking and harassing D.S.⁵ When police arrested Seo, they seized her phone and asked her for the password.⁶ Although they had a warrant for the phone, Seo refused to divulge her password.⁷ So the State was in a bind: it had legally seized a phone that it could not search because the phone was locked and passcode protected.⁸

This scenario is not unique to Hamilton County. Law enforcement agencies across the country struggle with what to do when they legally seize a phone and have court permission to search that phone but are unable to because it is locked.

Ultimately, the solution is to compel the suspect to unlock the phone. The suspect, however, can counter with a Fifth Amendment claim: if the government compels the suspect to unlock the phone, it may be unconstitutionally requiring the suspect to self-incriminate.

In some jurisdictions, courts have addressed this issue and established protocol for how to constitutionally compel a suspect to unlock a phone.⁹ In other jurisdictions, however, this issue remains unresolved, leaving law enforcement and prosecutors without clear guidance.

This paper offers recommendations for law enforcement and prosecutors in jurisdictions where there is no binding caselaw on

1. Eunjoo Seo v. State, 148 N.E.3d 952, 953 (Ind. 2020).

2. *Id.*

3. *Id.*

4. *Id.*

5. *Id.* at 953–54.

6. *Id.* at 954.

7. *Id.*

8. *Id.*

9. See *infra* notes 180, 221, 297, 313, and accompanying text.

this issue. Part II is an overview of passcodes and how they protect phone content. Part III is an explanation of relevant United States Supreme Court precedent on the privilege against self-incrimination. Part IV introduces the pertinent legal questions and explains how some lower courts have addressed this issue. Part V recommends how to successfully get court permission to compel suspects to unlock their phones.

I. TECHNOLOGY OVERVIEW

Before delving into the legal issues, it is helpful to understand the technology behind phone passcodes. Understanding how passcodes work helps explain why this issue has developed, what options law enforcement has, and the different legal issues lawyers and courts must consider. This section will give an overview of (A) the different types of phone passcodes, (B) what it means for a device to be “encrypted,” and (C) the possibility of using technology to forcibly unlock a passcode-protected phone.

A. Phone Passcodes

With smartphones, users can create passcodes that lock and unlock their phones.¹⁰ Passcodes are typically a personal identification number (PIN), an alphanumeric password, or a biometric feature.¹¹

A PIN is a four- or six-digit passcode.¹² If a phone is PIN protected, users unlock the phone by entering a previously selected string of digits.¹³ An alphanumeric password is like a PIN but allows users to create a passcode that includes both digits and letters.¹⁴

10. Tahir Musa Ibrahim, Shafi'i Muhammad Abdulhamid, Ala Abdusalam Alarood, Haruna Chiroma, Mohammed Ali Al-garadi, Nadim Rana, Amina Nuhu Muhammad, Adamu Abubakar, Khalid Haruna & Lubna A. Gabralla, *Recent Advances in Mobile Touch Screen Security Authentication Methods: A Systematic Literature Review*, 85 COMPUTS. & SEC. 1, 2 (2019).

11. *Id.* at 3–7.

12. *Id.* at 4.

13. *Id.*

14. Lorenzo Franceschi-Bicchierai, *Stop Using 6-Digit iPhone Passcodes*, VICE: MOTHERBOARD (Apr. 16, 2018, 11:56 AM), https://www.vice.com/en_us/article/59jq8a/how-to-make-a-secure-iphone-passcode-6-digits.

Biometrics are unique physical attributes used for identification and authentication.¹⁵ Common biometric authentication methods for phones are fingerprint, facial, and iris.¹⁶ For example, users can scan their thumbprints into their phone.¹⁷ When the phone is locked, users scan their thumb again; if the new scan matches the previously stored scan, the phone will unlock.¹⁸ This process is called “one-to-one matching” because the phone is comparing a current sample to a previously made sample.¹⁹

B. Phone Encryption

In addition to passcodes, smartphones increasingly use encryption to protect data while the phone is locked.²⁰ When a phone is encrypted, its contents²¹ (plaintext) are converted to unintelligible characters (ciphertext).²² A decryption key is necessary to change the contents from ciphertext to plaintext and vice versa.²³ A decryption key is composed of “bits,” which are strings of zeros and ones.²⁴ Decryption keys are typically 128- or 256-bits long and automatically generated by the phone’s software.²⁵ While a 256-bit key has significantly more possible keys than a 128-bit key, both have an “unimaginably large number[]” of possible keys and are thus considered uncrackable.²⁶

Importantly, the phone’s passcode is not the decryption key.²⁷ Rather, the passcode is a way to release the more complex

15. *What Are Biometrics?*, BIOMETRICS INST., <https://www.biometricsinstitute.org/what-is-biometrics/faqs/> (last visited Oct. 5, 2020).

16. Robin Feldman, *Considerations on the Emerging Implementation of Biometric Technology*, 25 HASTINGS COMM’NS & ENT. L.J. 653, 655 (2003).

17. *Id.* at 655–56.

18. *Id.*

19. *Id.*

20. Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 GEO. L.J. 989, 990 (2018).

21. “Contents” includes text, images, videos, and programs. *Id.* at 993.

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

23. *Id.*

24. Kerr & Schneier, *supra* note 20, at 993.

25. *Id.* at 993–94.

26. *Id.*

27. *Id.* at 995.

encryption key.²⁸ When a user enters the correct passcode, the phone accesses the decryption key, which then decrypts the device.²⁹ Thus, every time users lock their phones they also encrypt their phones' content.³⁰ When they unlock their phones, the content is automatically decrypted.³¹ This process is invisible to users.³²

The difference between locking and encrypting a device is subtle but significant. Locking a phone is like locking a file room's door; if you can find another way into the room—through a window, perhaps—the contents of the files are the same as if you had unlocked and entered through the door.³³ However, imagine that the door is locked *and* the files are shredded—that is an encrypted device.³⁴ In practice, this means that law enforcement can potentially access the contents of a locked, but not encrypted, phone by removing and accessing the storage device with laboratory equipment.³⁵ If the phone is encrypted, however, law enforcement will only see unintelligible data.³⁶ For simplicity's sake, unless otherwise noted, when this Note refers to unlocking a phone it also means decrypting an encrypted phone.³⁷

C. Breaking into Locked Phones

Of course, the simplest solution to this problem, in criminal investigations, is for suspects to voluntarily unlock their phones.³⁸

28. Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 *FORDHAM L. REV.* 203, 221 (2018).

29. *Id.* at 222.

30. *See id.* at 221.

31. *Id.*

32. Kerr & Schneier, *supra* note 20, at 994.

33. *See* Price & Simonetti, *supra* note 22, at 43 ("For example, early iPhones could be 'locked,' but they did not encrypt the data inside, making it possible to read user contents by bypassing the lock.").

34. *See id.*

35. *See* Sacharoff, *supra* note 28, at 221.

36. *Id.*

37. Because nearly all smartphones now use encryption, the distinction is not often necessary to point out. *Id.*

38. Potentially, if a phone is protected by biometrics, law enforcement could attempt to use the suspect's biometrics without the suspect's permission. For example, an officer could hold a phone protected by facial identification up to a suspect's face. This does, however, raise a Fourth Amendment concern over whether the state has illegally seized the suspect's biometric features. This Note will not cover that issue, but for a discussion of the topic see Opher Shweiki & Youli Lee, *Compelled Use of Biometric Keys to Unlock a Digital Device: Deciphering Recent Legal Developments*, 67 *DOJ J. FED. L. & PRAC.* 23, 25–34 (2019).

While some suspects may do so, it is unlikely that they will for a variety of reasons—including a reluctance to self-incriminate and a belief that the Constitution protects their noncompliance. Whatever the reason, when users refuse to unlock their phones, law enforcement can try to force the phone to unlock, so long as they have legally seized the phone. The likely success of this approach depends on the type of passcode protecting the phone.

1. Phones protected by PINs and alphanumeric passwords

PINs and alphanumeric passwords are designed in such a way that the fastest way to break into the phone is through a brute-force attack.³⁹ A brute-force attack entails attempting every possible passcode until the phone unlocks.⁴⁰ The longer the code, the longer a brute-force attack will take.⁴¹ To prevent brute-force attacks, many phone security systems have escalating time delays after a user enters an invalid passcode.⁴² These systems also let users enable an option that erases the phone's content after a certain amount of incorrect entries.⁴³ For example, the current iPhone operating system requires a user to wait one minute before entering a passcode after five failed attempts.⁴⁴ That delay escalates to one hour after nine failed attempts.⁴⁵ If the "Erase Data" function is turned on, the device automatically erases all data after ten consecutive failed attempts.⁴⁶

In the past, law enforcement has had difficulty breaking four- and six-digit PINs. For example, in 2015, gunmen killed fourteen people in San Bernardino, California.⁴⁷ The FBI believed that one of the gunmen's phones contained important evidence, which the FBI could not access because the phone was protected by

39. Kerr & Schneier, *supra* note 20, at 994.

40. *Id.*

41. *Id.* ("Adding a single bit to the encryption key only slightly increases the amount of work necessary to encrypt, but doubles the amount of work necessary to brute-force attack the algorithm.").

42. *Id.* at 1000.

43. *Id.*

44. *Passcodes*, APPLE INC., <https://support.apple.com/guide/security/passcodes-sec20230a10d/1/web/1> (last visited Oct. 5, 2020).

45. *Id.*

46. *Id.*

47. Mike Isaac, *Explaining Apple's Fight with the F.B.I.*, N.Y. TIMES (Feb. 17, 2006), <https://www.nytimes.com/2016/02/18/technology/explaining-apples-fight-with-the-fbi.html>.

a four-digit passcode.⁴⁸ A legal battle between Apple and the FBI ensued, and a federal court ordered Apple to unlock the iPhone.⁴⁹ Apple refused and, before scheduled court proceedings, a third party found a way to unlock the phone for the FBI.⁵⁰ To Apple's chagrin, the FBI refused to divulge how the third party unlocked the phone.⁵¹

Since the Apple-FBI standoff, passcodes have become more susceptible to brute-force attacks.⁵² Law enforcement relies on two companies to break into phones: Cellebrite and Grayshift.⁵³ Cellebrite is an Israeli-owned company that claims it can unlock phones running up to Android 10 and iOS 13.3.x, as well as devices manufactured by Motorola, LG, Sony, Nokia, and other companies.⁵⁴ Cellebrite sells "on-premise" devices, meaning that law enforcement officers can purchase Cellebrite technology and use it themselves.⁵⁵ Because this technology is sold only to law enforcement, it is hard to know the exact cost, but most estimates show prices ranging from \$2,499 to \$15,999, depending on the model.⁵⁶

Some agencies also use GrayKey, a device manufactured by Grayshift. Grayshift has publicly advertised its ability to crack a four-digit iPhone passcode in six-and-a-half to thirteen minutes.⁵⁷ If that number is accurate, it would take, on average, 22.2 hours to crack a 6-digit passcode, 92.5 days to crack an 8-digit passcode, and

48. *Id.*; Chris Fox & Dave Lee, *Apple Rejects Order to Unlock Gunman's Phone*, BBC NEWS (Feb. 17, 2016), <https://www.bbc.com/news/technology-35594245>.

49. *Id.*

50. Katie Benne, John Markoff & Nicole Perloff, *Apple's New Challenge: Learning How the U.S. Cracked Its iPhone*, N.Y. TIMES (Mar. 29, 2016), <https://www.nytimes.com/2016/03/30/technology/apples-new-challenge-learning-how-the-us-cracked-its-iphone.html>.

51. *Id.*

52. Franceschi-Bicchierai, *supra* note 14.

53. Price & Simonetti, *supra* note 22, at 47.

54. *Cellebrite Premium*, CELLEBRITE, <https://www.cellebrite.com/en/ufed-premium/> (last visited Oct. 5, 2020).

55. *Unlock and Extract Critical Mobile Data in Your Agency with Cellebrite's Premium*, CELLEBRITE, <https://www.cellebrite.com/en/cellebrite-premium-2/> (last visited Oct. 5, 2020).

56. *Product Information: Cellebrite UFED Series*, SC MEDIA (Oct. 1, 2015), <https://www.scmagazine.com/review/cellebrite-ufed-series/>.

57. *Researcher Estimates GrayKey Can Unlock 6-Digit iPhone Passcode in 11 Hours, Here's How to Protect Yourself*, APPLEINSIDER (Apr. 16, 2018), <https://appleinsider.com/articles/18/04/16/researcher-estimates-graykey-can-unlock-a-6-digit-iphone-passcode-in-11-hours-heres-how-to-protect-yourself>.

25.4 years to crack a 10-digit passcode.⁵⁸ In comparison, it would take five to six years to crack a six-character alphanumeric password.⁵⁹ Like Cellebrite, GrayKey is sold only to law enforcement and is an on-premise device that officers can use themselves.⁶⁰ One GrayKey model permits 300 uses and costs \$15,000; another model allows unlimited uses and costs \$30,000.⁶¹ Unlike Cellebrite, GrayKey only works on Apple devices.⁶² Further, GrayKey can only unlock some versions of iOS 12 and lower.⁶³

In response to these technologies, phone manufacturers develop better security systems.⁶⁴ For example, in 2018, Apple announced a software update that automatically disables the phone's charging port an hour after the phone is locked.⁶⁵ Because code-breaking devices plug into the charging port, this software update thwarts those devices.⁶⁶ Apple claimed that the update was not an attempt to "frustrate" law enforcement, but a way "to help customers defend against hackers, identity thieves and intrusions into their personal data."⁶⁷ Since the update, Cellebrite, but not Grayshift, has developed technology to work around that

58. @matthew_d_green, TWITTER (Apr. 16, 2018, 8:17 AM), https://twitter.com/matthew_d_green/status/985885001542782978?lang=en. Green is an associate professor and cryptographer at the Johns Hopkins Information Security Institute. *Matthew D. Green*, JOHNS HOPKINS UNIV. (Feb. 5, 2020), <https://isi.jhu.edu/~mgreen/>.

