Penn State Law Review

Volume 126 | Issue 2 Article 7

1-1-2022

Under Digital Lock and Key: Compelled Decryption and the Fifth Amendment

Kirstyn Watson

Under Digital Lock and Key: Compelled Decryption and the Fifth Amendment

Kirstyn Watson*

ABSTRACT

Modern encryption's strength has correlated with its exponential demand to the point that law enforcement cannot decrypt most devices. This level of encryption can leave law enforcement with no practical means of searching a device despite being legally entitled to do so. This issue, dubbed warrant-proof encryption, becomes especially troublesome when safeguarding national security interests or when the investigation of society's most egregious crimes demands that law enforcement officers obtain access to a device's contents. To combat this issue, law enforcement has turned to the court system to compel criminal defendants to unlock their encrypted devices. However, some defendants have argued that this compulsion violates their Fifth Amendment privilege against self-incrimination.

The Fifth Amendment privilege against self-incrimination protects individuals from being compelled by a court to act as a witness against themselves in criminal matters. However, this protection applies only to incriminating testimonial communications. Many courts disagree as to whether defendants' compelled password disclosures or compelled decryption constitutes incriminating testimonial communications that trigger Fifth Amendment protections.

State and federal courts differ in their views of the testimonial nature of passwords and in applying the foregone conclusion exception to compel defendants to disclose their passwords to encrypted devices. Additionally, split decisions over the testimonial nature of compelled password disclosures have fostered further divide regarding the compelled use of biometrics to decrypt devices. Because the United States Supreme Court has not yet directly addressed this issue, this Comment advocates for a uniform rule of law. Ultimately, compelled decryption and biometric security bypasses should not be interpreted as testimonial communications

* J.D. Candidate, The Pennsylvania State University, Penn State Law, 2022

when the foregone conclusion exception applies, therefore exempting them from Fifth Amendment protections.

Table of Contents

I. INTRODUCTION

On a Sunday afternoon in 2014, a woman and her two young children had been shopping at Target when something horrifically unexpected occurred.[1] As she browsed the aisles for Super Glue, a thirty-five-year-old man suddenly crouched to the floor and thrusted his illuminated iPhone beneath her skirt, violating her in front of her children and documenting

1. *See* State v. Stahl, 206 So.3d 124, 127 (Fla. Dist. Ct. App. 2016); Sarah Hagen, *Man Confronted Trying to Get Upskirt Video*, 10 TAMPA BAY WTSP (June 18, 2014, 10:21 PM), https://bit.ly/3pjZRb6 (detailing the video voyeurism issue in *State v. Stahl*).

the entire abhorrent encounter in graphic detail.[2] As she called out for help, the man fled the scene with the images locked away on his cell phone.[3]

Imagine a legal system that would prohibit law enforcement officers from unlocking that man's encrypted cell phone to obtain relevant evidence for his felony prosecution.[4] Prior to the ruling in *State v. Stahl*,[5] many victims of the most heinous crimes occurring in Sarasota, Florida endured that unfortunate reality.[6] The legal uncertainty in Sarasota cleared when the Florida Court of Appeals for the Second District ordered the man responsible for the Target assault, Aaron Stahl, to turn over his passcode so that law enforcement could access the contents of Stahl's cellphone.[7] Because the court compelled Stahl to assist in the decryption of his cellphone, law enforcement successfully brought Stahl to justice for video voyeurism.[8] While law enforcement successfully brought Stahl to justice for video voyeurism, state and federal courts have different viewpoints on the constitutionality of compelled decryption, creating inconsistencies in the law both across state lines[9] and even within individual states.[10] This

2. *See Stahl*, 206 So.3d at 127; Hagen, *supra* note 1.

3. *See Stahl*, 206 So.3d at 127; Hagen, *supra* note 1.

4. *See Stahl*, 206 So.3d at 127; Lorraine Bailey, *Florida Court Denies Protection for iPhone Passcode*, COURTHOUSE NEWS SERV. (Dec. 12, 2016), https://bit.ly/3912EeQ (discussing the *State v. Stahl* case).

5. *See Stahl*, 206 So.3d at 136–37 (holding that the defendant's act of providing a cellphone passcode is not a testimonial communication protected by the Fifth Amendment when the State has proven with reasonable particularity that the passcode exists, is within the defendant's possession, and is authentic).

6. According to Cynthia Meiners, who prosecuted Stahl, prior to the Stahl ruling, pedophiles and child pornographers could "carry around the fruits of [their] crime[s] in front of law enforcement officers, prosecutors and judges and taunt them with fact that they couldn't get the passcode . . . ." Jon Schuppe, *Give Up Your Password or Go to Jail: Police Push Legal Boundaries to Get into Cellphones*, NBC NEWS (June 7, 2019, 4:30 AM), https://nbcnews.to/3olLB0d.

7. *See Stahl*, 206 So.3d at 136–37.

8. *See* Schuppe, *supra* note 6 ("Facing the possibility of getting convicted at trial and sentenced to prison, Stahl agreed to plead no contest in exchange for probation.").

9. *See* State v. Lemmie, 462 P.3d 161, 165 (Kan. 2020) (noting the holding of the trial court that a compelled statement that is not in itself testimonial and, therefore, not protected by the Fifth Amendment, does not become testimonial just because it may lead to incriminating evidence.). *But see* Lewis v. State, 571 S.W.3d 498, 501–03 (2019) (discussing the holding of the trial court that defendants do not have to provide a passcode because they have an absolute right not to incriminate themselves under both the Arkansas Constitution and the United States Constitution).

10. *See Stahl*, 206 So.3d at 136–37 (holding that the defendant's act of providing a cellphone passcode is not a testimonial communication protected by the Fifth Amendment when the State has proven with reasonable particularity that the passcode exists, is within the defendant's possession, and is authentic). *But see* Garcia v. State, 302 So.3d 1051, 1057 (Fla. Dist. Ct. App. 2020) (holding that compelling a defendant to orally provide the passcode to his smartphones constituted a testimonial communication protected under the Fifth Amendment and that "the foregone conclusion exception or doctrine [does] not apply to compelled oral testimony").

Comment explains these inconsistencies and advocates for a uniform rule of law.

Part II of this Comment begins by exploring encryption's necessity in digital security and the investigatory challenges encryption poses to law enforcement.[11] Then, in analyzing a collateral consequence of those investigatory challenges, this Comment examines the security issues associated with backdoors that have prompted law enforcement to seek an alternative to compelling third parties to decrypt devices.[12] Next, Part II examines the Fifth Amendment privilege against self-incrimination in the context of criminal defendants challenging the constitutionality of courts compelling them to decrypt or unlock their personal devices.[13] Part II concludes with a discussion of the state and federal court splits regarding the constitutionality of compelling criminal defendants to decrypt their devices protected by traditional[14] and biometric passwords.[15]

Part III of this Comment analyzes whether compelled decryption violates the Fifth Amendment and contends that neither traditional passwords nor biometric passwords constitute incriminating testimonial communications upon the foregone conclusion exception's satisfaction.[16] Part III also highlights the importance and benefits of a uniform rule of law to avoid arbitrary results and ensure due process for all criminal defendants.[17]

Finally, Part IV of this Comment concludes that passwords and biometric security bypasses should not be interpreted as testimonial communications, especially when the foregone conclusion exception applies, therefore exempting them from Fifth Amendment protections.[18] To resolve the state and federal court splits, Part IV recommends that the United States Supreme Court definitively rules on the compelled decryption issue and applies the foregone conclusion test to require that the government need only prove that the defendant owns the device and knows its password.[19]