59. Julia P. Eckart, *The Department of Justice Versus Apple Inc.: The Great Encryption Debate Between Privacy and National Security*, 27 CATH. U.J.L. & TECH. 1, 10 (2019).

60. *GrayKey*, GRAYSHIFT, <https://graykey.grayshift.com/> (last visited Oct. 5, 2020).

61. Thomas Brewster, *Mysterious \$15,000 'GrayKey' Promises to Unlock iPhone X for the Feds*, FORBES (Mar. 5, 2018, 12:10 PM), <https://www.forbes.com/sites/thomasbrewster/2018/03/05/apple-iphone-x-graykey-hack/#6188c0fb2950>.

62. Andy Greenberg, *Cellebrite Says It Can Unlock Any iPhone for Cops*, WIRED (June 14, 2019, 6:05 PM), <https://www.wired.com/story/cellebrite-ufed-ios-12-iphone-hack-android/>.

63. *Id.*

64. Jack Nicas, *Apple to Close iPhone Security Hole That Law Enforcement Uses to Crack Devices*, N.Y. TIMES (June 13, 2018), <https://www.nytimes.com/2018/06/13/technology/apple-iphone-police.html>.

65. *Id.*

66. *Id.*

67. Roger Fingas, *Apple Confirms iOS 12's 'USB Restricted Mode' Will Thwart Police, Criminal Access*, APPLEINSIDER (June 13, 2018), <https://appleinsider.com/articles/18/06/13/apple-confirms-ios-12s-usb-restricted-mode-designed-to-thwart-spies-criminals-police-seizures>; Heather Kelly, *Apple Closes Law Enforcement Loophole for the iPhone*, CNN BUS. (June 14, 2018, 5:35 AM), <https://money.cnn.com/2018/06/13/technology/apple-iphone-law-enforcement/index.html>.

software update.⁶⁸ This cycle resembles a cat-and-mouse game where phone companies develop new software that seems impermeable, a forensics company develops a workaround, the phone manufacture creates a fix, and so on.⁶⁹

2. Phones protected by biometrics

In addition to passcodes, many phones are protected by biometrics. The three most common types for phones are fingerprint, facial, and iris identification.

Fingerprint identification, also called touch identification, unlocks a phone when a “live” fingerprint placed on a sensor matches a previously stored mathematical representation of that fingerprint.⁷⁰ To create a stored mathematical representation, users repeatedly place different sections of their fingerprint on the phone’s sensor.⁷¹ Because the sensor is smaller than the average adult fingerprint, these repeated placements allow the phone to gather a complete representation of the fingerprint.⁷² However, when users later unlock their phones, only a section of their fingerprint is actually sensed.⁷³ This means that phones unlock by comparing a smaller portion of a “live” fingerprint to a complete, stored representation.⁷⁴

Similar to fingerprint identification, facial identification works by comparing a “live” image of someone’s face to a previously stored image.⁷⁵ The images are compared for mathematical, and not just pictorial, likeness.⁷⁶ For example, Apple’s Face ID uses over 30,000 infrared dots to form a “depth map” that is a mathematical representation of the face.⁷⁷ It also requires that the user’s attention be directed at the device.⁷⁸ Apple claims that facial identification is

68. Greenberg, *supra* note 62.

69. *Id.*

70. *About Touch ID Advanced Security Technology*, APPLE INC. (Sept. 11, 2017) [hereinafter *About Touch ID*], <https://support.apple.com/en-us/HT204587>.

71. *Id.*

72. *Id.*

73. *Id.*

74. *Id.*

75. *About Face ID Advanced Technology*, APPLE INC. (Feb. 26, 2020) [hereinafter *About Face ID*], <https://support.apple.com/en-us/HT208108>.

76. *Id.*

77. *Id.*

78. *Id.*

more secure than fingerprint identification; it says the likelihood of a random person looking at an iPhone protected by Face ID and unlocking it are 1 in 1,000,000⁷⁹ (compared to 1 in 50,000 for Touch ID).⁸⁰

Iris identification is a less popular biometric-identification method.⁸¹ Iris identification uses an infrared light to take a high-resolution image of an iris.⁸² If the image matches a previously stored image, the phone unlocks.⁸³ Samsung, which makes phones with iris scanners, claims that “because virtually no two irises are alike as well as being almost impossible to replicate, scanning your irises is a fool-proof method of mobile security.”⁸⁴

Unlike PINs or alphanumeric passwords, biometrics cannot be “guessed” through a brute-force attack. However, biometrics can sometimes be replicated and the phone “tricked” into unlocking.

For example, a German hacking group claimed it unlocked an iPhone 5s with a fake finger created from a photograph of the user’s fingerprint on a glass surface.⁸⁵ Likewise, researchers at New York University and Michigan State University claimed they made fake fingerprints composed of common features that could unlock phones up to sixty-five percent of the time.⁸⁶ However, these fake fingerprints were not tested on actual phones, and other

79. However, the “statistical probability is different for twins and siblings that look like you and among children under the age of 13, because their distinct facial features may not have fully developed.” *Id.*

80. *About Touch ID*, *supra* note 70. But see JV Chamary, *No, Apple’s Face ID Is Not a ‘Secure Password’*, FORBES (Sept. 18, 2017, 11:00 AM), <https://www.forbes.com/sites/jvchamary/2017/09/18/security-apple-face-id-iphone-x/#30063e4d4c83> (claiming there is “no real evidence to prove [Face ID] is more secure”).

81. Many phones, like iPhones, do not have iris scanners, possibly because they do not work well with screen protectors, contacts, and glasses. *Comparison: iPhone X vs. Galaxy Note 8 Biometrics*, APPLEINSIDER (Dec. 11, 2017), <https://appleinsider.com/articles/17/12/11/comparison-iphone-x-vs-galaxy-note-8-biometrics>.

82. *Iris Recognition*, ELEC. FRONTIER FOUND. (Oct. 25, 2019), <https://www EFF.ORG/pages/iris-recognition>.

83. *Id.*

84. *How Does the Iris Scanner Work on Galaxy S9, Galaxy S9+, and Galaxy Note9?*, SAMSUNG, <https://www.samsung.com/global/galaxy/what-is/iris-scanning/> (last visited Oct. 5, 2020).

85. *Chaos Computer Club Breaks Apple TouchID*, CHAOS COMPUT. CLUB (Sept. 21, 2013, 10:04 PM), <https://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid>.

86. Aditi Roy, Nasir Memon & Arun Ross, *MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems*, 12 IEEE TRANSACTIONS ON INFO. FORENSICS & SEC. 9, 2013–25 (Sept. 2017).

researchers expect the unlock rate would be much lower in real-world conditions.⁸⁷ These examples show that breaking into a fingerprint-protected phone is possible, but victory is unpredictable and expensive.

Groups have also had success with fake faces and eyes. For example, Forbes used a three-dimensional, printed head to break into four different phones running Android.⁸⁸ The fake head did not work on iPhones.⁸⁹ A different researcher, however, was able to fool an iPhone X's Face ID using a three-dimensional printer, silicone, and paper tape.⁹⁰ Similarly, a hacking group posted a video of its members unlocking an iris-protected Samsung phone by creating a "dummy eye" with a digital photograph, office printer, and contact lens.⁹¹

Importantly, there are often restrictions on when biometrics will unlock a phone. For example, Motorola phones require users to enter a PIN or password if the phone has been locked for seventy-two hours, has restarted, or has unsuccessfully read a fingerprint five times.⁹² Likewise, iPhone Touch ID and Face ID will not work if, among other reasons, there have been five unsuccessful reading attempts, the phone has been locked for forty-eight hours, or the phone has just turned on.⁹³

In sum, locked phones are not impenetrable. However, breaking into a locked phone is impractical for three reasons: (1) it is expensive, (2) it takes time, and (3) the technology is

87. Vindu Goel, *That Fingerprint Sensor on Your iPhone Is Not as Safe as You Think*, N.Y. TIMES (Apr. 10, 2017), <https://www.nytimes.com/2017/04/10/technology/fingerprint-security-smartphones-apple-google-samsung.html>.

88. This process requires fifty cameras, which take pictures of the model's head, and software to compile all of the pictures. Thomas Brewster, *We Broke Into a Bunch of Android Phones With a 3D-Printed Head*, FORBES (Dec. 13, 2018, 7:00 AM), <https://www.forbes.com/sites/thomasbrewster/2018/12/13/we-broke-into-a-bunch-of-android-phones-with-a-3d-printed-head/#18bd796f1330>.

89. *Id.*

90. Mai Nguyen, *Vietnamese Researcher Shows iPhone X Face ID 'Hack'*, REUTERS (Nov. 14, 2017, 6:46 AM), <https://www.reuters.com/article/us-apple-vietnam-hack/vietnamese-researcher-shows-iphone-x-face-id-hack-idUSKBN1DE1TH>.

91. *Hacking the Samsung Galaxy S8 Iris Scanner*, CHAOS COMPUT. CLUB (May 23, 2017), <https://media.ccc.de/v/biometrie-s8-iris-en>.

92. *Use Fingerprint Security – Moto G Plus 4th Generation*, MOTOROLA, <https://support.motorola.com/us/en/solution/MS110999> (last visited Oct. 5, 2020).

93. *About Face ID*, *supra* note 75; *About Touch ID*, *supra* note 70.

constantly changing. For those reasons, law enforcement agencies may choose to try compelling suspects to unlock their phones.

II. THE FIFTH AMENDMENT PRIVILEGE AGAINST SELF-INCRIMINATION

The Fifth Amendment guarantees that “[n]o person . . . shall be compelled in any criminal case to be a witness against himself.”⁹⁴ This privilege is triggered only when someone is “[1] compelled [2] to make a testimonial communication [3] that is incriminating.”⁹⁵ In compelled-phone-unlock cases, both parties often agree that the passcode was compelled and is incriminating.⁹⁶ Thus, the issue in these cases is usually whether unlocking a phone is a testimonial communication. The sections below describe how the United States Supreme Court has defined “testimonial communication.”

A. Testimonial Communications

In order to be testimonial, a communication must, “explicitly or implicitly, relate a factual assertion or disclose information.”⁹⁷ Likewise, testimonial communications require individuals to express the contents of their minds.⁹⁸ For that reason, the privilege against self-incrimination is not implicated when suspects give a blood sample,⁹⁹ stand in a lineup,¹⁰⁰ or wear certain clothing.¹⁰¹ Although these actions may be compelled and incriminating,

94. U.S. CONST. amend. V.

95. *Fisher v. United States*, 425 U.S. 391, 408 (1976).

96. *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011 (Grand Jury Subpoena)*, 670 F.3d 1335, 1341 (11th Cir. 2012) (“Here, the Government appears to concede, as it should, that the decryption and production are compelled and incriminatory.”). Prosecutors are likely to concede that the act is incriminating because even non-inculpatory communications are incriminating if they “furnish a link in the chain of evidence” needed to prosecute. *Hoffman v. United States*, 341 U.S. 479, 486 (1951); *see also* *United States v. Hubbell*, 530 U.S. 27, 37 (2000) (“It has, however, long been settled that [the Fifth Amendment’s] protection encompasses compelled statements that lead to the discovery of incriminating evidence even though the statements themselves are not incriminating and are not introduced into evidence.”).

97. *Doe v. United States*, 487 U.S. 201, 210 (1988).

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

99. *Schmerber v. California*, 384 U.S. 757, 765 (1966).

100. *United States v. Wade*, 388 U.S. 218, 221–22 (1967).

101. *Holt v. United States*, 218 U.S. 245, 252–53 (1910).

they are not testimonial communications because they do not require individuals to reveal the contents of their minds.¹⁰²

While defining and clarifying the meaning of testimonial communication, the Supreme Court has articulated two important doctrines: the act-of-production doctrine and the foregone-conclusion doctrine.

1. *The act-of-production doctrine*

When suspects hand over documents, they are making a testimonial communication—wholly independent from the documents’ contents—that they have possession, control, and ownership over those documents.¹⁰³ This is the act-of-production doctrine.¹⁰⁴

For example, the government may subpoena suspects’ diaries, believing that those diaries contain evidence of a crime. The entries in the diaries are most certainly testimonial communications. Putting that aside, however, if the suspects surrender their diaries, they would also be making testimonial communications—through the act of production—that they own those diaries, have possession of those diaries, and that those diaries are the ones the government requested.¹⁰⁵ As the Supreme Court put it, “[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.”¹⁰⁶

2. *The foregone-conclusion doctrine*

If the government already knows the information conveyed, however, the act of production is not a testimonial communication.¹⁰⁷ This is called the “foregone-conclusion doctrine” because suspects add “little or nothing to the sum total of the Government’s information” by producing the requested information.¹⁰⁸ In other words, if the information that suspects

102. *Schmerber*, 384 U.S. at 765; *Wade*, 388 U.S. at 221–22; *Holt*, 218 U.S. at 252–53.

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

104. *Id.*

105. *See id.*

106. *Id.*

107. *Id.* at 411.

108. *Id.*

communicate through the act of production is already known by the government, the suspects are simply surrendering information – not testifying.¹⁰⁹

Returning to the example from above, presume that the government can independently prove that the suspects own and have control over the requested diaries. In that case, any potential testimonial communication is a foregone conclusion, and the Fifth Amendment is not implicated.¹¹⁰

3. U.S. Supreme Court precedent

The Supreme Court first articulated the act-of-production and foregone-conclusion doctrines in *United States v. Fisher*. The Court applied these doctrines again in *United States v. Doe* and *United States v. Hubbell*. A description of the facts and holdings of each case is helpful to understanding how the Supreme Court identifies testimonial communications.

a. *United States v. Fisher*.

In *Fisher*, Internal Revenue agents interviewed taxpayers suspected of violating federal income tax laws.¹¹¹ After the interviews, the taxpayers collected tax documents from their accountants and sent the documents to their lawyers.¹¹² When the IRS served summonses on the lawyers for those documents, the lawyers refused to comply, claiming, in part, that turning over the documents would force the taxpayers to compulsorily incriminate themselves.¹¹³

The Court's analysis focused on whether the documents were a testimonial communication by the taxpayers. The Court reiterated that "the privilege protects a person only against being incriminated by his own compelled testimonial communications."¹¹⁴ Although compelling taxpayers to produce an accountant's workpapers "without doubt involves substantial compulsion," the actual creation of the workpapers was not compelled.¹¹⁵ Further, the taxpayers were not being forced to reveal

109. *Id.*

110. *See generally id.* at 393–94.