II. BACKGROUND

Encryption is a necessary security feature in the digital world, but modern encryption has become so powerful that even law enforcement

11. *See* discussion *infra* Section II.A.
12. *See* discussion *infra* Section II.B.
13. *See* discussion *infra* Section II.C.
14. *See* discussion *infra* Section II.D.1.
15. *See* discussion *infra* Section II.D.2.
16. *See* discussion *infra* Sections III.A, III.B.
17. *See* discussion *infra* Section III.C.
18. *See* discussion *infra* Part IV.
19. *See* discussion *infra* Part IV.

cannot break it.[20] Encryption thus presents a challenge to law enforcement when law enforcement is legally entitled to search an encrypted device but has no practical means of doing so.[21] For example, when law enforcement has a warrant to search a phone but does not know its password, encryption keeps the phone's contents clandestine.[22] To combat the encryption issue, law enforcement has looked to third parties to unlock devices through backdoors[23] and to the judiciary to issue orders to compel criminal defendants to unlock their own devices.[24] However, some defendants have argued that such compulsion violates their Fifth Amendment privilege against self-incrimination.[25]

A. Encryption and Digital Security

Modern devices, such as cellphones and computers, utilize encryption to protect data from unauthorized access.[26] The encryption process begins with plaintext's evolution into ciphertext, which causes the data to become unintelligible without the corresponding encryption key.[27] Essentially, encryption uses an algorithm to scramble data into an unreadable form using three components: (1) "an encryption method[;]"[28] (2) "an encryption key[;]"[29] and (3) "a decryption key[.]"[30]

Encryption is necessary to maintain digital security in the modern world.[31] Almost every aspect of modern life, including personal

20. *See* Riley v. California, 573 U.S. 373, 389 (2014).

21. *See* KRISTIN FINKLEA, CONG. RSCH. SERV., R44481, ENCRYPTION AND THE "GOING DARK" DEBATE 1 (2016) (discussing "warrant-proof encryption").

22. *See id.*

23. See Arjun Kharpal, *Apple vs FBI: All You Need to Know*, CNBC (Mar. 29, 2016, 6:34 AM), https://cnb.cx/3ulybp5.

24. *See generally* Commonwealth v. Davis, 220 A.3d 534 (Pa. 2019); State v. Andrews, 243 N.J. 447 (2020); Commonwealth v. Jones, 481 Mass. 540 (2019).

25. *See generally Davis*, 220 A.3d at 538; *Andrews*, 243 N.J. at 485; *Jones*, 481 Mass. at 541.

26. *See* ROBERT CIESLA, ENCRYPTION FOR ORGANIZATIONS AND INDIVIDUALS: BASICS OF CONTEMPORARY AND QUANTUM CRYPTOGRAPHY 60 (Welmoed Spahr et al. eds., 2020).

27. *See id.*; *see also* Candice Gliksberg, Note, *Decrypting the Fourth Amendment: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Encryption Technologies*, 50 LOY. L.A. L. REV. 765, 769 (2017); Dan Terzian, *The Fifth Amendment, Encryption, and the Forgotten State Interest*, 61 UCLA L. REV. DISCOURSE 298, 302 (2014).

28. *See* CIESLA, *supra* note 26, at 8 ("An encryption method is the mathematical means of how a message or file is scrambled to appear completely random to a third party.").

29. Two main approaches exist for encryption: symmetric and asymmetric. The symmetric approach uses a single key for data's encryption and decryption; whereas asymmetric encryption uses a public key to encrypt data and a separate, private key to decrypt the data. *See id.* at 8–9.

30. *See id.* at 8 ("Only the party with a decryption key (i.e., a password) can access the plaintext contents of the file.").

31. *See id.* at 1.

communications, school, work, socializing, banking, conducting business, and shopping has a digital component.[32] Encryption protects all of these digital communications.[33] Malicious third parties can intercept unencrypted digital communications during their unprotected transmission.[34] After intercepting unencrypted data, those malicious third parties can easily read private communications or access users' confidential information.[35] Among these communications could be financial transactions, trade secrets, or private correspondences that could have devastating consequences if intercepted in their plaintext form.[36] Fortunately, most modern operating systems have built-in encryption solutions that offer users an easy way to achieve a high level of security.[37]

Mobile phones, for example, use encryption,[38] and most default to encrypt data automatically when the user locks the phone.[39] To access this data's plaintext form, users must wield the encryption key, the password, or the resources and knowledge to decrypt the data by cracking the encryption code.[40] The most common authentication mechanisms for mobile devices are traditional passcodes, unlock patterns, and biometrics passwords.[41]

Biometrics "electronically identify[] a person based on his or her physiological or behavioral characteristics."[42] Apple began allowing users to use biometric passwords to unlock their mobile devices with the launch of the fingerprint scanner built into the iPhone 5S in 2013.[43] In addition to fingerprint recognition, biometric identifiers also include facial

32. *See* Gliksberg, *supra* note 27, at 779.

33. *See id.*

34. *See* Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 425 (2012).

35. *See id.*

36. *See id.* (explaining that malicious third parties, like hackers or other bad actors, could steal payments intended for others or create copies of the financial transactions and even attempt to exploit the situation multiple times); *see also* Gliksberg, *supra* note 27, at 779.

37. *See* CIESLA, *supra* note 26, at 60–61.

38. *See* Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 FORDHAM L. REV. 203, 206 (2018).

39. *See id.* at 220.

40. *See* Terzian, *supra* note 27, at 302. When a device is protected by a strong password, cracking its encryption is not feasible. *See id.*

41. *See* Heather Kelly, *Passcode Loyalists Shun ID Advances: As Phones Increase Use of Biometrics, Skeptics Fear Security Risks*, CHI. TRIB. (Nov. 17, 2019), https://bit.ly/3n1kxWE.

42. INT'L COMM. FOR INFO. TECH. STANDARDS INCITS SECRETARIAT, INFO. TECH. INDUS. COUNCIL (ITI), STUDY REPORT ON BIOMETRICS IN E-AUTHENTICATION 25 (2007), https://bit.ly/3HpwGNa.

43. *See* Andy Greenberg, *Apple's New iPhone 'Touch ID' Makes Fingerprint Scans Easy, But Don't Ditch Passcodes Yet*, FORBES (Sept. 10, 2013, 3:28 PM) https://bit.ly/3ppOO0c.

recognition, iris recognition, voice recognition, and hand geometry.[44] Additionally, computer science experts predict new forms of biometric identifiers may be emerging, such as heartbeat, signature, and gait identification.[45] Biometrics appeal to users because of their convenience compared to repeatedly entering a passcode.[46] Not only do biometrics unlock devices faster, but biometric passwords also increase security when compared to passcodes alone, although a combination of the two is ideal.[47]

Despite the necessity of encryption to maintain digital security, encryption also hinders law enforcement's ability to perform its public safety function.[48] When encrypted devices lock, "data becomes protected by sophisticated encryption that renders a phone all but 'unbreakable' unless police know the password."[49] Without obtaining the password from a suspect, a device's encryption renders it practically impenetrable[50] because the government cannot bypass the encryption within a reasonable amount of time.[51] For example, if law enforcement attempted a brute-force attack[52] on the 256-bit encryption used by MacOs,[53] the process would take billions of years.[54] Therefore, law enforcement has sought alternative means to penetrate encryption such as by compelling third parties like Apple and Google to assist in the decryption[55] or by compelling criminal defendants to decrypt their own devices.[56]

---

44. *See id.*

45. *See* Kelly, *supra* note 41.