111. *Id.* at 394.

112. *Id.*

113. *Id.* at 394–95.

114. *Id.* at 409.

115. *Id.* at 409–10.

the contents of their minds because they were not compelled to “restate, repeat, or affirm the truth of the contents of the documents sought.”¹¹⁶ Since the tax documents were prepared by accountants, and did not contain any testimonial declarations by the taxpayers, the Court held that the taxpayers could not claim the documents were their testimony.¹¹⁷

Yet the Court recognized that compliance with the subpoena “concedes the existence of the papers demanded and their possession or control by the taxpayer.”¹¹⁸ In other words, by producing the documents, the taxpayers would be testifying that the documents exist, are the documents requested, and are in their possession.¹¹⁹

Ultimately, however, the Court decided that producing the documents would not be a testimonial communication.¹²⁰ This was because the “existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government’s information by conceding that he in fact has the papers.”¹²¹ By complying with the subpoena, the taxpayers were not communicating any information to the government that the government did not already know.¹²² So the Fifth Amendment did not protect the taxpayers from producing the documents.¹²³

b. United States v. Doe.

In *Doe*, a grand jury subpoenaed bank records from Doe, its target.¹²⁴ Doe surrendered some records but invoked the Fifth Amendment privilege against self-incrimination for other records.¹²⁵ When the government subpoenaed banks for those records, the banks refused, citing bank-secrecy laws.¹²⁶ In response, the government asked the district court to order Doe to sign consent forms.¹²⁷ These forms applied to “any and all accounts over which

116. *Id.* at 409.

117. *Id.*

118. *Id.* at 410.

119. *Id.*

120. *Id.* at 410–11.

121. *Id.*

122. *Id.*

123. *Id.* at 414.

124. *Doe v. United States*, 487 U.S. 201, 202 (1988).

125. *Id.* at 202–03.

126. *Id.* at 203.

127. *Id.* at 203–04.

Doe had a right of withdrawal, without acknowledging the existence of any such account.”¹²⁸ The district court, after an appeal to the Court of Appeals for the Fifth Circuit, ordered Doe to sign the form.¹²⁹ When Doe refused to sign, he was held in civil contempt; this sanction was stayed pending the Supreme Court’s decision.¹³⁰

At the Supreme Court, Doe claimed that signing the forms would be an incriminating, testimonial communication.¹³¹ The Court, however, held that by signing and executing the forms Doe would not be communicating, explicitly or implicitly, any factual assertions or conveying any information to the government.¹³² This was because the consent forms, by speaking in the hypothetical and not referring to specific accounts, did not acknowledge that the accounts actually existed or were controlled by Doe.¹³³ Ultimately, by signing the forms, Doe would not be making any statement about the existence of the bank accounts or his control over those accounts.¹³⁴

Dissenting, Justice Stevens argued that a suspect “may in some cases be forced to surrender a key to a strongbox containing incriminating documents” but may not be forced to “reveal the combination to his wall safe.”¹³⁵ The problem with the latter, he argued, is that it requires a suspect to “use his mind to assist the Government in developing its case.”¹³⁶ For Justice Stevens, requiring Doe to execute the consent forms is akin to requiring him to reveal a safe combination.¹³⁷

In a footnote, the majority said it did not “disagree with the dissent that ‘[t]he expression of the contents of an individual’s mind’ is testimonial communication for purposes of the Fifth Amendment.”¹³⁸ It did, however, feel that what the

128. *Id.* at 204.

129. *Id.* at 205–06.

130. *Id.*

131. *Id.* at 207.

132. *Id.* at 215.

133. *Id.*

134. *Id.* at 215–16.

135. *Id.* at 219 (Stevens, J., dissenting).

136. *Id.* at 220 (Stevens, J., dissenting).

137. *Id.*

138. *Doe*, 487 U.S. at 210 n.9.

government requested was more like asking Doe for a key than a safe combination.¹³⁹

Thus, signing the form was non-testimonial and the Fifth Amendment did not protect Doe.¹⁴⁰

c. *United States v. Hubbell*.

In *Hubbell*, Webster Hubbell, a member of the Whitewater Development Corporation, pled guilty to mail fraud and tax evasion.¹⁴¹ As part of that plea, Hubbell “promised to provide the Independent Counsel with ‘full, complete, accurate, and truthful information’ about matters relating to the Whitewater investigation.”¹⁴² To see if Hubbell was complying with that promise, the Independent Counsel subpoenaed eleven different categories of documents; Hubbell provided those documents, which a grand jury used to charge Hubbell with other crimes.¹⁴³ The district court, however, dismissed the indictment after determining that the act-of-production doctrine protected Hubbell.¹⁴⁴ The case made its way to the Supreme Court.¹⁴⁵

The Court decided that Hubbell was constitutionally protected from complying with the subpoena.¹⁴⁶ It held that the government’s request in this instance violated Hubbell’s privilege against self-incrimination because the information it asked for was not a “foregone conclusion.”¹⁴⁷ Unlike in *Fisher*, where the government could independently prove the existence and authenticity of the requested documents, the government here had no prior knowledge of the documents that Hubbell produced in response to the subpoena.¹⁴⁸ Indeed, the subpoena asked for such a breadth of information that the prosecutor “needed [Hubbell’s] assistance both to identify potential sources of information and to produce those sources.”¹⁴⁹ This communicated facts not already known to

139. *Id.*

140. *Id.* at 217.

141. *United States v. Hubbell*, 530 U.S. 27, 30 (2000).

142. *Id.*

143. *Id.* at 31.

144. *Id.* at 31–32.

145. *Id.* at 34.

146. *Id.* at 45–46.

147. *Id.* at 44.

148. *Id.* at 44–45.

149. *Id.* at 41.

the government¹⁵⁰ and required Hubbell “to make extensive use of the contents of his own mind.”¹⁵¹ Accordingly, his act of production was testimonial, and the Fifth Amendment protected him.¹⁵²

In sum, the government cannot compel individuals to make self-incriminating, testimonial communications. While this protection is limited to factual assertions that convey information, it includes acts of production that reveal new information to the government.

III. APPLYING THE FIFTH AMENDMENT TO COMPELLED PHONE UNLOCKS¹⁵³

Given the reality of how difficult it is to unlock a phone, law enforcement may try compelling suspects to unlock their phones. Specifically, law enforcement may try to compel suspects to (1) disclose their passcodes orally or in writing, (2) enter a passcode without disclosing it, or (3) produce their phones in a decrypted form.¹⁵⁴

While compulsion might be technologically simpler than trying to break into a phone, it raises difficult legal questions regarding the privilege against self-incrimination. Specifically, compelling suspects to unlock their phones raises two questions: First, is there a testimonial communication? Second, does the foregone-conclusion doctrine apply? Because the analysis may vary depending on the type of passcode, PINs and alphanumeric passwords are addressed first and biometrics second.

A. Phones Protected by PINs and Alphanumeric Passwords

1. Is there a testimonial communication?

When law enforcement seeks to compel a suspect to unlock a phone, the first question that courts address is whether the suspect

150. *Id.* at 44–45.

151. *Id.* at 43 (internal quotation marks omitted).

152. *Id.* at 44–45.

153. This Note only includes opinions and orders, accessible via Westlaw and LexisNexis, from federal circuit courts, federal district courts, and state appellate courts. State trial court decisions have been excluded based on their sheer volume and inaccessibility.

154. Kerr & Schneier, *supra* note 20, at 1001–02.

is making a testimonial communication by unlocking the phone. A phone passcode may be testimonial in two different ways.

First, a passcode may be testimonial if the actual passcode explicitly relates a fact. For example, suspected heroin dealers would be relating a fact if their passcodes were “ISELLHEROIN.” Because this passcode relates a fact that is incriminating, compelling it would likely implicate the Fifth Amendment.¹⁵⁵ However, this situation is not probable and has not yet been addressed by a court.

Second, unlocking a phone is testimonial if the act of producing the passcode communicates information independent from the phone’s passcode. By unlocking a phone, users at the very least communicate that they know the passcode to that phone.¹⁵⁶ Users may also be communicating that they have possession, control, or ownership over the phone.¹⁵⁷

But the act of unlocking a phone may not be testimonial if there is no dispute that the suspect owns the phone and if the suspect is not asked to reveal the password to law enforcement.¹⁵⁸ For example, an FBI agent asked a suspect to unlock a phone and the suspect did so, without telling or showing the agent the password.¹⁵⁹ The Fourth Circuit said: “Certainly, [the suspect] has not shown that her act communicated her cell phone’s unique password.”¹⁶⁰ This was because the phone’s ownership was never in dispute and the suspect “simply used the unexpressed contents of her mind to type in the passcode herself.”¹⁶¹ But the court ultimately resolved this issue on other grounds, meaning it did not

155. This type of passcode would not implicate the Fifth Amendment, however, if the passcode were typed in by the user and not disclosed to the government. Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767, 779 (2019).

156. See, e.g., *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011* (*Grand Jury Subpoena*), 670 F.3d 1335, 1346 (11th Cir. 2012); *Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 614 (Mass. 2014).

157. See, e.g., *Grand Jury Subpoena*, 670 F.3d at 1346; *Gelfgatt*, 11 N.E.3d at 614.

158. *United States v. Oloyede*, 933 F.3d 302, 309 (4th Cir. 2019), cert. denied sub nom. *Popoola v. United States*, 140 S. Ct. 1212 (2020), and cert. denied sub nom. *Ogundele v. United States*, 140 S. Ct. 1213 (2020), and cert. denied sub nom. *Popoola v. United States*, 140 S. Ct. 2554 (2020).

159. *Id.* at 308.

160. *Id.* at 309.

161. *Id.*

make a ruling on whether the suspect had made a testimonial communication.¹⁶²

Contrary to the Fourth Circuit's reasoning, most courts do find that the act of unlocking phones is a testimonial communication.¹⁶³ To support this conclusion, some courts reference Justice Stevens's safe analogy from his *Doe* dissent.¹⁶⁴ Applying this analogy to phones, some courts have stressed that passcodes are not like a key because passcodes are not physical items.¹⁶⁵ Rather, passcodes are contained within a person's mind, like a safe combination.¹⁶⁶ Thus, requiring suspects to reveal or use their passcodes also requires them to reveal the contents of their minds.¹⁶⁷

One court, however, has questioned the relevance of this analogy.¹⁶⁸ While the safe analogy may be useful for physical documents, the court reasoned, it does not translate well to modern phone technology.¹⁶⁹ Unfortunately, the Court did not provide analysis on why it does not translate well.

Fortunately, others have analyzed why this analogy may no longer be applicable. For example, two scholars argue that "[l]ike many attempts to compare the digital and the physical worlds, the safe analogy has some intuitive appeal, but it only tells part of the story."¹⁷⁰ The analogy "only tells part of the story" because phone passcodes encrypt and decrypt the data they protect; safe combinations do not.¹⁷¹ For another scholar, the analogy is unhelpful because it states a truism—obviously, revealing a safe combination is testimonial because it "is a statement of a person's

162. *Id.* at 309–10.

163. *See infra* notes 180, 221. In all of these cases, the courts determined that the act of unlocking a phone was a testimonial communication.

164. *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011* (*Grand Jury Subpoena*), 670 F.3d 1335, 1346 (11th Cir. 2012); *G.A.Q.L. v. State*, 257 So. 3d 1058, 1061 (Fla. Dist. Ct. App. 2018); *Commonwealth v. Davis*, 220 A.3d 534, 548 (Pa. 2019).

165. *E.g., Davis*, 220 A.3d at 548 ("There is no physical manifestation of a password, unlike a handwriting sample, blood draw, or a voice exemplar.").

166. *Grand Jury Subpoena*, 670 F.3d at 1346; *G.A.Q.L.*, 257 So. 3d at 1061; *Davis*, 220 A.3d at 548.

167. *Grand Jury Subpoena*, 670 F.3d at 1346; *G.A.Q.L.*, 257 So. 3d at 1061; *Davis*, 220 A.3d at 548.

168. *State v. Stahl*, 206 So. 3d 124, 135 (Fla. Dist. Ct. App. 2016).

169. *Id.*

170. Price & Simonetti, *supra* note 22.

171. *Id.*

thoughts revealed to the government.”¹⁷² A suspect can decrypt a phone, however, without revealing the passcode to the government.¹⁷³

Another consideration is the difference between unlocking and decrypting a phone. As explained above, most phones today encrypt when they are locked.¹⁷⁴ This means that a phone’s contents are unreadable until a user enters the passcode, which releases a more complex decryption key that makes the contents readable again.¹⁷⁵

However, only two courts have addressed the unlocking/decrypting distinction, and they found that it did not impact the analysis. A federal district court in Washington, D.C., asserted that the distinction is not relevant because decryption “is accomplished by the machine” and there is no evidence that it “requires any mental effort by the [suspect].”¹⁷⁶ Likewise, a Florida district court of appeal held that the distinction “is of no consequence” because decryption “is simply an abbreviated means of decrypting the phone’s contents.”¹⁷⁷ Neither court delved more into the analysis.¹⁷⁸ Thus, this distinction does not seem like it will be dispositive in most cases, but that could change as more courts address this issue.

Regardless of whether a court finds the safe analogy or the unlocking/decrypting distinction persuasive, it will undoubtedly find that unlocking a phone is testimonial because when suspects unlock a phone they communicate that they know the passcode.¹⁷⁹

2. Does the foregone-conclusion doctrine apply?

Next, courts must determine if the foregone-conclusion doctrine applies, thus making the act of production non-testimonial. This issue is where courts differ the most—not just in how they answer the question but also in how they frame the question. Specifically, courts are split on whether, for the exception

172. Kerr, *supra* note 155, at 782.

173. *Id.*

174. See text accompanying *supra* notes 20–37.

175. *Id.*

176. *In re Search of [Redacted]* D.C., 317 F. Supp. 3d 523, 538 (D.D.C. 2018).