46. In 2016, Apple released figures stating that iPhone users enter their passcodes approximately 80 times per day. *See id.*

47. *See id.* (noting that most smartphones that employ biometrics still require a passcode or pattern when the user first turns on the phone and in other instances).

48. *See* FINKLEA, *supra* note 21, at 1.

49. Riley v. California, 573 U.S. 373, 389 (2014) (holding that the government cannot conduct a warrantless search of a mobile phone incident to an arrest without exigent circumstances).

50. *See* Andrew J. Ungberg, Note, *Protecting Privacy Through a Responsible Decryption Policy*, 22 HARV. J.L. & TECH. 537, 541 (2009).

51. *See id.*

52. A brute force attack is a method of decryption whereby the person attempting to decrypt the device systematically enters every possible encryption key combination until the correct combination's discovery. *See* CIESLA, *supra* note 26, at 11.

53. *See id.* at 61 (noting that a 256-bit width means that there are 2^{256} or 115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457, 584,007,913,129,639,936 possible key combinations); *see also* 256-Bit Encryption, TECHOPEDIA, https://bit.ly/3CfkBqf (last visited Nov. 14, 2021).

54. *See* Ungberg, *supra* note 50, at 540–41.

55. *See* Kharpal, supra note 23.

56. *See, e.g.*, State v. Stahl, 206 So.3d 124, 127 (Fla. Dist. Ct. App. 2016).

B. *Decryption Through the Use of Backdoors*

Requiring third parties like Apple and Google to weaken encryption or create backdoors creates security vulnerabilities.[57] Weakened encryption would threaten privacy and potentially compromise people's digital identities by providing unauthorized users access to private messages, health records, financial data, location data, or access to a phone's camera and microphone—all without the owner's knowledge.[58] Additionally, a backdoor[59] for law enforcement solves one problem but simultaneously creates another problem, a security vulnerability.[60] Backdoors have the potential to be exploited not only by law enforcement officers who might fail to first obtain proper authorization, but also by malicious actors, hackers, and unfriendly foreign states.[61] To date, no researchers have successfully developed a backdoor that only authorized personnel can access.[62]

Without a feasible means to compel third parties to decrypt devices, law enforcement officers have turned to the courts to compel criminal suspects to unlock their devices in order to allow law enforcement officers to execute their search warrants.[63] However, many defendants argue that their Fifth Amendment privilege against self-incrimination protects them from court-compelled device decryption.[64]

C. *The Fifth Amendment Privilege Against Self-Incrimination*

Pursuant to the Fifth Amendment of the United States Constitution, "No person . . . shall be compelled in any criminal case to be a witness against himself . . . ."[65] The Supreme Court has interpreted this clause, often referred to as the "right against self-incrimination," to prohibit the government from compelling a person into becoming "the deluded

---

57. *See* Shannon Lear, Note, *The Fight Over Encryption: Reasons Why Congress Must Block the Government from Compelling Technology Companies to Create Backdoors into Their Devices*, 66 CLEV. ST. L. REV. 443, 465 (2018).

58. *See id.* at 469.

59. *See* FINKLEA, *supra* note 21, at 4 (defining "backdoor" like a "master key" or "the ability for access by any entity, including a government agency, to encrypted user data without the user's explicit authorization").

60. *See id.*; *see also* Lear, *supra* note 57, at 465 (noting that creating a backdoor "undermines national security because it creates a vulnerability in data security").

61. *See* FINKLEA, *supra* note 21, at 4.

62. *See id.*

63. *See* discussion *infra* Part III.

64. *See* discussion *infra* Section III.B.

65. U.S. CONST. amend. V; *see also* Culombe v. Connecticut, 367 U.S. 568, 581–82 (1961) (noting that the Fifth Amendment's "essence is the requirement that the State which proposes to convict and punish an individual produce the evidence against him by the independent labor of its officers, not by the simple, cruel expedient of forcing it from his own lips").

instrument of his own conviction."[66] The Supreme Court has further interpreted the Fifth Amendment to protect defendants against involuntary confessions[67] and prevent prosecutors from using a defendant's silence as an admission of guilt.[68]

The Supreme Court imposed the protection against self-incrimination on states' criminal procedures through the Fourteenth Amendment.[69] However, the Supreme Court has interpreted the Fifth Amendment privilege against self-incrimination to apply only when the accused person is "compelled to make a testimonial communication that is incriminating."[70] A testimonial communication qualifies as compelled when an authority orders a person, under the threat of a contempt penalty if the person refuses, to speak or act.[71]

To receive Fifth Amendment protections, the compelled act or speech must also be a testimonial communication.[72] The Supreme Court has stated that "in order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a 'witness' against himself."[73] A case's facts and circumstances determine whether a compelled communication qualifies as a testimonial communication under the Fifth Amendment.[74]

Importantly, testimonial communications encompass more than just spoken words or written statements.[75] An act of production[76] can qualify as a testimonial communication if the act concedes the existence,

66. *See Culombe*, 367 U.S. at 581–83 (citing 2 WILLIAM HAWKINS, PLEAS OF THE CROWN 595 (8th ed. 1824)).

67. *See* Malloy v. Hogan, 378 U.S. 1, 8 (1966).

68. *See* Griffin v. California, 380 U.S. 609, 615 (1965).

69. *See* U.S. CONST. amend. XIV ("No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law."); *see also Culombe*, 367 U.S. at 582–83; *Malloy*, 378 U.S. at 8 (holding that the right against self-incrimination is incorporated through the Fourteenth Amendment, which means that state courts shall not infringe upon the privilege against self-incrimination just as federal courts shall not infringe upon the Fifth Amendment).

70. Fisher v. United States, 425 U.S. 391, 408 (1976) (holding that the court did not violate the Fifth Amendment by compelling the defendants' attorneys to produce the defendants' accounting records in a tax evasion case).

71. *See* State v. Hall, 65 Wis. 2d 18, 30–31 (1974).

72. *See Fisher*, 425 U.S. at 408.

73. Doe v. United States, 487 U.S. 201, 210 (1988) (holding that the Fifth Amendment privilege against self-incrimination did not excuse the petitioner for failing to provide incriminating business documents because producing the documents was not a testimonial communication).

74. *See Fisher*, 425 U.S. at 410 (noting that there are no categorical answers to the questions of whether "tacit averments" are testimonial or incriminating).

75. *See id.* at 411.

76. *See id.* at 409 (distinguishing an act of production from oral testimony).

possession and control, or authenticity of a document or object that tends to incriminate.[77] However, physical acts that do not require defendants to use the contents of their minds or disclose their knowledge are nontestimonial.[78] For example, displaying physical characteristics like providing samples of fingerprints;[79] saliva, hair, and blood;[80] standing in a lineup;[81] making a particular gesture;[82] and donning particular articles of clothing,[83] or committing physical acts like creating handwriting[84] or voice samples,[85] are not testimonial communications because they are "not coterminous with communications that relay facts."[86]

In addition to a communication's compulsion and testimonial nature, the Supreme Court requires that communications must also be incriminating for the Fifth Amendment to apply.[87] The United States Supreme Court categorizes testimony as incriminating when the witness reasonably believes that the testimony could be used in a criminal proceeding or lead to the discovery of other evidence that could be used in a criminal proceeding.[88] However, the Fifth Amendment's privilege against self-incrimination does not forbid the compelled production of all incriminating evidence, only compelled testimonial communications.[89]

---

77. *See id.* at 410.

78. *See* State v. Andrews, 243 N.J. 447, 466 (2020).

79. *See* United States v. Wade, 388 U.S. 218, 223 (1967).

80. *See* Schmerber v. California, 384 U.S. 757, 761 (1966).

81. *See Wade*, 388 U.S. at 221 ("Neither the lineup itself nor anything shown by this record that [the defendant] was required to do in the lineup violated his privilege against self-incrimination.").

82. *See id.* at 223.

83. *See* Holt v. United States, 218 U.S. 245, 252–53 (1910) ("[T]he prohibition of compelling a man in a criminal court to be witness against himself is a prohibition of the use of physical or moral compulsion to extort communications from him, not an exclusion of his body as evidence when it may be material.").

84. Although an individual's voice and handwriting are types of communication, not "every compulsion of an accused to use his voice or write compels a communication within the cover of the privilege. A mere handwriting exemplar, in contrast to the content of what is written, like the voice or body itself, is an identifying physical characteristic outside its protection." Gilbert v. California, 388 U.S. 263, 266–67 (1967).

85. *See* United States v. Dionisio, 410 U.S. 1, 5–6 (1973) ("It has long been held that the compelled display of identifiable physical characteristics infringes no interest protected by the privilege against compulsory self-incrimination.").

86. State v. Andrews, 243 N.J. 447, 466 (2020); *see also* United States v. Hubbell, 530 U.S. 27, 35 (2000) (holding that the Fifth Amendment's privilege against self-incrimination prevents the State from compelling a defendant to admit the existence of and produce incriminating documents if the State is unable to describe the documents with reasonable particularity).

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

88. *See* Hiibel v. Sixth Jud. Dist. Ct of Nev., 542 U.S. 177, 190 (2004) (holding that the Fifth Amendment "protects against any disclosures that the witness reasonably believes could be used in a criminal prosecution or could lead to other evidence that might be so used").

89. *See Fisher*, 425 U.S. at 408.

Even if a court compels a defendant to make a compelled, incriminating testimonial communication, the communication does not necessarily trigger the Fifth Amendment's privilege against self-incrimination because the foregone conclusion exception may still apply.[90]

The foregone conclusion exception stipulates that an act of production does not violate the Fifth Amendment so long as the government already knew the facts conveyed by the act.[91] The foregone conclusion exception requires the State to establish its knowledge of: (1) the existence of the evidence; (2) the defendant's possession or control of the evidence; and (3) the authenticity of the evidence.[92] Though the foregone conclusion test appears straightforward, courts inconsistently apply the exception's test to compelled decryption cases.[93]

D. The Fifth Amendment's Case Law Regarding Compelled Decryption

State and federal courts reach inconsistent conclusions regarding Fifth Amendment protections, or lack thereof, in the context of compelling defendants to unlock their encrypted and lawfully seized devices.[94] When analyzing Fifth Amendment protections for encrypted devices, courts typically differ in two ways: (1) their views of the testimonial nature of traditional passwords and biometric passwords;[95] and (2) their interpretations of whether the foregone conclusion doctrine compels defendants to disclose their passwords to encrypted devices.[96]

---

90. *See id.* at 411.

91. *See id.* (noting that the individual must contribute "little or nothing to the sum total of the Government's information"); *see also Hubbell*, 530 U.S. at 35.

92. *See Fisher*, 425 U.S. at 411. For example, the State can establish that a defendant's ownership or control over a mobile phone is a foregone conclusion by proving facts such as the billing information being in the defendant's name, the defendant listing the phone number as his own on unrelated documents, and the cell site location information corroborating the defendant's presence at certain locations. *See* Commonwealth v. Jones, 481 Mass. 540, 545 (2019).

93. *See* discussion *infra* Sections II.D.1.c, II.D.1.d.

94. *See generally* Commonwealth v. Davis, 220 A.3d 534, 543 (Pa. 2019) (holding that compelling a defendant to disclose his computer password violates the Fifth Amendment because a password disclosure is an incriminating testimonial communication and the foregone conclusion exception does not apply to the compelled oral disclosure of passwords); State v. Andrews, 243 N.J. 447, 466 (2020).(holding that requiring a defendant to disclose his cellphone password did not violate the Fifth Amendment because a password disclosure is a testimonial act but is permissible under the foregone conclusion exception).

95. *See* discussion *infra* Sections II.C.

96. *See* discussion *infra* Sections II.C.

1. Traditional Passwords and Passcodes

The Supreme Court has not definitively ruled on whether compelling a defendant to disclose a password or decrypt a password-protected device constitutes a testimonial communication.[97] Accordingly, both state courts[98] and federal courts[99] have reached different conclusions about the testimonial nature of passwords.

a. Some Courts Hold That Passwords Are Not Incriminating Testimonial Communications

Various state and federal courts, including the Fourth Circuit, have held that passcodes are not inherently testimonial or incriminating.[100] In addition to the Fourth Circuit, state courts in Florida,[101] Kansas,[102] and Nevada[103] have held that passwords are either not inherently testimonial or not incriminating.

In *United States v. Oloyede*,[104] the defendant participated in a conspiracy to defraud elderly victims on online dating sites.[105] At the request of a federal law enforcement officer and without being *Mirandized*,[106] the defendant entered the password to her locked iPhone out of the officer's view.[107] The officer requested the device's decryption pursuant to a valid search warrant's execution.[108] The court ruled that the

97. *See Davis*, 220 A.3d at 543.

98. *See* Lewis v. State, 571 S.W.3d 498, 501–03 (Ark. Ct. App. 2019) (holding defendants do not have to provide a passcode because defendants have an absolute right not to incriminate themselves under the Arkansas Constitution and the United States Constitution). *But see* State v. Lemmie, 462 P.3d 161, 165 (Kan. 2020) (holding that a compelled statement that is not in itself testimonial and, therefore, not protected by the Fifth Amendment does not become testimonial just because it may lead to incriminating evidence.).

99. *See* United States v. Oloyede, 933 F.3d 302, 308 (4th Cir. 2019) (holding that the act of entering a passcode is not a testimonial communication). *But see* United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1346 (11th Cir. 2012) (holding that the decryption of hard drives is testimonial in nature).

100. *See Oloyede*, 933 F.3d at 308; *Lemmie*, 462 P.3d at 165; Mickelson v. State, No. 78513, 2020 WL 5837973, at *1 (Nev. Sept. 30, 2020); State v. Stahl, 206 So.3d 124, 127 (Fla. Dist. Ct. App. 2016).

101. *See Stahl*, 206 So.3d at 127.

102. *See Lemmie*, 462 P.3d at 165.

103. *See Mickelson*, 2020 WL 5837973 at *1

104. *Oloyede*, 933 F.3d 302 (4th Cir. 2019).

105. *See id.* at 306–07.

106. The Miranda Rule requires that people who are detained or taken into police custody are advised of their constitutional rights to remain silent and to legal representation prior to any questioning or making any statements. *See* Miranda v. Arizona, 384 U.S. 436, 478–79 (1966). A person's un-Mirandized statements are presumptively inadmissible against them in later proceedings. *See Miranda Rule*, BLACK'S LAW DICTIONARY (11th ed. 2019).

107. *See Oloyede*, 933 F.3d at 308.