177. *G.A.Q.L. v. State*, 257 So. 3d 1058, 1062 n.1 (Fla. Dist. Ct. App. 2018)

178. *Id.*; *In re Search of [Redacted]* D.C., 317 F. Supp. 3d at 538.

179. See *supra* note 156 and accompanying text.

to apply, the forgone conclusion must be the suspect's knowledge of the phone's *passcode* or the suspect's knowledge of the phone's *contents*.

a. Courts that apply the foregone-conclusion doctrine when the government can independently prove that the suspect knows the phone's passcode.

Some courts have held that the foregone-conclusion doctrine applies when the government can independently prove that the suspect knows the phone's passcode.¹⁸⁰ Arguably, when a suspect unlocks a phone, that suspect is only communicating that they

180. *In re State's Application to Compel M.S. to Provide Passcode*, No. A-4509-18T2, 2020 WL 5498590, at *3-4 (N.J. Super. Ct. App. Div. Sept. 11, 2020) (holding that the foregone-conclusion doctrine applies when the suspect's ownership and control of phone is not disputed); *State v. Andrews*, 234 A.3d 1254, 1274 (N.J. 2020) (holding that "although the act of producing the passcodes is presumptively protected by the Fifth Amendment, its testimonial value and constitutional protection may be overcome if the passcodes' existence, possession, and authentication are foregone conclusions"); *State v. Pittman*, 452 P.3d 1011, 1020 (Or. Ct. App. 2019) (holding that the "state did not need to establish, however, that the contents of the iPhone were a foregone conclusion"), *review allowed*, 458 P.3d 1121 (Or. 2020); *Commonwealth v. Jones*, 117 N.E.3d 702, 710 (Mass. 2019) (holding that "the only fact conveyed by compelling a defendant to enter the password to an encrypted electronic device is that the defendant knows the password . . ."); *State v. Johnson*, 576 S.W.3d 205, 227 (Mo. Ct. App.) (holding that foregone conclusion applied because the only "facts conveyed through [the suspect's] act of producing the passcode were the existence of the passcode, his possession and control of the phone's passcode, and the passcode's authenticity"), *transfer denied* (June 25, 2019), *cert. denied*, 140 S. Ct. 472 (2019); *United States v. Spencer*, No. 17-cr-00259-CRB-1, 2018 WL 1964588, at *3 (N.D. Cal. Apr. 26, 2018) (holding that "the government need only show it is a foregone conclusion that [the suspect] has the ability to decrypt the devices"); *In re Search of a Residence in Aptos, California 95003*, No. 17-mj-70656-JSC-1, 2018 WL 1400401, at *6 (N.D. Cal. Mar. 20, 2018) (holding "that if the [suspect's] knowledge of the relevant encryption passwords is a foregone conclusion, then the Court may compel decryption under the foregone conclusion doctrine"); *In re Grand Jury Investigation*, 88 N.E.3d 1178, 1182 (Mass. App. Ct. 2017) (holding that foregone conclusion applied because "the Commonwealth knew that a PIN code was necessary to access the iPhone, that the [suspect] possessed and controlled the iPhone, and that the petitioner knows the PIN code and is able to enter it"); *State v. Stahl*, 206 So. 3d 124, 136-37 (Fla. Dist. Ct. App. 2016) (holding that the Fifth Amendment was not implicated because "the State established, with reasonable particularity, its knowledge of the existence of the passcode, [the suspect's] control or possession of the passcode, and the self-authenticating nature of the passcode"); *Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 615 (Mass. 2014) (holding that the "facts that would be conveyed by the [suspect] through his act of decryption—his ownership and control of the computers and their contents, knowledge of the fact of encryption, and knowledge of the encryption key—already are known to the government and, thus, are a 'foregone conclusion'"); *United States v. Gavegnano*, 305 F. App'x 954, 956 (4th Cir. 2009) (holding that any "self-incriminating testimony that [the suspect] may have provided by revealing the password was already a 'foregone conclusion' because the Government independently proved that [the suspect] was the sole user and possessor of the computer").

know the phone's passcode.¹⁸¹ So, the argument goes, the foregone-conclusion doctrine applies if law enforcement can independently prove that the suspect knows the phone's passcode. If so, the compulsion adds "little or nothing to the sum total of the Government's information,"¹⁸² and the Fifth Amendment is not implicated.

In one of the earlier cases applying this reasoning, *Commonwealth v. Gelfgatt*, the Massachusetts Supreme Judicial Court held that the foregone-conclusion doctrine applied because the Commonwealth could independently prove that the suspect had ownership over the locked devices and knowledge of the devices' encryption keys.¹⁸³ Here, an attorney was arrested on suspicion that he was carrying out a fraudulent mortgage scheme.¹⁸⁴ When he was arrested, law enforcement seized several computers¹⁸⁵ that were encrypted and password protected.¹⁸⁶ Law enforcement officers were not able to circumvent the encryption, and the attorney would not unlock the devices, although he did confirm his ability to decrypt them.¹⁸⁷ The Commonwealth then moved to compel the attorney to decrypt the devices, which the judge denied, citing the Fifth Amendment privilege against self-incrimination.¹⁸⁸

On appeal, the court held that the Fifth Amendment did not protect the attorney from entering the decryption keys because the foregone-conclusion doctrine applied.¹⁸⁹ The court said, "The facts that would be conveyed by the defendant through his act of decryption—his ownership and control of the computers and their contents, knowledge of the fact of encryption, and knowledge of the encryption key—already are known to the government and,

181. Although it may be probable that knowledge of a phone's passcode and knowledge of its contents are synonymous, it is not certain. For example, suspects could have been told the passcode by someone else, or they could have not accessed the phone for some time.

182. *Fisher v. United States*, 425 U.S. 391, 411 (1976).

183. *Gelfgatt*, 11 N.E.3d at 615.

184. *Id.* at 609–10.

185. Although this case is about computers, not phones, the Fifth Amendment analysis is the same.

186. *Gelfgatt*, 11 N.E.3d at 610.

187. *Id.*

188. *Id.* at 611.

189. *Id.* at 615.

thus, are a ‘foregone conclusion.’”¹⁹⁰ In other words, the Commonwealth already knew the attorney could decrypt the computers, so the attorney would not be communicating any new information by entering the passcode. Here, the court is clear that the focus of the analysis should be whether it is a foregone conclusion that the suspect knows the passcode.¹⁹¹

An important question at this stage is how the government can prove it “knows” the suspect can unlock the phone. In some cases, like *Gelfgatt*, suspects may confirm their ability to unlock a phone. In other cases, however, the government may have to prove that knowledge with supplemental evidence. For example, in *State v. Stahl*, a Florida district court of appeal held that the foregone-conclusion doctrine applied because the State proved, via the suspect’s own admissions and phone records, that the suspect knew the phone’s passcode.¹⁹² In *Stahl*, police arrested a man they believed was using his phone to take inappropriate pictures of women.¹⁹³ The man denied taking the pictures and gave police permission to search his iPhone, which was at his house.¹⁹⁴ When the suspect refused to unlock the iPhone, the State moved to compel him to do so.¹⁹⁵ The trial court denied the motion on Fifth Amendment grounds, and the State appealed.¹⁹⁶

On appeal, the court held that the State could compel the suspect to unlock his phone. The court held that the State had “established that it knows with reasonable particularity that the *passcode* exists, is within the accused’s possession or control, and is authentic.”¹⁹⁷ The State established the suspect knew the passcode because he had earlier identified the phone as his, and the phone’s

190. *Id.*

191. *Id.*

192. *State v. Stahl*, 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016).

193. *Id.* at 127.

194. *Id.* at 128.

195. *Id.*

196. *Id.*

197. *Id.* at 136 (emphasis in original). The State established that a passcode exists simply by stating that the phone could not be unlocked without a passcode. *Id.* Further, the court held that, with locked phones, “we must recognize that the technology is self-authenticating—no other means of authentication may exist.” *Id.* In other words, the passcode is authenticated when the suspect enters it into the phone.

number and service provider matched those listed on the suspect's cellphone-carrier records.¹⁹⁸

Similarly, in *Commonwealth v. Jones*, the Massachusetts Supreme Judicial Court listed several pieces of information to support its holding that the Commonwealth had independently proved the suspect's knowledge of the phone's passcode.¹⁹⁹ In *Jones*, the suspect was arrested for trafficking a person for sexual servitude.²⁰⁰ When police arrested the suspect, they seized a locked LG phone from his person.²⁰¹ When the suspect refused to unlock the phone, the Commonwealth moved to compel the suspect to provide the passcode; this was denied.²⁰² On appeal, the court held that the suspect could be compelled to enter the passcode because his knowledge of the passcode was a foregone conclusion.²⁰³

The court relied on several pieces of evidence to find that the suspect's knowledge of the passcode was a foregone conclusion.²⁰⁴ First, the woman who reported the suspect told police that the suspect regularly used an LG phone to contact her.²⁰⁵ She also showed the police her phone, which had the LG's number listed under the suspect's name in her contacts list.²⁰⁶ The subscriber information for the LG had a listed backup number; that backup number belonged to the suspect.²⁰⁷ Using cell-site location records, the police were also able to show that the suspect and the LG were in the same locations at various times.²⁰⁸ Finally, the court found it important that the LG was on the suspect's person when he was arrested.²⁰⁹ The totality of the evidence was enough to convince the court that the suspect had knowledge of the passcode.²¹⁰

To counteract this evidence, the suspect claimed that the Commonwealth had to prove he had *exclusive* control over

198. *Id.*

199. *Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 717 (Mass. 2014).

200. *Id.* at 706.

201. *Id.*

202. *Id.*

203. *Id.* at 707.

204. *Id.* at 717.

205. *Id.*

206. *Id.*

207. *Id.*

208. *Id.*

209. *Id.*

210. *Id.*

the phone.²¹¹ The suspect pointed to evidence that others also used the phone to show that he was not the LG's sole owner.²¹² The court, however, held that the Commonwealth did not have to prove sole or exclusive ownership.²¹³ Rather, it only had to prove the suspect's knowledge of the passcode.²¹⁴

Another important question is the burden of proof that the government must meet. In *Stahl*, the court held that the government has to know that the suspect can unlock the phone, but it does not have to have "perfect knowledge."²¹⁵ Specifically, the court identified the standard as whether the government can know this information with "reasonable particularity."²¹⁶ The court did not expressly define what level this standard is, nor have other courts that have adopted this standard.²¹⁷ Alternatively, some courts have set the standard at "clear and convincing evidence"²¹⁸ or "beyond a reasonable doubt."²¹⁹ However, "reasonable particularity" is the more common standard.²²⁰

211. *Id.*

212. *Id.*

213. *Id.*

214. *Id.*

215. *State v. Stahl*, 206 So. 3d 124, 135 (Fla. Dist. Ct. App. 2016) (quoting *United States v. Greenfield*, 831 F.3d 106, 116 (2d Cir. 2016)).

216. *Id.*

217. *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011 (Grand Jury Subpoena)*, 670 F.3d 1335, 1344 (11th Cir. 2012) ("Where the location, existence, and authenticity of the purported evidence is known with reasonable particularity, the contents of the individual's mind are not used against him, and therefore no Fifth Amendment protection is available."); *In re Search of a Residence in Aptos, California 95003*, No. 17-MJ-70656-JSC-1, 2018 WL 1400401, at *6 (N.D. Cal. Mar. 20, 2018) ("Finally, the government's showing of independent knowledge must be made to the standard of 'reasonable particularity.'"); *State v. Pittman*, 452 P.3d 1011, 1019 (Or. Ct. App. 2019) ("That is why it matters whether the government has identified the documents with 'reasonable particularity' in the subpoena.>").

218. *United States v. Spencer*, No. 17-cr-00259-CRB-1, 2018 WL 1964588, at *3 (N.D. Cal. Apr. 26, 2018) ("The question, accordingly, is whether the government has shown by clear and convincing evidence that [the suspect's] ability to decrypt the three devices is a foregone conclusion.").

219. *Commonwealth v. Jones*, 117 N.E.3d 702, 714 (Mass. 2019) ("[F]or the foregone conclusion to apply, the Commonwealth must prove beyond a reasonable doubt that the defendant knows the password.").

220. This is likely because there is United States Supreme Court and federal circuit court precedent that uses the phrase "reasonable particularity." *United States v. Hubbell*, 530 U.S. 27, 30 (2000); *Grand Jury Subpoena*, 670 F.3d at 1344; *In re Grand Jury Subpoena*, Dated April 18, 2003, 383 F.3d 905, 910 (9th Cir. 2004).

In short, some courts will compel suspects to unlock phones if the government can independently prove that the suspect knows the passcode. Usually, the government must prove this with “reasonable particularity.” This independent knowledge can be proved in a variety of ways. The easiest way is if suspects confirm their ability to unlock a phone. Absent that confirmation, law enforcement can rely on a variety of evidence to prove knowledge of the passcode; for example, the phone was found on the suspect, another person can connect the suspect to the phone, cell-site location records connect the suspect to the phone, and cellphone-carrier records also connect the suspect to the phone.

b. Courts that apply the foregone conclusion doctrine only when the government has demonstrated independent knowledge of the phone’s contents.