108. *See id.*

act was not a testimonial communication because the defendant merely used the "the unexpressed contents of her mind" to unlock the device.[109] Because the defendant never communicated the phone's unique password to the federal law enforcement agent, the court reasoned that the act of entering a password was more akin to "surrendering a key to a strongbox" than "telling an inquisitor the combination to a wall safe."[110] The court further reasoned that, despite the lack of Miranda warnings, the self-incrimination clause "cannot be violated by the introduction of nontestimonial evidence obtained as a result of voluntary statements."[111]

Florida's Second District Court of Appeals similarly held that compelling a defendant to disclose his cellphone password did not violate the Fifth Amendment because the password had no testimonial significance.[112] Specifically, in *State v. Stahl*, the court held that a defendant's password does not have testimonial significance.[113] The court further reasoned that a compelled non-testimonial statement cannot become testimonial simply because it might lead to incriminating evidence.[114] State courts in Kansas have similarly ruled that non-testimonial compelled statements do not become testimonial simply because they might lead to incriminating evidence.[115]

The Supreme Court of Nevada took a different approach and found that passcodes are not incriminating in *Mickelson v. State*.[116] Travis Mickelson shot a firearm at a group of Sikh men, and after hitting one of the men, Mickelson fled the scene.[117] Later, law enforcement arrested Mickelson and convinced him to decrypt his phone by entering the passcode.[118] Law enforcement subsequently obtained a warrant to search Mickelson's phone and found recorded phone calls in which Mickelson

109. *See id.* at 309 (citing United States v. Hubbell, 530 U.S. 27, 43 (2000)) (noting that *United States v. Hubbell* "distinguish[es] 'surrender[ing] the key to a strongbox,' which is not communicative, from 'telling an inquisitor the combination to a wall safe,' which is communicative").

110. *See id.*

111. *Id.* at 309–10.

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

113. *See id.* at 134 ("In this case, the communication was sought only for its content and the content has no other value or significance . . . . Providing the passcode does not 'betray any knowledge [the defendant] may have about the circumstances of the offenses' for which he is charged.")

114. *See id.*

115. *See* State v. Lemmie, 462 P.3d 161, 165 (Kan. 2020) (noting the holding of the trial court that "[t]he production of the password and the pass code is a nonfactual statement in this Court's view that merely facilitated the production of evidence for which the State had already obtained a warrant based upon evidence independent of the defendant's statements . . . .").

116. *See* Mickelson v. State, No. 78513, 2020 WL 5837973, at *1 (Nev. Sept. 30, 2020).

117. *See id.* at *1.

118. *See id.*

confessed to the crime and made racial remarks about the Sikh men.[119] The court held that "[a] cellphone passcode is not inherently incriminating" especially when the phone's ownership is undisputed.[120] However, some courts disagree on passwords being inherently testimonial or incriminating.

b. Other Courts Hold That Passwords Are Incriminating Testimonial Communications

Various state and federal courts, including the Third and Eleventh Circuits, have held that passwords are incriminating testimonial communications.[121] Courts that follow this logic have held that passwords and decryption cannot be compelled unless the foregone conclusion exception is satisfied; although, courts disagree as to the requirements needed to satisfy the exception and whether it should apply to passwords.[122]

In *Lewis v. State*,[123] the Arkansas Court of Appeals took a singularly unique approach and did not analyze whether compelling a defendant to produce a password is a testimonial communication or whether the compulsion falls within the foregone conclusion exception.[124] Rather, the court merely asserted that defendants have the absolute right to not incriminate themselves and to not provide their passcode to law enforcement.[125]

In *State v. Pittman*,[126] the Oregon Supreme Court held that unlocking a passcode-protected phone is an incriminating testimonial communication.[127] The court reasoned that unlocking a passcode-protected phone communicates that the defendant knows the passcode and

119. *See id.*

120. *See id.*

121. *See* United States v. Apple Mac Pro Comput., 851 F.3d 238, 248 (3d Cir. 2017); United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1346 (11th Cir. 2012); State v. Pittman, 367 Ore. 498, 518 (2021); Lewis v. State, 571 S.W.3d 498, 501–03 (Ark. Ct. App. 2019); Commonwealth v. Davis, 220 A.3d 534, 543 (Pa. 2019); State v. Andrews, 243 N.J. 447, 466 (2020).

122. *See generally Davis*, 220 A.3d at 543 (holding that compelling a defendant to disclose his computer password violates the Fifth Amendment because a password disclosure is an incriminating testimonial communication and the foregone conclusion exception does not apply to the compelled oral disclosure of passwords); *Andrews*, 243 N.J. at 466 (holding that requiring a defendant to disclose his cellphone password did not violate the Fifth Amendment because a password disclosure is a testimonial act but is permissible under the foregone conclusion exception).

123. Lewis v. State, 571 S.W.3d 498, 501–03 (Ark. Ct. App. 2019).

124. *See id.*

125. *See id.*

126. State v. Pittman, 367 Ore. 498 (2021).

127. *See id.* at 518.

knows how to access the contents of the phone.[128] However, the court distinguished passcode-protected phones from biometric-protected phones because a phone protected by fingerprint recognition would only require the defendant to demonstrate that she knew how to move her finger.[129] Therefore, the court can only require the defendant to unlock her phone if the foregone conclusion exception applies.[130]

c. Some Courts Hold That the Foregone Conclusion Doctrine Applies to Passwords

The Third[131] and Fourth[132] Circuits, as well as state courts in Florida,[133] Massachusetts,[134] New Jersey,[135] Illinois,[136] Indiana,[137] and Maine[138] have held that compelling defendants to unlock encrypted devices or provide passwords is not a testimonial communication when the foregone conclusion exception is satisfied.[139] These courts'

128. *See id.* at 517–18.

129. *See id.*

130. *See id.* at 533–34.

131. *See* United States v. Apple Mac Pro Comput., 851 F.3d 238, 241 (3d Cir. 2017).

132. *See* United States v. Oloyede, 933 F.3d 302, 306 (4th Cir. 2019); United States v. Gavegnano, 305 F. App'x 954, 955 (4th Cir. 2009).

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

134. *See* Commonwealth v. Jones, 481 Mass. 540, 545 (2019); Commonwealth v. Gelfgatt, 468 Mass. 512, 514 (2014) (holding that "the act of decryption" is not a testimonial communication when the foregone conclusion exception applies).

135. *See* State v. Andrews, 243 N.J. 447, 456 (2020).

136. *See* People v. Johnson, 90 N.E.3d 634, 636 (Ill. App. Ct. 2017) (acknowledging the trial court's holding that the foregone conclusion exception applies to passcodes and holding that the defendant was in direct civil contempt of court when, in defiance of a court order, she did not unlock her cellular phone due to allegedly forgetting her passcode).

137. *See* Seo v. State, 148 N.E.3d 952, 953 (Ind. 2020). The court reasoned that "giving law enforcement an unlocked smartphone communicates to the State, at a minimum, that (1) the suspect knows the password; (2) the files on the device exist; and (3) the suspect possesses those files." *See id.* at 955. The court further reasoned that absent evidence that the State can demonstrate that it already knows the information it is seeking, the foregone conclusion exception does not apply. *See id.*

138. *See* State v. Trant, 2015 Me. Super. LEXIS 272 (2015) (holding that even though a passcode is testimonial in nature, compelling production of a passcode does not offend the Fifth Amendment provided that the elements of the foregone conclusion exception are met).

139. *See* United States v. Oloyede, 933 F.3d 302, 309 (4th Cir. 2019).

interpretations do not require reasonable particularity[140] to satisfy the foregone conclusion exception.[141]

In *United States v. Apple Mac Pro Computer*,[142] the Third Circuit held that requiring a defendant to produce his lawfully seized devices in a "fully unencrypted state" did not violate the Fifth Amendment and that the foregone conclusion exception applies to encrypted devices.[143] The court reasoned that the foregone conclusion exception applied because "the affidavit supporting the application for the search warrant established that (1) the Government had custody of the devices; (2) prior to the seizure, [the defendant] possessed, accessed, and owned all devices; and (3) there [were] images on the electronic devices that constitute child pornography."[144] Therefore, "any potentially testimonial component of the act . . . 'adds little or nothing to the sum total of the Government's information.'"[145]

Like the Third Circuit, the Fourth Circuit held that compelling passwords is permissible under the Fifth Amendment using the same standard for the foregone conclusion exception.[146] In *United States v. Gavegnano*,[147] the Fourth Circuit held that a defendant's Fifth Amendment right against self-incrimination was not violated when, upon request and after he invoked his *Miranda* rights, the defendant revealed his computer password.[148] The court reasoned that the foregone conclusion exception applied "because the Government independently proved that [the defendant] was the sole user and possessor of the computer."[149]

---

140. The reasonable particularity standard requires the State to prove more than its knowledge of the existence of the evidence, the defendant's ownership or control of the evidence, and the authenticity of the evidence. *See* United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1346 (11th Cir. 2012). The standard also requires the State to prove with "reasonable particularity" that the State already knows the contents of the evidence. *See id.*; *see also* United States v. Ponds, 454 F.3d 313, 320–21 (D.C. Cir. 2006); *In re* Grand Jury Subpoena, 383 F.3d 905, 910 (9th Cir. 2004).

141. *See* United States v. Apple Mac Pro Comput., 851 F.3d 238, 248 (3d Cir. 2017); *Oloyede*, 933 F.3d at 319; United States v. Gavegnano, 305 F. App'x 954, 956 (4th Cir. 2009); State v. Stahl, 206 So.3d 124, 135 (Fla. Dist. Ct. App. 2016); Commonwealth v. Jones, 481 Mass. 540, 561 (2019); Commonwealth v. Gelfgatt, 468 Mass. 512, 519 (2014); State v. Andrews, 243 N.J. 447, 471 (2020); People v. Johnson, 90 N.E.3d 634, 638 (Ill. App. Ct. 2017).

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

143. *See id.* at 248.

144. *Id.*

145. *Id.* at 247.

146. *See* United States v. Gavegnano, 305 F. App'x 954, 956 (4th Cir. 2009).

147. *See id.*

148. *See id.* ("Any self-incriminating testimony that he may have provided by revealing the password was already a 'foregone conclusion . . . .'").

149. *See id.*

In *State v. Andrews*,[150] the New Jersey Supreme Court held that compelling a defendant to disclose his cellphone password did not violate the defendant's Fifth Amendment privilege against self-incrimination.[151] The defendant was a law enforcement officer suspected of aiding a narcotics dealer in avoiding criminal exposure by revealing the identity of an undercover police officer.[152] The State obtained a warrant to search the defendant's iPhones but could not access the phones without the defendant's passcodes.[153] The court ordered the defendant to disclose the passcodes, reasoning that the act of giving the password was more akin to surrender than testimony.[154] The court further reasoned that the passwords had little evidentiary value and were merely pathways to access lawfully obtained evidence.[155]

d. Other Courts Hold the Foregone Conclusion Exception Does Not Apply to Passwords or Additional Requirements Must Be Satisfied

Conversely, a state court in Pennsylvania[156] declined to extend the foregone conclusion exception to passwords.[157] The Eleventh Circuit[158] and a Virginia state court[159] have required that the forgone conclusion exception requires evidence beyond the defendant's ownership of the device and knowledge of its password.[160]

The Supreme Court of Pennsylvania held in *Commonwealth v. Davis*[161] that compelling a defendant to disclose the computer password to his lawfully-seized, encrypted computer violated the defendant's Fifth Amendment right against self-incrimination.[162] The court reasoned that compelling a defendant to disclose a password constitutes an incriminating testimonial communication because such a compulsion requires

150. State v. Andrews, 243 N.J. 447 (2020).

151. *See id.* at 485.

152. *See id.* at 456.

153. *See id.*

154. *See id.* at 480–81. ("Based on the record [in this case], we have little difficulty concluding that compelled production of the passcodes falls within the foregone conclusion exception . . . . The State's demonstration of the passcodes' existence, [defendant's] previous possession and operation of the cellphones, and the passcodes' self-authenticating nature render the issue one of surrender, not testimony.").

155. *See id.* at 481.

156. *See* Commonwealth v. Davis, 220 A.3d 534, 550 (Pa. 2019).

157. *See id.*

158. *See* United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1346 (11th Cir. 2012).

159. *See* Commonwealth v. Baust, 89 Va. Cir. 267, 271 (2014).

160. *See generally Davis*, 220 A.3d at 550; Seo v. State, 148 N.E.3d 952, 953 (Ind. 2020).

161. *See Davis*, 220 A.3d at 550.

162. *See id.* at 548.

defendants to recall contents of their minds that imply facts that will incriminate them.[163] Furthermore, the court declined to extend the foregone conclusion exception, as applied to documents, to require the compelled disclosure of passwords.[164] However, the court noted in dicta that nonverbal communications would not have the same protections as verbal communications.[165]

Interestingly, Justice Max Baer's dissenting opinion in *Commonwealth v. Davis* argued that the act was not a testimonial communication[166] and that the foregone conclusion exception should have applied.[167] Justice Baer reasoned that the government did not ask the defendant to "speak his guilt" but instead to merely "allow the government to execute a warrant that it lawfully obtained."[168] Additionally, the dissent argued that the majority's argument would fail if the device had a biometric password such as a fingerprint, facial recognition, or iris scan because such acts of production do not require defendants to make use of their minds' contents.[169]

The Eleventh Circuit[170] added extra requirements to the foregone conclusion exception when it held that compelling passwords violates the

163. *See id.*

164. *See id.* at 550 ("[W]e construe the foregone conclusion rationale to be one of limited application, and, consistent with its teachings in other decisions, believe the exception to be inapplicable to compel the disclosure of a defendant's password to assist the Commonwealth in gaining access to a computer.")

165. *See id.* at 548 ("Distilled to its essence, the revealing of a computer password is a verbal communication, not merely a physical act that would be nontestimonial in nature.").

166. Even if an act of production has testimonial aspects, the compulsion of the act is not necessarily precluded by the Fifth Amendment's privilege against self-incrimination. *See id.* at 554 (Baer, J., dissenting). "[T]he compulsion of Appellant's password is an act of production, requiring him to produce a piece of evidence similar to the act of production requiring one to produce a business or financial document, as occurred in *Fisher*." *Id.* (Baer, J., dissenting).

167. Justice Baer thought the foregone conclusion should have applied to passwords because "it was a foregone conclusion that the government knew that the password to decrypt the files existed, that Appellant had exclusive control over the password, and that the password was authentic." *See id.* at 558 (Baer, J., dissenting). The foregone conclusion exception should apply because "the testimonial aspects of the password disclosure 'adds little or nothing to the sum total of the government's information.'" *See id.* (Baer, J., dissenting).

168. *See id.* at 555 (Baer, J., dissenting). The Commonwealth already possessed evidence of the defendant's guilt, which was required to obtain the warrant to search the defendant's laptop. *See id.* (Baer, J., dissenting).

169. *See id.* at 557 (Baer, J., dissenting) ("Under those circumstances, the individual is not using the contents of his mind but, rather, is performing a compelled act of placing his finger or face in the appropriate position to decrypt the files.").

170. *See* United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1346 (11th Cir. 2012).