Some courts have held that the foregone-conclusion doctrine only applies when the government has demonstrated independent knowledge of the phone’s contents.²²¹ This requires law

221. *Varn v. State*, No. 1D19-1967, 2020 WL 5244807, at *3 (Fla. Dist. Ct. App. Sept. 3, 2020) (holding that the focus of the foregone-conclusion doctrine “is whether the State has identified with reasonable particularity the evidence it seeks within the passcode-protected cell phone”); *Eunjoo Seo v. State*, 148 N.E.3d 952, 958 (Ind. 2020) (holding that the foregone conclusion doctrine did not apply because “the State has failed to demonstrate that any particular files on the device exist or that [the suspect] possessed those files”); *Commonwealth v. Davis*, 220 A.3d 534, 551 n.9 (Pa. 2019) (holding that even if the foregone conclusion-doctrine could apply, the “Commonwealth must establish: (1) the existence of the evidence demanded; (2) the possession or control of the evidence by the defendant; and (3) the authenticity of the evidence”); *Pollard v. State*, 287 So. 3d 649, 657 (Fla. Dist. Ct. App. 2019) (holding that the foregone-conclusion doctrine only applies if “the state can describe with reasonable particularity the information it seeks to access on a specific cellphone. . .”), *reh’g denied* (Dec. 23, 2019), *review dismissed* No. SC20-110, 2020 WL 1491793 (Fla. Mar. 25, 2020); *People v. Spicer*, 125 N.E.3d 1286, 1291 (Ill. App. Ct. 2019) (holding that “the proper focus” of the foregone-conclusion doctrine “is not on the passcode but on the information the passcode protects”); *G.A.Q.L. v. State*, 257 So. 3d 1058, 1063 (Fla. Dist. Ct. App. 2018) (holding that “the object of the foregone conclusion exception is not the password itself, but the data the state seeks behind the passcode wall”); *SEC v. Huang*, No. CV 15-269, 2015 WL 5611644, at *3 (E.D. Pa. Sept. 23, 2015) (holding that the foregone-conclusion doctrine did not apply because the SEC had no evidence that “any of the documents it alleges reside in the passcode protected phones”); *Commonwealth v. Baust*, 89 Va. Cir. 267, 271 (Va. Cir. Ct. 2014) (holding that a phone password was not a foregone conclusion because “it is not known outside of [the suspect’s] mind” and that the Commonwealth could not compel decryption because “the existence and location of the [phone’s contents are] not a foregone conclusion.”); *Grand Jury Subpoena*, 670 F.3d at 1346 (holding that the foregone-conclusion doctrine did not apply because “[n]othing in the record before us reveals that the Government knows whether any files exist and are located on the hard drives . . .”); *In re Boucher (Boucher II)*, No. 2:06-MJ-91, 2009 WL 424718, at *3 (D. Vt. Feb. 19, 2009)

enforcement to describe what information it expects to find on the locked phone. Because only two courts using this approach have concluded that a suspect's knowledge of a phone's content was a foregone conclusion, it is hard to know for certain how much detail a court would require before granting a motion to compel.

The leading case on this approach—which requires law enforcement to prove that the device's contents are a foregone conclusion—is *Grand Jury Subpoena* from the Eleventh Circuit. In this case, law enforcement seized several laptops and external hard drives from the hotel room of a suspected child pornographer.²²² The government was unable to access some portions of the drives, which were encrypted.²²³ So a grand jury issued a subpoena requiring Doe to decrypt the hard drives and any “containers or folders” that might be on the drives.²²⁴ Doe claimed that complying with the subpoena would violate his Fifth Amendment privilege against self-incrimination.²²⁵

The Eleventh Circuit agreed with Doe and held that he could refuse to comply with the subpoena on Fifth Amendment grounds.²²⁶ Specifically, the court held that “the Government has failed to show any basis, let alone shown a basis with reasonable particularity, for its belief that encrypted files exist on the drives, that Doe has access to those files, or that he is capable of decrypting the files.”²²⁷ To successfully compel Doe to decrypt the drives, the government would have to prove that it knew “what, if anything, was hidden behind the encrypted wall.”²²⁸ For example, the government would have to prove the existence and location of files that it expected to find.²²⁹

Most courts that hold the foregone-conclusion doctrine only applies when the government proves independent knowledge of the phone's contents closely follow the Eleventh Circuit's reasoning. For example, in *People v. Spicer*, an Illinois appellate

(holding that the foregone conclusion doctrine applies because the “Government . . . knows of the existence and location of the Z drive and its files”).

222. *Grand Jury Subpoena*, 670 F.3d at 1339.

223. *Id.*

224. *Id.*

225. *Id.*

226. *Id.* at 1349.

227. *Id.*

228. *Id.*

229. *Id.* at 1346.

court carefully tracked the Eleventh Circuit's reasoning. Here, the suspect was a passenger in a vehicle pulled over for speeding.²³⁰ During the stop, officers found cocaine where the suspect was sitting.²³¹ Officers arrested the suspect and, during a search incident to arrest, seized a phone on his person.²³² The suspect refused to provide the phone's passcode, and the State filed a motion to compel him to do so, which was denied.²³³

On review, the court upheld the denial because the State did not establish that the phone's contents were a foregone conclusion.²³⁴ While the State did request categories of information, like call logs and text messages, it did not "identify any documents or specific information."²³⁵ Relying heavily on the Eleventh Circuit's analysis, the court held that the Fifth Amendment protected the suspect from unlocking the phone.²³⁶

One court, however, has applied an even stricter standard than the Eleventh Circuit. In *Commonwealth v. Davis*, the Pennsylvania Supreme Court suggested that a compelled phone unlock would always violate the Fifth Amendment. In *Davis*, police seized the computer of a suspected child pornographer.²³⁷ The computer was locked and encrypted, and the suspect confirmed he was the sole owner of the computer and knew the password.²³⁸ The Commonwealth filed a motion to compel him to unlock the computer, which the trial court granted.²³⁹ However, on appeal, the state supreme court denied the motion.²⁴⁰ Referring to the foregone-conclusion doctrine, the court said: "Indeed, we conclude the compulsion of a password to a computer cannot fit within this exception."²⁴¹ This suggests that the court would, in all situations, find it a Fifth Amendment violation to compel suspects to unlock their phones. The court did, however, note that even if it found the

230. *People v. Spicer*, 125 N.E.3d 1286, 1288–89 (Ill. App. Ct. 2019).

231. *Id.*

232. *Id.*

233. *Id.*

234. *Id.* at 1292.

235. *Id.*

236. *Id.*

237. *Commonwealth v. Davis*, 220 A.3d 534, 538 (Pa. 2019).

238. *Id.*

239. *Id.* at 539.

240. *Id.* at 550.

241. *Id.*

foregone-conclusion doctrine could apply, it would require the Commonwealth to identify the specific files it expects to find on the device.²⁴²

Similarly, in *Eunjoo Seo v. State*, the Indiana Supreme Court detailed three reasons why it believes application of the foregone-conclusion doctrine to phones is “concerning.”²⁴³ In this case, which was explained in the introduction, the State requested permission to compel a suspect to unlock her phone; previously, law enforcement had done a forensic download of the same phone.²⁴⁴ The court denied the request, finding that the State failed to prove “that (1) the suspect knows the password; (2) the files on the device exist; and (3) the suspect possesses those files.”²⁴⁵ Although a detective could describe generally what apps and evidence he expected to find on the phone, the court held this was not enough because the State needed to be able to describe “particular files.”²⁴⁶ The court further said that even if the police could describe particular files, they would be granted access only to those files and not the entire phone.²⁴⁷

After denying the State’s request, the court continued with a discussion of why it found the foregone-conclusion doctrine “concerning” in this context.²⁴⁸ First, the court said that “[s]martphones are everywhere and contain everything” and are thus unlike the business documents that are traditionally covered by the foregone-conclusion doctrine.²⁴⁹ Second, it predicted that allowing the foregone-conclusion doctrine to apply to phones would essentially allow law enforcement “unbridled access” to potential evidence.²⁵⁰ Third, the court argued that U.S. Supreme Court precedent counsels against this application of the doctrine, noting that the “Supreme Court has hesitated to apply even entrenched doctrines to novel dilemmas.”²⁵¹

242. *Id.* at 551 n.9.

243. *Eunjoo Seo v. State*, 148 N.E.3d 952, 958–62 (Ind. 2020).

244. *Id.* at 953–54.

245. *Id.* at 957.

246. *Id.* at 958.

247. *Id.* at 960.

248. *Id.* at 959–62.

249. *Id.* at 959.

250. *Id.* at 960.

251. *Id.* at 961.

Here, the court's reasoning strongly suggests that situations where the foregone-conclusion doctrine would permit law enforcement to compel a phone unlock are exceptional, at least in Indiana.

At the writing of this Note, only two courts had used this foregone-conclusion approach and found that the Fifth Amendment was not implicated.

In *Varn v. State*, the State moved to compel Varn to disclose his cellphone password because it suspected he was transmitting child pornography.²⁵² Because law enforcement officers had already searched the phone of someone that Varn messaged with, they were able to detail what they expected to find on Varn's phone.²⁵³ For example, they could recite texts "verbatim" and give "detailed and graphic descriptions of seven still images and two video screenshots depicting child pornography."²⁵⁴

On review, a Florida district court of appeal held that the specific information the officers provided was enough to satisfy the foregone-conclusion doctrine.²⁵⁵ This was because the officers were able to describe with "reasonable particularity" the evidence it expected to find on the phone.²⁵⁶ Notably, the court said that it would not always require this "level of specificity . . . to trigger the foregone conclusion exception."²⁵⁷ But it did not attempt to explain exactly what level of specificity it requires.²⁵⁸

In *Boucher II*,²⁵⁹ an Immigration and Customs Enforcement Special Agent, trained in recognizing child pornography, searched the laptop of a passenger stopped at the U.S.-Canada border.²⁶⁰ While examining the laptop's contents, the agent identified several files as child pornography.²⁶¹ The agent arrested the passenger and

252. *Varn v. State*, No. 1D19-1967, 2020 WL 5244807, at *2-3 (Fla. Dist. Ct. App. Sept. 3, 2020).

253. *Id.*

254. *Id.* at *3.

255. *Id.* at *4.

256. *Id.* at *3-4.

257. *Id.* at *4.

258. *See id.*

259. This case is labeled *Boucher II* to distinguish it from another case that is discussed later. *See supra* notes 371-379 and accompanying text.

260. *In re Boucher (Boucher II)*, No. 2:06-mj-91, 2009 WL 424718, at *1-2 (D. Vt. Feb. 19, 2009).

261. *Id.* at *2.

shut down the laptop.²⁶² Later, the government tried to re-access the files but could not because the laptop's "Z" drive—where the pornography was located—was encrypted. A grand jury subpoenaed the passenger for the laptop's passcode, but the passenger moved to quash, and the magistrate judge granted the motion.²⁶³

On appeal, the court held that the Fifth Amendment was not implicated because the files sought on the Z drive were a foregone conclusion.²⁶⁴ First, the court noted that, in order for the foregone-conclusion doctrine to apply, the government must establish independent knowledge of the "existence and location" of the files sought.²⁶⁵ The government met that burden, the court concluded, because the agent had already seen the files on the Z drive and could explain them and their location.²⁶⁶ Ultimately, providing access to those files would not add anything to the government's information, and the foregone-conclusion doctrine applied.²⁶⁷

As with the first approach—which focuses on the suspect's knowledge of the passcode—courts focusing on the phone's content must decide what burden of proof the government must meet. The Eleventh Circuit held that the government must be able to describe the device's contents with a "reasonable particularity."²⁶⁸ Unlike the first approach, where there was some variation in the burden of proof, all cases following this approach that identify a burden identify that burden as "reasonable particularity."²⁶⁹ This is likely because, unlike with the first approach, all the cases following this approach have a circuit court decision to follow that clearly defines a burden of proof. As with the first approach, however, courts have not given much guidance on what "reasonable particularity" means.

262. *Id.*

263. *Id.* at *1–2.

264. *Id.* at *3.

265. *Id.*

266. *Id.*

267. *Id.*

268. *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011 (Grand Jury Subpoena)*, 670 F.3d 1335, 1344 (11th Cir. 2012).

269. *In re Boucher (Boucher II)*, No. 2:06-mj-91, 2009 WL 424718, at *3 (D. Vt. Feb. 19, 2009); *People v. Spicer*, 125 N.E.3d 1286, 1290 (Ill. App. Ct. 2019); *Pollard v. State*, 287 So. 3d 649, 657 (Fla. Dist. Ct. App. 2019); *G.A.Q.L. v. State*, 257 So. 3d 1058, 1063 (Fla. Dist. Ct. App. 2018); *SEC v. Huang*, No. 15-269, 2015 WL 5611644, at *3 (E.D. Pa. Sept. 23, 2015).

In review, some courts will not grant a motion to compel a phone unlock unless the government can describe with reasonable particularity the phone's contents. This approach—in comparison to the approach that focuses on the suspect's knowledge of the passcode—makes it less likely that the government will successfully compel the unlock. Because courts almost always find that the foregone-conclusion doctrine does not apply in these scenarios, it is hard to know what evidence is enough. But a court is more likely to find that the foregone-conclusion doctrine applies if the government has actually seen the phone's contents and can therefore describe the content and its location.

c. Courts that have not clearly chosen one approach.

Three courts—an intermediate state court, a federal circuit court, and a federal district court—have not clearly chosen one approach.²⁷⁰

In *Garcia v. State*, a Florida district court of appeal held that the foregone-conclusion doctrine did not apply, but it did not say what the focus of that doctrine should be.²⁷¹ The court first explained that United States Supreme Court precedent does not support applying the foregone-conclusion doctrine when the compelled testimony is *oral* testimony.²⁷² The court had two reasons for this. First, it thought “that it would be imprudent” to extend the doctrine beyond the limited application of *Fisher v. United States*.²⁷³ Second, it believed that the foregone-conclusion doctrine would almost always apply in phone-unlock cases because it is usually clear that the suspect owns the phone.²⁷⁴ This, the court explained, would be a “death knell” to Fifth Amendment protections.²⁷⁵

In the case before the court, the State was compelling the suspect to orally reveal his passcode; thus, the court said the foregone-conclusion doctrine could not apply.²⁷⁶ While the court was clear that the foregone-conclusion cannot apply when a

270. See *Garcia v. State*, No. 5D19-590, 2020 WL 5088056, at *5 (Fla. Dist. Ct. App. Aug. 28, 2020); *United States v. Apple MacPro Comput.*, 851 F.3d 238, 242–44 (3d Cir. 2017); *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012).

271. *Garcia*, 2020 WL 5088056, at *4–5.

272. *Id.* at *4.

273. *Id.*

274. *Id.*

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

276. *Id.* at *5.

suspect is compelled to *orally* reveal a passcode, it did not address other situations – like compelling a suspect to unlock a phone with biometrics or produce a decrypted phone.²⁷⁷

The Third Circuit heard an appeal from a suspect who was held in contempt for failing to comply with an order to decrypt his laptop and external hard drives.²⁷⁸ Because the suspect did not preserve his Fifth Amendment claims in the trial court, the Third Circuit reviewed the lower court's decision for plain error.²⁷⁹

Ultimately, the court held that the lower court did not err in holding the suspect in contempt for failing to comply with the order.²⁸⁰ In a footnote, the court clarified that it was not necessarily concluding that the devices' contents are the correct focus of the foregone-conclusion doctrine.²⁸¹ It also acknowledged that "a very sound argument" can be made that the proper focus is the government's ability to prove the suspect knows the passcode.²⁸² Because its review was limited to plain error, the court clarified that it "need not decide here that the inquiry can be limited to the question of whether [the suspect's] knowledge of the password itself is sufficient to support application of the foregone conclusion doctrine."²⁸³ Thus, in the Third Circuit, at least, the question of the foregone-conclusion doctrine's proper scope is left for another day.

In *United States v. Fricosu*, a federal district court in Colorado held that the foregone-conclusion doctrine applied when the government moved to compel a suspect to produce a decrypted laptop.²⁸⁴ Rather than picking one approach, the court found both that the government had independent knowledge of the existence and location of files on the laptop *and* that the suspect was the sole owner and possessor of the laptop.²⁸⁵

Admittedly, the court in *Fricosu* spent more time explaining the evidence that demonstrated that the suspect could decrypt

277. See *id.* at *5 n.2 (declining to address whether the State could compel a suspect to unlock a phone with biometrics).

278. *Apple MacPro Comput.*, 851 F.3d at 243–44.

279. *Id.* at 244.

280. *Id.* at 249.

281. *Id.* at 248 n.7.

282. *Id.*

283. *Id.*

284. *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012).

285. *Id.*

the laptop.²⁸⁶ The court also held that the government's inability to describe "the specific content of any specific documents is not a barrier to production."²⁸⁷ This may suggest that the court is leaning towards the first approach, which only requires that the government has independent knowledge that the suspect knows the passcode.²⁸⁸ However, the *Fricosu* court cites the *Boucher II* decision—where a federal district court in Vermont held that the phone's contents should be the focus of the foregone-conclusion doctrine—so it is not clear that the court clearly chose one approach.²⁸⁹ It is also possible that because this was an earlier decision (from 2012), and the issue was fairly new, the court did not feel the need to clearly pick one approach. Given the court's ambiguity, this decision does not fall squarely into either of the two main categories.

Another interesting aspect of the *Fricosu* decision is the burden of proof that the court used. Rather than using "reasonable particularity," as many other courts do, the court in *Fricosu* held that the foregone-conclusion doctrine applied based on a "preponderance of the evidence."²⁹⁰ The court did not explain why it chose this standard but simply stated that was the appropriate standard.²⁹¹

d. Is there a clear trend?

As of the writing of this Note, twenty-one cases addressed this issue.²⁹² Of those twenty-one cases, eleven held that the focus of the foregone-conclusion doctrine must be the suspect's knowledge of the passcode.²⁹³ Ten held that the phone's contents must be the focus.²⁹⁴ Three did not clearly choose one approach.²⁹⁵ Courts are therefore far more likely to pick one of the two main approaches. But there is not a clear "majority view." Particularly because the

286. *Id.*

287. *Id.*

288. *Id.*

289. *Id.*

290. *Id.*

291. *Id.*

292. See *supra* notes 180, 221, 270 and accompanying text.

293. See *supra* note 180 and accompanying text.

294. See *supra* note 221 and accompanying text.

295. See *supra* note 270 and accompanying text.

sample size is not large, it would be unwise to claim that one approach is more favored.

Further, there is not a clear trend suggesting that one approach is becoming more popular and that the other is falling out of favor. As Figure 1 shows, this issue became more prevalent starting in 2018. That year, more courts focused on the suspect's knowledge of the passcode. In 2019, three courts focused on the suspect's knowledge of the passcode, while a different three courts focused on the government's knowledge of the phone's contents. In 2020, the courts are likewise evenly split, with one court not clearly choosing one approach. As with above, these numbers do not suggest a particular trend, especially given the small sample size.

Year	Focus of Foregone-Conclusion Doctrine		
	Suspect's knowledge of passcode	Government's knowledge of phone's contents	No clear approach
2009	1 case	1	0
2012	0	1	1
2013	0	0	0
2014	1	1	0
2015	0	1	0
2016	1	0	0
2017	1	0	1
2018	2	1	0
2019	3	3	0
2020	2	2	1

Figure 1

It is also not clear that the type of court is germane. As Figure 2 shows, intermediate state appellate courts are the most likely to address this issue. Also, the different court systems are evenly split—with the exception of the highest state appellate courts, which have one more case deciding that the foregone-conclusion doctrine applies if the government can independently prove that the suspect knows the passcode.

	Focus of Foregone-Conclusion Doctrine		
	Suspect's knowledge of passcode	Government's knowledge of phone's contents	No clear approach
Federal Circuit Court	1 case	1	1
Federal District Court	2	2	1
Highest State Appellate Court	3	2	0
Intermediate State Appellate Court	5	5	1

Figure 2

It is possible that, in the coming years, one approach will trend more and become the majority approach. This would certainly be true if the United States Supreme Court granted certiorari. For now, however, it is difficult to predict how a given court will decide.

B. Phones Protected by Biometrics

Unlike with PINs and alphanumeric passwords, the analysis for biometrics is centered on whether the act is testimonial and not whether the foregone-conclusion doctrine applies. Because biometric passcodes use physical characteristics, multiple courts have held that compelling suspects to unlock their phones with fingerprints is not testimonial, and thus the Fifth Amendment does not apply. Some courts, however, have held that unlocking a phone with a fingerprint is a testimonial communication. The following sections address each approach in turn.

1. Courts that have held biometrics are not testimonial²⁹⁶

Some courts hold that suspects can be compelled to unlock their phones using biometric passcodes.²⁹⁷ The reasoning is that using a biometric is a purely physical act that does not require suspects to divulge the contents of their minds.²⁹⁸ In that regard, suspects can be compelled to unlock their phones via biometrics, just as they can be compelled to stand in a lineup, wear certain clothes, and submit to fingerprinting.

In *Commonwealth v. Baust*, the first case to address a compelled-biometric phone unlock, the Circuit Court of Virginia held that a suspect could not be compelled to produce his phone's passcode.²⁹⁹ He could, however, be compelled to produce his fingerprint to

296. There are only two jurisdictions where courts have held that compelling a suspect to unlock a phone via a PIN or password is a testimonial communication, but that compelling a suspect to unlock a phone via biometrics is not a testimonial communication. *State v. Stahl*, 206 So. 3d 124, 135 (Fla. Dist. Ct. App. 2016); *Commonwealth v. Baust*, 89 Va. Cir. 267, 271 (2014). This contrast is likely not meaningful, however, because all jurisdictions that have addressed PIN and password compulsion have held that there was a testimonial communication. See *supra* Section III.A.1. Thus, a contrast will exist in any jurisdiction where a court holds that biometrics are not testimonial.

297. *In re Search Warrant No. 5165*, No. 5:20-MJ-5165, 2020 WL 3581608, at *10 (E.D. Ky. July 2, 2020) (holding that “[t]he use of biometrics might be compelled and might also be incriminating, but neither of these things make it testimonial”); *In re Search Warrant Application for Cellular Tel. in U.S. v. Barrera*, 415 F. Supp. 3d 832, 839 (N.D. Ill. 2019) (holding that a “biometric procedure is first and foremost a physical act” and thus not testimonial); *In re Search of a White Google Pixel 3 XL Cellphone in a Black Incipio Case*, 398 F. Supp. 3d 785, 794 (D. Idaho 2019) (holding that requiring a suspect to unlock a phone with a fingerprint does not “violate the Fifth Amendment because it does not require the suspect to provide any testimonial evidence”); *In re Search of [Redacted] D.C.*, 317 F. Supp. 3d 523, 540 (D.D.C. 2018) (holding that the compelled use of a suspect's biometric features was non-testimonial); *State v. Diamond*, 905 N.W.2d 870, 875 (Minn. 2018) (holding that “providing a fingerprint to unlock a cellphone is not a testimonial communication under the Fifth Amendment”), *cert. denied*, 138 S. Ct. 2003 (2018); *In re Search Warrant Application for [Redacted Text]*, 279 F. Supp. 3d 800, 801 (N.D. Ill. 2017) (holding that “requiring the application of the fingerprints to the sensor does not run afoul of the self-incrimination privilege because that act does not qualify as a testimonial communication”); *Stahl*, 206 So. 3d at 135 (“Compelling an individual to place his finger on the iPhone would not be a protected act; it would be an exhibition of a physical characteristic, the forced production of physical evidence, not unlike being compelled to provide a blood sample or provide a handwriting exemplar.”); *Baust*, 89 Va. Cir. at 271 (holding that a “fingerprint like a key, however, does not require the witness to divulge anything through his mental processes”).

298. Notably, almost all cases refer specifically to using the suspect's fingerprints. One court, however, gave authorization to compel the suspect's “fingerprints, face, or irises” to unlock any devices found on the searched premises. *In re Search of [Redacted] D.C.*, 317 F. Supp. 3d at 540.

299. *Baust*, 89 Va. Cir. at 271.

unlock the phone.³⁰⁰ This would not implicate the Fifth Amendment because it “does not require the witness to divulge anything through his mental processes.”³⁰¹ Thus, requiring the suspect to put his fingerprint on a phone does not “communicate any knowledge” and is non-testimonial.³⁰²

Similarly, in *State v. Diamond*, the Minnesota Supreme Court listed two reasons for finding that a fingerprint is non-testimonial.³⁰³ First, the suspect was only compelled to provide the fingerprint “for the physical, identifying characteristics of [the suspect’s] fingerprint, not any communicative testimony inherent in providing the fingerprint.”³⁰⁴ So providing the fingerprint was just like standing in a lineup or giving a voice exemplar.³⁰⁵ Second, providing the fingerprint did not reveal the content of the suspect’s mind.³⁰⁶ The court noted that the suspect did not have to self-select what fingerprint would be used³⁰⁷ and could have even been unconscious for the whole process.³⁰⁸

A federal district court in Kentucky also held that biometrics are not testimonial and emphasized their mindless nature.³⁰⁹ The court reasoned that requiring suspects to use their biometrics does not require them to reveal the contents of their minds.³¹⁰ The court explained that even though using biometrics requires suspects to do something, “it requires nothing more than the [suspects] looking in a particular direction or placing their body parts in a certain place.”³¹¹ Thus, the court determined that the Fifth Amendment

300. *Id.*

301. *Id.*

302. *Id.*

303. *State v. Diamond*, 905 N.W.2d 870, 875–76 (Minn. 2018).

304. *Id.* at 875.

305. *Id.* at 875–76.

306. *Id.* at 876.

307. Other courts have found it relevant that law enforcement officers, and not the suspect, selects which fingers are applied to the phone’s sensors. *In re Search of A White Google Pixel 3 XL Cellphone in a Black Incipio Case*, 398 F. Supp. 3d 785, 793 (D. Idaho 2019); *In re Search of [Redacted] D.C.*, 317 F. Supp. 3d 523, 539 (D.D.C. 2018); *In re Search Warrant Application for [Redacted Text]*, 279 F. Supp. 3d 800, 803–804 (N.D. Ill. 2017).

308. *Diamond*, 905 N.W.2d at 877.

309. *In re Search Warrant No. 5165*, No. 5:20-MJ-5165, 2020 WL 3581608, at *10 (E.D. Ky. July 2, 2020).

310. *Id.* at *9.

311. *Id.* at *10.

does not protect suspects from being compelled to unlock their phones via biometrics.³¹²

2. *Courts that have held biometrics are testimonial*

Other courts, however, have held that using biometrics to unlock a phone is a testimonial communication.³¹³ All of these courts emphasize that cellphones are new technology and carry a vast array of invasive, detailed information. Each court's Fifth Amendment analysis, however, is slightly different. For that reason, each case is explained in turn.

In *United States v. Wright*, the most recent case, a federal district court in Nevada held that a suspect's Fifth Amendment rights were violated when law enforcement "forcibly unlocked his smartphone . . . by holding it up to his face."³¹⁴ The court reasoned that "a biometric feature is functionally the same as a passcode, and because telling a law enforcement officer your passcode would be testimonial, so too must the compelled use of your biometric feature to unlock a device."³¹⁵ Here, the court makes it clear that it sees no distinction between a PIN or alphanumeric password and a biometric passcode.

The court offered no commentary on what the government would have to prove in order for the foregone-conclusion doctrine to apply. Arguably, the court would hold that the government only has to prove the suspect knows the passcode because the court said

312. *Id.*

313. *United States v. Wright*, 431 F. Supp. 3d 1175, 1187 (D. Nev. 2020) (holding that "unlocking a phone with your face equates to testimony that you have unlocked the phone before, and thus you have some level of control over the phone"); *In re Search of a Residence in Oakland (Residence in Oakland)*, 354 F. Supp. 3d 1010, 1016 (N.D. Cal. 2019) (holding that "if a person cannot be compelled to provide a passcode because it is a testimonial communication, a person cannot be compelled to provide one's finger, thumb, iris, face, or other biometric feature to unlock that same device"); *United States v. Warrant*, No. 19-mj-71283-VKD-1, 2019 WL 4047615, at *2 (N.D. Cal. Aug. 26, 2019) (holding "that requiring an individual to use a biometric feature to unlock an electronic device so that its contents may be accessed is an act of production that is inherently testimonial in the context of a criminal investigation"); *In re Application for a Search Warrant (Application for a Search Warrant)*, 236 F. Supp. 3d 1066, 1073 (N.D. Ill. 2017) (holding that the use of biometrics to unlock a phone is testimonial because with the "touch of a finger, a suspect is testifying that he or she has accessed the phone before, at a minimum, to set up the fingerprint password capabilities, and that he or she currently has some level of control over or relatively significant connection to the phone and its contents").