Fifth Amendment if the reasonable particularity standard is not met.[171] In *United States v. Doe*,[172] the Eleventh Circuit held that compelling a defendant to produce unencrypted data on his password-protected laptops and external hard drives[173] violated the Fifth Amendment.[174] The Eleventh Circuit reasoned that an act of production can be testimonial when the "act conveys some explicit or implicit statement of fact that certain materials exist, are in the subpoenaed individual's possession or control, or are authentic."[175]

The Eleventh Circuit also outlined two situations in which an act of production is not testimonial.[176] First, when the Government compels a physical act that does not require defendants to access their minds' contents, the Fifth Amendment is not implicated.[177] Such an act would be like providing "the key to the lock of a strongbox containing documents" because defendants would not have to provide anything from their minds.[178] Second, the Fifth Amendment is not implicated if the Government can demonstrate with "reasonable particularity" that the information was a foregone conclusion, even if the act conveys information about the existence, location, possession, or authenticity of the subpoenaed materials.[179]

In *Commonwealth v. Baust*, a Virginia state court interpreted the foregone conclusion exception completely differently and held that disclosing passcodes always constitutes testimonial communications protected by the Fifth Amendment.[180] This is true regardless of whether the government can prove the defendant's ownership of the device and prove with reasonable particularity what will be discovered on the device.[181] In *Baust*, the defendant recorded himself committing a violent

171. *See generally* United States v. Doe, 670 F.3d 1335, 1346–49 (11th Cir. 2012) (holding that compelling passwords violates the Fifth Amendment when the reasonable particularity standard is not met); Seo v. State, 148 N.E.3d 952, 955 (Ind. 2020) (holding that absent evidence that the State can demonstrate that it already knows the information it is seeking, the foregone conclusion exception does not apply).

172. *See Doe*, 670 F.3d at 1352.

173. External hard drives are portable, supplemental storage devices for computers. *See* Meira Gebel, *What Is an External Hard Drive? One Of the Best Ways to Protect Your Important Files, Explained*, BUS. INSIDER, https://bit.ly/3iVpWe4 (last visited Jan. 27, 2021).

174. *See Doe*, 670 F.3d at 1346–49.

175. *Id.* at 1345 (citing Curcio v. United States, 354 U.S. 118, 128 (1957)) ("The touchstone of whether an act of production is testimonial is whether the government compels the individual to use 'the contents of his own mind' to explicitly or implicitly communicate some statement of fact.").

176. *See id.*

177. *See id.*

178. *See id.*

179. *See id.* at 1345–46.

180. *See* Commonwealth v. Baust, 89 Va. Cir. 267, 271 (2014).

181. *See id.* at 269.

assault and transmitted the recording to the victim on his smartphone.[182] The Virginia Circuit Court held that although the defendant could be compelled to unlock the smartphone with his fingerprint, the court could not compel the defendant to produce his password.[183] The court reasoned that the password could not be considered a foregone conclusion because the password didn't exist anywhere else outside the defendant's own mind.[184] The Virginia court differed from other courts in its interpretation of the foregone conclusion doctrine by focusing on whether the password itself was a foregone conclusion, rather than whether the defendant's control of the device or the evidence on the device was a foregone conclusion.[185]

2. Biometric Passwords

Just as courts are divided regarding the testimonial nature of compelled password disclosures, courts are also split on the compelled use of biometrics to decrypt devices.[186] While the majority of courts view biometric passwords as nontestimonial communications,[187] the minority of courts view them as testimonial.[188]

a. The Majority View

Most courts have held that compelling defendants to unlock their encrypted devices using biometric passwords does not violate the Fifth Amendment.[189] In *State v. Diamond*,[190] the Minnesota Supreme Court held that police did not violate the defendant's Fifth Amendment rights when he provided them with his fingerprint to unlock his cellphone.[191] The court reasoned that the act of unlocking the phone did not constitute a testimonial communication because "the compelled act [of providing a fingerprint] elicited only physical evidence from [the defendant's] body and did not reveal the contents of his mind."[192]

182. *See id.* at 267.
183. *See id.* at 270–71.
184. *See id.* at 271.
185. *See id.* ("[I]f the password was a foregone conclusion, the Commonwealth would not need to compel Defendant to produce it because they would already know it.").
186. *See* discussion *infra* Sections II.D.2.a, II.D.2.b.
187. *See* discussion *infra* Section II.D.2.a.
188. *See* discussion *infra* Section II.D.2.b.
189. *See* State v. Diamond, 905 N.W.2d 870, 872 (Minn. 2018); United States v. Barrera, 415 F. Supp. 3d 832, 842 (N.D. Ill. 2019); *In re* Search Warrant No. 5165, 470 F. Supp. 3d 715, 726 (E.D. Ky. 2020).
190. *See* State v. Diamond, 905 N.W.2d 870 (Minn. 2018).
191. *See id.* at 872.
192. *See id.*

Similarly, in *United States v. Barrera*,[193] the Illinois Northern District Court held that requiring defendants to scan their biometrics does not violate the Fifth Amendment.[194] Specifically, the court held that compelling defendants to press their fingers to the iPhone home button to unlock their device is permissible under the Fifth Amendment.[195] The court cited three factors in its determination.[196] First, the court reasoned that a finger is more akin to a key than a combination.[197] "[I]n the context of an iPhone, a finger is a modern substitute for a key."[198] The court reasoned that a key, like a finger, is a physical object that requires no communication of mental thoughts or information from within a defendant's mind.[199] Second, the act of pressing a finger to the home button is more akin to a physical act than testimony.[200] Third, the implicit inference of ownership drawn from the defendant unlocking a phone does not amount to a testimonial communication.[201]

In the case of *In re Search Warrant No. 5165*,[202] the Kentucky Eastern District Court held that using biometric identifiers to unlock a device does not constitute a testimonial communication; however, in order to obtain a warrant, the government must have: (1) reasonable suspicion that the suspect being compelled to provide their biometrics committed a criminal act; and (2) reasonable suspicion that the suspect's biometrics would

193. United States v. Barrera, 415 F. Supp. 3d 832 (N.D. Ill. 2019).

194. *See id.* at 842.

195. *See id.*

196. *See id.* at 838–39 ("(1) [W]hether the biometric unlock is more like a key than a combination; (2) whether the biometric unlock is more like a physical act than testimony; and (3) whether the implicit inferences that arise from the biometric unlock procedure is sufficient to be of testimonial significance under the Fifth Amendment.").

197. *See id.* at 839; *see also 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).

198. *Barrera*, 415 F. Supp. 3d at 839.

199. *See id.*

200. The biometric procedure does not require any verbal statement and "such a forcing is 'compulsion of the accused to exhibit his physical characteristics, not compulsion to disclose any knowledge he might have.'" *See id* at 839–40; *see also* United States v. Wade, 388 U.S. 218, 222 (1967).

201. In nearly any compelled physical act, an incriminating inference can be drawn. *See Barrera*, 415 F. Supp. 3d at 841. For example, an incriminating inference exists when a defendant surrenders a key to a strongbox when the defendant had possession of the key and access to the strongbox. *See id.* Additionally, a defendant who provides a handwriting exemplar suggests an incriminating inference that the defendant knows how to write. *See id.* However, neither of those actions are sufficient to establish legal testimonial significance. *See id.* Therefore, although an incriminating inference can be drawn that a defendant whose fingerprint opens an iPhone at one point had possession of and access to the phone, the act does not rise to the level of a testimonial communication. *See id.* Additionally, because iPhones can store up to five fingerprints, the implicit inference is insufficient to suggest that the defendant had exclusive control over or access to the phone. *See id.*

202. *See In re* Search Warrant No. 5165, 470 F. Supp. 3d 715 (E.D. Ky. 2020).

unlock the device.[203] The warrant at issue in the case of *In re Search Warrant* sought to permit law enforcement to compel "all individuals present at the [premises]" to use their biometric identifiers to unlock "any [electronic devices]" which could be opened with biometrics.[204] Although the court held that the warrant was overbroad, the court also reasoned that "pursuant to controlling Supreme Court case law, compelled biometrics are not testimonial."[205] Although biometrics might be compelled and might be incriminating in certain instances, neither of those conditions make the conduct testimonial.[206]

b. The Minority View

A magistrate judge in the California Northern District Court held that biometric features used to unlock electronic devices are testimonial under the Fifth Amendment's privilege against self-incrimination.[207] The judge distinguished providing a biometric password from providing a fingerprint or DNA sample for two reasons.[208] First, the judge reasoned that a biometric password is "functionally equivalent" to a traditional passcode and should receive equal treatment under the law.[209] Second, the judge reasoned that unlike using a fingerprint sample as physical evidence to compare the defendant's fingerprints to the fingerprints found at the crime scene, the act of unlocking a phone concedes that the suspect, at one point in time, possessed or controlled the device.[210]

Like the California Northern District Court, the Nevada District Court also held that displaying a biometric identifier constitutes a testimonial communication.[211] In the Nevada District Court, the judge held that law enforcement violated the defendant's Fifth Amendment rights

203. *See id.* at 735.