314. *Wright*, 431 F. Supp. 3d at 1179.

315. *Id.* at 1187.

that “unlocking a phone with your face equates to testimony that you have unlocked the phone [using a passcode] before, and thus you have some level of control over the phone.”³¹⁶ But that is far from a clear statement.

In *United States v. Warrant*, a federal district court in California held that biometrics could not be compelled unless specific conditions were met.³¹⁷ As in *Wright*, the court here found “no meaningful distinction between unlocking a device with a password and unlocking a device with a biometric feature.”³¹⁸ The court did, however, say that the foregone conclusion doctrine *may* apply if two conditions are met: “(1) the device is found on the person of one of the [suspects]”³¹⁹ and “(2) as to a particular device, law enforcement personnel have information that the particular individual who is compelled to apply his or her biometric feature(s) has the ability to unlock that device, such that his or her ability to unlock the device is a foregone conclusion.”³²⁰

So the court in *Warrant* applied the stricter biometric standard by saying that biometrics are testimonial and thus covered by the Fifth Amendment.³²¹ But the court also used the less strict foregone-conclusion doctrine; that is, the court only required the government to prove that a suspect had the ability to unlock a particular device; it did not require the government to show independent knowledge of the phones’ contents.³²²

In contrast to *Warrant*, a federal district court in Illinois held that the foregone-conclusion doctrine would only apply if the government had independent knowledge of the phone’s contents.³²³ In *Application for a Search Warrant*, the government requested permission to apply the fingerprints of any person found on the search premises to any Apple devices found during the search.³²⁴ The federal district court held that this type of

316. *Id.*

317. *Warrant*, 2019 WL 4047615, at *4.

318. *Id.* at *2.

319. *Id.* at *4.

320. *Id.*

321. *Id.* at *2.

322. *Id.* at *4.

323. *In re Application for a Search Warrant (Application for a Search Warrant)*, 236 F. Supp. 3d 1066, 1074 (N.D. Ill. 2017).

324. *Id.* at 1067.

compulsion did relate a factual assertion.³²⁵ “With a touch of a finger,” the court said, “a suspect is testifying that he or she has accessed the phone before, at a minimum, to set up the fingerprint password capabilities, and that he or she currently has some level of control over or relatively significant connection to the phone and its contents.”³²⁶ Thus, the act of putting a fingerprint on a cellphone’s sensor is a testimonial communication.³²⁷

The court next addressed whether the foregone-conclusion doctrine applied and held that it did not. The court held that in order for the foregone-conclusion doctrine to apply, the government would have to have independent knowledge of the “existence and nature of the electronic information sought.”³²⁸ Because the government did not establish this, the court denied the motion to compel.³²⁹

A federal district court in California used the same reasoning as *Application for a Search Warrant*, but also cast doubt on whether the foregone-conclusion doctrine could ever apply.³³⁰ In *Residence in Oakland*, the government requested a search warrant to seize digital devices found at a home.³³¹ The government also requested permission to compel any individuals at the home to provide their biometrics “for the purposes of unlocking the digital devices found.”³³² The request was not limited to any particular person or device.³³³ The court held that this would be requiring a testimonial communication.³³⁴ The court also noted that this act would be different from other non-testimonial acts—such as submitting to a DNA swab or fingerprinting—for two reasons.³³⁵ First, the biometric features would be serving the same function as a passcode—unlocking a device to secure content.³³⁶ Second, using

325. *Id.* at 1073.

326. *Id.*

327. *Id.*

328. *Id.* at 1074.

329. *Id.*

330. *In re Search of a Residence in Oakland (Residence in Oakland)*, 354 F. Supp. 3d 1010, 1017 (N.D. Cal. 2019).

331. *Id.* at 1013.

332. *Id.*

333. *Id.* at 1014.

334. *Id.* at 1015–16.

335. *Id.* at 1015.

336. *Id.*

biometrics in this way would communicate information, namely that a person has ownership or control over the device.³³⁷

The court also held that the foregone-conclusion doctrine did not apply and that for the doctrine to apply the government would have to show “prior knowledge of the existence or the whereabouts of the documents ultimately produced.”³³⁸ Notably, the court seemed skeptical that this standard could ever be met because smartphones “contain large amounts of data . . . the full contents of which cannot be anticipated by law enforcement.”³³⁹ Ultimately, it is unclear whether this court would ever hold that the foregone-conclusion doctrine does apply.

To summarize, some courts have held that suspects can be compelled to unlock phones using biometrics because biometrics are purely physical characteristics that are non-testimonial. Other courts, however, have held that biometrics are testimonial and will not grant a motion to compel unless the foregone-conclusion doctrine applies. Among the courts holding that biometrics are testimonial, there is no clear consensus on what the government must prove in order for the foregone-conclusion doctrine to apply.

3. Court that has not clearly chosen one approach

There is also a federal district court in Virginia that has not clearly chosen one approach.³⁴⁰ In this case, the government requested permission to unlock a suspect’s phone using either the suspect’s finger or face.³⁴¹ The court acknowledged that other courts are split on whether the use of biometrics is testimonial and said that “[n]o clear consensus has emerged” on this issue.³⁴² The court granted the request, which may suggest that the court decided that using biometrics is not testimonial.³⁴³ But the court did not say the act was nontestimonial.³⁴⁴ Rather, the court stated its

337. *Id.* at 1016.

338. *Id.* at 1017.

339. *Id.*

340. *In re Search Warrant*, 437 F. Supp. 3d 515, 516 (W.D. Va. 2020).

341. *Id.* at 515.

342. *Id.* at 516.

343. *Id.*

344. *Id.*

reasoning for granting the request was that “the data on any electronic device may be lost if not unlocked in a timely manner.”³⁴⁵

Given that all other courts to address this issue have specifically decided whether the act is testimonial or nontestimonial, this case seems more like an outlier than a potential trendsetter.

4. *Is there a clear trend?*

As with PINs and passwords, there is no clear majority approach. Of the thirteen cases addressing these issues, there are: eight cases where the court held that biometrics are not testimonial;³⁴⁶ four cases where the court held that biometrics are testimonial;³⁴⁷ and one case where the court did not clearly choose one approach.³⁴⁸

Although twice as many courts have held that biometrics can be compelled, the sample size is small, and the legal landscape could shift drastically as more cases are decided. There also is not a clear trend in one direction; of the two cases decided in 2020 that clearly chose an approach, one found that biometrics did not implicate the Fifth Amendment, while the other found that they did. As Figure 3 shows, there is no clear trend in one direction:

Year	Not testimonial	Testimonial	No clear approach
2014	1 case	0	0
2016	1	0	0
2017	1	1	0
2018	2	0	0
2019	2	2	0
2020	1	1	1

Figure 3

It is also not clear that court system is germane. As Figure 4 shows, federal district courts are almost evenly split on this issue. Notably, no state appellate courts have held that the use of

345. *Id.*

346. *See supra* note 297 and accompanying text.

347. *See supra* note 313 and accompanying text.

348. *See supra* note 340 and accompanying text.

biometrics is testimonial – only federal district courts have reached that conclusion. But again, it is hard to tell if those trends are meaningful given the small sample size.

	Not testimonial	Testimonial	No clear approach
Federal Circuit Court	0 cases	0	0
Federal District Court	5	4	1
Highest State Appellate Court	1	0	0
Intermediate State Appellate Court	2	0	0

Figure 4

Given the small universe of cases and the varying analysis, it is difficult to surmise how a court addressing this for the first time would decide.

C. Additional Factors That May Influence a Court's Decision

A court may consider other factors, in addition to or as part of the testimonial-communication and foregone-conclusion analyses, when deciding whether to grant a motion to compel. Two important factors that a court may consider are (1) is the prosecutor offering immunity and (2) what specifically the prosecutor wants to compel.

1. Is the prosecutor offering immunity?

Some courts have held that—where a communication *is* testimonial and the foregone-conclusion doctrine *is not* met—the government may still compel a passcode if the suspect is offered immunity. But the caselaw on this issue is sparse and courts have disagreed on what the scope of the immunity should be. Specifically, some courts only require “act-of-production” immunity, while others require “derivative-use” immunity.

Act-of-production immunity only precludes the government from using the suspect's actions to prove the existence, authenticity, and custody of the requested information.³⁴⁹ With this immunity, the government is still able to use the information it collects against the suspect.³⁵⁰ Derivate-use immunity, however, precludes the government from using the information gathered against the suspect.³⁵¹

The Supreme Court, in *United States v. Hubbell*, held that a suspect's Fifth Amendment rights were violated because only act-of-production immunity was offered.³⁵² In this case, a grand jury issued a subpoena requiring Hubbell to turn over eleven categories of documents.³⁵³ Hubbell complied with the subpoena, but only after the government got a court order granting Hubbell immunity.³⁵⁴ A dispute arose, however, regarding the scope of that immunity.³⁵⁵ The government argued that the immunity only covered the act of production—meaning the immunity only precluded the government from using Hubbell's actions to prove the existence, authenticity, and custody of the documents.³⁵⁶ Hubbell, however, argued that the government could also not make derivative use of the documents' contents—meaning the government could not use the documents against him at trial.³⁵⁷

The Supreme Court sided with Hubbell. It held that the documents' contents could not be used against Hubbell in a criminal prosecution unless the government could show "that the evidence it used in obtaining the indictment and proposed to use at trial was derived from legitimate sources 'wholly independent' of the testimonial aspect of respondent's immunized conduct in assembling and producing the documents described in the subpoena."³⁵⁸ Because the government could not make that

349. *United States v. Hubbell*, 530 U.S. 27, 40–41 (2000).

350. *Id.*

351. *Id.* at 32.

352. *Id.* at 45–46.

353. *Id.* at 31.

354. *Id.*

355. *Id.* at 31–32.

356. *Id.* at 40–41.

357. *See id.* at 32.

358. *Id.* at 45.

showing, it could not use the documents against Hubbell, even with the grant of immunity.³⁵⁹

The Eleventh Circuit also held that derivative-use immunity is necessary to protect a suspect's rights.³⁶⁰ Here, the grand jury subpoena required its target, Doe, to produce unencrypted versions of his hard drives.³⁶¹ The U.S. Attorney requested that the court offer Doe immunity, but only for the act of production.³⁶² In other words, the immunity would not prevent the government from using the contents of the hard drives against Doe in a criminal prosecution.³⁶³ The trial court granted the order, which Doe challenged on appeal.³⁶⁴

The Eleventh Circuit agreed with Doe, holding that act-of-production immunity did not suffice to protect his Fifth Amendment rights.³⁶⁵ When it comes to Fifth Amendment rights, the court said, derivative-use immunity is the "critical threshold."³⁶⁶ The court also noted that even if the contents themselves are not testimonial, act-of-production immunity still does not suffice because those contents are still derived from testimonial statements.³⁶⁷ Thus, the government could only compel Doe to turn over the decrypted hard drives if it offered Doe derivative-use immunity.³⁶⁸

In contrast, a federal district court in Colorado held that a suspect could be compelled to produce the decrypted contents of her laptop, in part because the suspect was offered immunity that precluded the government from using her act of production against her.³⁶⁹ But the court in this case also held that the foregone-conclusion doctrine applied, so it is difficult to say how much the grant of immunity affected the case's outcome.³⁷⁰

359. *Id.* at 45–46.

360. *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011 (Grand Jury Subpoena)*, 670 F.3d 1335, 1351–52 (11th Cir. 2012).

361. *Id.* at 1337.

362. *Id.* at 1338.

363. *Id.*

364. *Id.*

365. *Id.* at 1351–52.

366. *Id.* at 1351.

367. *Id.* at 1351–52.

368. *Id.* at 1349–50.

369. *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1238 (D. Colo. 2012).

370. *Id.* at 1237.

In sum, if the foregone-conclusion doctrine does not apply, the government may still be able to compel a phone unlock by offering immunity. The necessary scope of that immunity, however, may differ depending on the jurisdiction. In jurisdictions where the focus of the foregone-conclusion doctrine is just the suspect's knowledge of the passcode, act-of-production immunity may be sufficient. But where the phone's contents are the focus, derivative-use immunity may be required.

2. *What was the suspect compelled to produce?*

Another issue that some courts, and scholars, find important is what specifically the suspect is compelled to do. Suspects can potentially be compelled to disclose the passcode, enter the passcode without disclosing it, or produce a decrypted device. Arguably, if the suspect is compelled to disclose the passcode, verbally or in writing, then the act-of-production doctrine does not apply and the foregone-conclusion doctrine is unavailable. This is because disclosing the passcode would be direct testimony and not a production of an already created document or file.

For example, in *Boucher I*, a grand jury subpoenaed Boucher to enter a passcode to decrypt his hard drive.³⁷¹ The government suggested that Boucher could enter the passcode without "the government, the grand jury, or the Court observing or recording the password in any way."³⁷² Boucher, however, maintained that this would violate his Fifth Amendment rights.³⁷³

A federal district court in Vermont agreed with Boucher; it held that compelling him to enter his passcode was testimonial because it would convey the fact that Boucher knows the passcode and has control over the laptop.³⁷⁴ Next, the court held that the foregone-conclusion doctrine could not apply because a passcode is not a "physical thing," but rather something that exists solely in Boucher's mind.³⁷⁵ The court further explained: "This information is unlike a document, to which the foregone conclusion doctrine usually applies, and unlike any physical evidence the government

371. *In re Boucher (Boucher I)*, No. 2:06-mj-91, 2007 WL 4246473, at *1 (D. Vt. Nov. 29, 2007), *rev'd*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

372. *Id.* at *2.

373. *Id.*

374. *Id.* at *3.

375. *Id.* at *6.

could already know of. It is pure testimonial production rather than physical evidence having testimonial aspects.”³⁷⁶

The government appealed this decision but, learning from its earlier misstep, requested that Boucher hand over the decrypted contents of the hard drive rather than entering his passcode.³⁷⁷ Here, the court did assess the foregone-conclusion doctrine and found that the government had made the requisite showing.³⁷⁸ Thus, the court directed Boucher to produce a decrypted version of his hard drive.³⁷⁹ Ultimately, then, the court was only willing to apply the foregone-conclusion doctrine when the government moved to compel the suspect to produce a decrypted device, but not to disclose his passcodes.

Similarly, in *United States v. Spencer*, a federal district court in California held that a suspect *could* be ordered to turn over his decrypted devices but *could not* be compelled to disclose the devices’ passcodes.³⁸⁰ The court reasoned that requiring Spencer to disclose the passcode “orally or in writing” would be a testimonial communication not covered by the act of production and thus self-incriminating.³⁸¹

In *Garcia v. State*, a Florida district court of appeal was explicit that it would not apply the foregone-conclusion doctrine if the State was trying to compel an *oral* disclosure of a passcode.³⁸² It said “that the foregone conclusion exception or doctrine does not apply to compelled oral testimony.”³⁸³ The court did not address whether it would be willing to compel a suspect to enter a passcode or produce a decrypted device.³⁸⁴

376. *Id.*

377. *In re Boucher (Boucher II)*, No. 2:06-mj-91, 2009 WL 424718, at *1 (D. Vt. Feb. 19, 2009).

378. *Id.* at *3.

379. *Id.* at *4.

380. *United States v. Spencer*, No. 17-cr-00259-CRB-1, 2018 WL 1964588, at *2 (N.D. Cal. Apr. 26, 2018).

381. *Id.* & n.1. Another court said that if the government moved to compel disclosure, the motion “could be considered under the traditional analysis of the self-incrimination privilege—that of verbal communications.” *State v. Stahl*, 206 So. 3d 124, 133 n.9 (Fla. Dist. Ct. App. 2016). The court, however, did not say whether compelling disclosure of the passcode would preclude a foregone-conclusion analysis. *Id.*

382. *Garcia v. State*, No. 5D19-590, 2020 WL 5088056, at *5 (Fla. Dist. Ct. App. Aug. 28, 2020).

383. *Id.*

384. *See id.* at *4-5.

The Massachusetts Supreme Judicial Court, however, held a suspect could be required to enter a passcode, so long as he was not compelled to disclose it orally or in writing.³⁸⁵ This differs from *Boucher I*, where the court held that even compelling a suspect to enter the passcode outside of the government's and court's presence would violate the Fifth Amendment.³⁸⁶

A Massachusetts federal district court took an entirely different approach, holding that requiring a suspect to unlock a phone before surrendering it still violated the Fifth Amendment.³⁸⁷ In *Jimenez*, the government wanted to access the contents of a suspect's phone, but it admitted that forcing the suspect to disclose the passcode would violate the Fifth Amendment.³⁸⁸ So instead the government asked that the suspect be ordered to unlock his phone and then relinquish it.³⁸⁹ The court denied the request, holding that "[w]hether the [suspect] is forced to reveal his passcode or unlock the phone in the presence of law enforcement does not impact the analysis; both situations would force [the suspect] to 'disclose the contents of his own mind' and accordingly are testimonial acts violating the Fifth Amendment."³⁹⁰ Thus, the government's attempts to work around the Fifth Amendment were unsuccessful.

In sum, it could be dispositive that a suspect is being compelled to disclose a passcode, enter a passcode, or produce decrypted content. However, most courts that have addressed compelled phone unlocks have not addressed this specific question. So it is difficult to predict how a court tackling this issue for the first time would consider the methods employed.

IV. RECOMMENDATIONS FOR PROSECUTORS AND LAW ENFORCEMENT

Because phones, especially those that encrypt, are becoming increasingly common, law enforcement officers will likely face more scenarios where they need to collect evidence from a locked phone. This is difficult in jurisdictions where no court has

385. *Commonwealth v. Jones*, 117 N.E.3d 702, 710–11 n.9 (Mass. 2019).

386. *In re Boucher (Boucher I)*, No. 2:06-mj-91, 2007 WL 4246473, at *6 (D. Vt. Nov. 29, 2007), *rev'd*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

387. *United States v. Jimenez*, 419 F. Supp. 3d 232, 233 (D. Mass. 2020).

388. *Id.*

389. *Id.*

390. *Id.*

addressed when suspects can be compelled to unlock a phone. In those jurisdictions, law enforcement and prosecutors have no clear guidance on how to legally collect evidence. Precedent from other jurisdictions, however, can offer suggestions for how to proceed. The following are recommendations for law enforcement officers and prosecutors who would like to compel a suspect to unlock a phone but have no controlling legal guidance on the issue.

First, request to compel the suspect to unlock the device using biometrics.³⁹¹ This is a good starting place because some courts have held that placing a fingerprint on a sensor is no different from standing in a lineup or submitting to a blood draw. Because biometrics are a purely physical key, and do not require the government to access the suspect's mind, there is a persuasive argument that there is no testimonial communication. If the court agrees, then the parties do not even have to address the foregone-conclusion doctrine. Thus, starting with biometrics could solve the problem in a simple way.

There are ways to make a biometric request more likely to succeed. For one, the government can stipulate that it, and not the suspect, will select which fingers to place on the device's sensors. As some courts have noted, this makes this process even more "mindless" for the suspect, making it less likely that the act is testimonial. Further, the government can produce facts that connect the suspect to the phone. This would be helpful if the court is inclined to think that using biometrics is testimonial and an act of production. In this situation, showing that the suspect has possession, control, or ownership of the phone could make the act of production a foregone conclusion. Additionally, some courts have held that it is a Fifth Amendment violation to require everyone at the scene of a search to apply their fingers to any device found. Making a request for a particular suspect to apply their fingers to a specific phone may make the motion more persuasive.

But there are drawbacks to using biometrics. To begin with, biometrics will not always unlock a phone. If the phone has been in police custody for several days, or has not been unlocked for several days, it may not unlock unless a PIN or alphanumeric password is entered. This could be problematic if law enforcement seizes a phone and has to wait for court permission or has to spend

391. See *supra* Section III.B.

time linking the phone to a particular suspect. Also, if a suspect has not entered biometrics into the phone, then biometrics are not an option.

Second, have factual findings connecting the suspect to the phone.³⁹² While this might be helpful in biometrics cases, it is particularly important in cases where the government is trying to compel a PIN or alphanumeric password. Because a court is most likely to find that compelling a passcode is testimonial and an act of production, the government will need to demonstrate that whatever facts the suspect relates are a foregone conclusion. A person who unlocks a phone using a passcode at the very least conveys knowledge of the phone's passcode. Thus, the government should, at a minimum, be able to demonstrate that the suspect knows the passcode. This may also mean demonstrating that the suspect has possession, control, or ownership of the phone.

There are various types of evidence that can demonstrate a suspect knows a passcode. The most compelling evidence is if the suspect admits knowledge of the passcode. But other evidence may be an adequate substitute for that admission. For example, appropriate evidence could include the following: the phone was found on the suspect; the phone is registered in the suspect's name; a third party testifies that the phone belongs to the suspect; the suspect has previously said that he or she can unlock the phone; and phone records connect the phone to the suspect. While a court will perhaps not find any of these dispositive, a combination of them could likely demonstrate that the suspect knows the passcode. The prosecution can also make its motion more compelling by arguing that it has demonstrated the suspect's knowledge with a "reasonable particularity." Since this is the standard that the majority of courts have adopted, other courts may be willing to adopt it as well.

A deficiency of this approach, however, is that a court may not find this evidence sufficient to satisfy the foregone-conclusion doctrine. A court may decide that the government has to prove the phone's contents—and not just the suspect's knowledge of the passcode—are a foregone conclusion. If that is the case, then this evidence will not satisfy the Fifth Amendment.

392. See *supra* Section III.A.2.a.

Third, be able to describe the phone's contents as much as possible.³⁹³ This could be describing messages, photos, or videos that the government expects to find on the phone. It could also be explaining what apps are on the phone and what evidence that app contains. This evidence could be collected if the government has previously seen the phone's contents or has a third party who can describe the contents. The benefit of this approach is that it is the highest standard; if the government can describe the phone's contents, a court is very likely to find that the foregone-conclusion doctrine applies.

This approach, however, will likely frustrate law enforcement in many situations. Scenarios where law enforcement can describe the phone's content may be few and far between. Further, courts vary on how much detail they expect. While many have adopted the "reasonable particularity" standard, that phrase does not lend much help in understanding exactly how much detail a court will require.

Potentially, a court could decide that, because phones contain a vast body of detailed information, the contents can never truly be a foregone conclusion. In other words, there is no possible way that the government could describe the contents of a phone to the point where the government would unlock the phone and not learn any new information. This may be particularly true given the Supreme Court's language in *Riley v. California*. In *Riley*, the Court held that it is generally unconstitutional for law enforcement officers to search the contents of an arrestee's phone without a warrant.³⁹⁴ The Court noted the "immense storage capacity"³⁹⁵ of smartphones and emphasized that "there is an element of pervasiveness that characterizes cell phones but not physical records."³⁹⁶ The Court's warning that smartphones are different from physical records may lead other courts to impose a high standard when it comes to compelling a suspect to unlock a phone.³⁹⁷

393. See *supra* Section III.A.2.b.

394. *Riley v. California*, 573 U.S. 373, 401 (2014).

395. *Id.* at 393.

396. *Id.* at 395.

397. For example, the Indiana Supreme Court, citing *Riley* extensively, cautioned against the "unbridled access" to information that law enforcement would have if able to compel suspects to unlock phones. *Eunjoo Seo v. State*, 148 N.E.3d 952, 959–61 (Ind. 2020). Additionally, at least two other courts have cited *Riley* when establishing that the foregone-conclusion doctrine does not allow the government to compel suspects to unlock phones

Fourth, offer immunity for the act of production.³⁹⁸ For example, stipulate that the government will not prove that the phone belongs to the suspect by entering evidence that the suspect unlocked the phone. If the suspect has immunity, the Fifth Amendment is not implicated because the communication, even if it is compelled and testimonial, is not incriminating. This could help assuage a court's fears that the government has not fully established independent knowledge of a suspect's knowledge of a passcode.

Act-of-production immunity, however, may not be enough for some courts. These courts may require that the government also offer derivative-use immunity—meaning that the prosecution will not use the phone's contents against the suspect at trial. If it is possible to offer this type of immunity without rendering the contents useless, then derivative-use immunity could be offered. But because the prosecution typically wants to access the phone because it believes the contents will be helpful in prosecuting the suspect, derivative-use immunity may not be practical.

Fifth, do not request that the suspect disclose the passcode orally or in writing.³⁹⁹ Requesting that the suspect disclose the passcode may make the foregone-conclusion doctrine unavailable. This is because a court may find that disclosing the passcode is a verbal communication and not an act of production, and the foregone-conclusion doctrine is only available as an exception to the act-of-production doctrine.

If law enforcement has control of the device, the prosecution could request that the suspect enter the passcode. It could also stipulate that the suspect will enter the passcode in privacy, without law enforcement watching or recording. This makes it more likely that the suspect is only relaying information via the

with biometric features. *In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073 (N.D. Ill. 2017); *United States v. Wright*, 431 F. Supp. 3d 1175, 1187 n.9 (D. Nev. 2020). Other courts, however, discussed *Riley* but still found that a suspect could be compelled to unlock a phone via biometrics. *In re* Search of [Redacted] D.C., 317 F. Supp. 3d 523, 539–40 (D.D.C. 2018); *In re* Search Warrant No. 5165, No. 5:20-MJ-5165, 2020 WL 3581608, at *14 (E.D. Ky. July 2, 2020); *In re* Search Warrant Application for Cellular Tel. in *U.S. v. Barrera*, 415 F. Supp. 3d 832, 842 (N.D. Ill. 2019); *In re* Search Warrant Application for [Redacted Text], 279 F. Supp. 3d 800, 806–807 (N.D. Ill. 2017). Thus, some courts may find *Riley* essential to their decision on this issue, while others may not.

398. See *supra* Section IV.C.1.

399. See *supra* Section III.C.2.

act of production, which makes the foregone-conclusion doctrine available.

If law enforcement does not have the phone in custody, it could request that the suspect turn over a decrypted version of the phone. Again, this would be an act of production because the suspect is relaying information through the act of producing evidence.

The difficulty with having the suspect unlock the phone is that it reduces the government's control over the phone. Potentially, the suspect could sabotage the phone. For example, the suspect could repeatedly enter an incorrect passcode until the phone erases all data. Or the suspect could remove data before turning it over. That is a possibility that law enforcement will have to consider.

CONCLUSION

Returning to Hamilton County, and Seo's locked phone, the State moved to compel Seo to unlock her phone.⁴⁰⁰ Seo still refused, and the State moved to hold her in contempt.⁴⁰¹ Seo appealed, claiming her Fifth Amendment privilege against self-incrimination, and the contempt order was stayed.⁴⁰² The court of appeals held that Seo could not be compelled to unlock her phone, but the State appealed.⁴⁰³

The Indiana Supreme Court agreed with the court of appeals, holding that Seo's Fifth Amendment rights would be violated if she were compelled to unlock her phone.⁴⁰⁴ The court chose a strict interpretation of the foregone-conclusion doctrine, explaining that it would only apply if the State could describe the "particular files" on Seo's phone.⁴⁰⁵ But the court did not stop there. Instead, it gave an itemized explanation of why it believes the foregone-conclusion doctrine is ill-suited for compelled-phone-unlock cases.⁴⁰⁶

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

401. *Id.*

402. *Id.*

403. *Id.*

404. *Id.* at 953.

405. *Id.* at 958.

406. *Id.* at 958–62.

Seo demonstrates the complexity of these cases—they involve old law, new technology, constitutional rights, and competing interests. For now, law enforcement officers and prosecutors in jurisdictions without guiding precedent can develop best practices using the available cases.