204. *Id.* at 720.

205. *Id.* at 729. Although using biometric technology may require physical action, using biometrics does not require defendants to express the contents of their minds. *See id.* Therefore, "[t]he only thought that can be inferred and attributed to the person is that [they] affirmatively looked at a phone screen." *Id.*

206. *See id.* ("When deciding whether an act is testimonial or not, the governing case law simply does not take into account the power or immediacy of the incriminating inference acquired from the physical characteristic."); *see also In re* Search Warrant Application, 279 F. Supp. 3d 800, 805 (N.D. Ill. 2017).

207. *See In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1015 (N.D. Cal. 2019).

208. *See id.*

209. *See id.* 1015–16 ("It follows, however, 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.").

210. *See id.* at 1016 ("[A] successful finger or thumb scan confirms ownership or control of the device, and, unlike fingerprints, the authentication of its contents cannot be reasonably refuted.").

211. *See* United States v. Wright, 431 F. Supp. 3d 1175, 1181 (D. Nev. 2020).

when officers forcibly unlocked the defendant's smartphone by holding the phone to the defendant's face to bypass the device's facial recognition unlocking mechanism.[212] The court reasoned that the implied assertion that the defendant had control over the phone because he could unlock it with his face was testimonial for purposes of the Fifth Amendment.[213] These cases demonstrate the lack of uniformity in the law regarding compelled decryption for biometric-protected devices.[214]

III. ANALYSIS

Compelling criminal defendants to decrypt their devices pursuant to a court order has been held constitutional by several courts.[215] These courts correctly interpret the Fifth Amendment, and their holdings should be universally applied so that criminal defendants in all jurisdictions can be compelled to decrypt their devices pursuant to a court order without violating the Constitution.[216] In order to resolve the state and federal court splits, the United States Supreme Court should expeditiously rule on this issue.[217] In most cases, traditional passwords are not incriminating testimonial communications because of the foregone conclusion exception, and, therefore, do not implicate the Fifth Amendment's privilege against self-incrimination.[218] Additionally, the logic used by courts that have ruled that compelling biometric passwords violates the Fifth Amendment has many shortcomings, portraying both a technical misunderstanding of encryption and biometric keys as well as a legal misunderstanding of the Fifth Amendment.[219] Lastly, a uniform rule of law is necessary to prevent differing results for similar compulsions across jurisdictions and to uphold due process and equal protection.[220]

A. Passwords Are Not Incriminating Testimonial Communications

Passwords do not constitute incriminating testimonial communications triggering Fifth Amendment protections, even without applying the foregone conclusion exception.[221] As technology advances,

212. *See id.* at 1179.
213. *See id.* at 1186.
214. *See id.*; *In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1015 (N.D. Cal. 2019). *But see* State v. Diamond, 905 N.W.2d 870, 878 (Minn. 2018); United States v. Barrera, 415 F. Supp. 3d 832, 842 (N.D. Ill. 2019); *In re* Search Warrant No. 5165, 470 F. Supp. 3d 715, 735 (E.D. Ky. 2020).
215. *See* Commonwealth v. Gelfgatt, 468 Mass. 512, 519 (2014); State v. Andrews, 243 N.J. 447, 466 (2020).
216. *See* discussion *infra* Sections III.A, III.B.
217. *See* discussion *infra* Sections III.A, III.B.
218. *See* discussion *infra* Section III.A.
219. *See* discussion *infra* Section III.B.
220. *See* discussion *infra* Section III.C.
221. *See* State v. Stahl, 206 So.3d 124, 127 (Fla. Dist. Ct. App. 2016).

the continued viability of the key-combination dichotomy articulated in the dissenting opinion of *Doe v. United States*[222] becomes increasingly questionable.[223] When analyzing alphanumeric passwords following *Doe*, courts have grappled with whether identifying the key which will open a strongbox is actually distinct from telling an officer the combination which will open a safe.[224] Compelling a key's production requires three acts, only one of which is cognitive: "remembering the key's location, retrieving it, and producing it."[225] Producing a decrypted device requires the same number of acts and cognition: "remembering the password, entering it, and producing the decrypted drive."[226] Providing the sequence of numbers that will unlock an encrypted phone is no different than identifying the key that will open a strongbox from a keyring with hundreds of possible keys.[227] Therefore, while the key-combination dichotomy provides a pithy analogy, its arbitrariness provides little help in distinguishing testimonial and nontestimonial acts.[228]

Some courts have adopted the key logic in finding that passcodes are nontestimonial because they are nonfactual statements that merely facilitate the production of evidence but have no evidentiary value in and of themselves.[229] Using similar reasoning, other courts have found that passcodes are not inherently incriminating.[230]

Even if revealing a passcode constitutes an incriminating testimonial communication because of the implied assertion that the passcode knower has ownership or control over the device, the testimonial value of passcodes is limited to the defendant's ownership and control of the device.[231] Therefore, the foregone conclusion exception can easily be satisfied if law enforcement proves that the defendant had ownership or control over the device. Any testimonial inference that can be drawn from the defendant's knowledge of the passcode adds nothing that the government was unable to prove prior to the unlocking. No additional

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

223. *See Stahl*, 206 So.3d at 135.

224. *See id.*

225. Terzian, *supra* note 27, at 310.

226. *Id.*

227. *See id.* at 310–11.

228. *See id.* at 311.

229. *See* State v. Lemmie, 462 P.3d 161, 165 (Kan. 2020) (noting the trial court's holding).

230. *See* Mickelson v. State, No. 78513, 2020 WL 5837973, at *1 (Nev. Sept. 30, 2020). The Supreme Court of Nevada held that evidence obtained from a defendant's cellphone did not violate the defendant's Fourth or Fifth Amendment rights when the defendant voluntarily provided the police officer with the passcode. *See id.* The court reasoned that a cell phone passcode is not inherently incriminating, particularly when the phone was retrieved from the suspect's pocket and he never disputed his ownership over the phone. *See id.*

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

evidence, such as reasonable particularity of the device's contents, should be required in a Fifth Amendment analysis because reasonable particularity has no relevance in determining testimonial significance.[232] The reasonable particularity standard requires the State to establish more than what the Supreme Court requires to satisfy the forgone conclusion exception, thus inventing an entirely new and arbitrary standard.[233]

B. Biometrics Are Not Incriminating Testimonial Communications

Biometric keys, like fingerprints and facial recognition, should not implicate the Fifth Amendment because both constitute nontestimonial acts of production that do not require individuals to access their mind's contents.[234] Providing these biometric keys is no different than providing handwriting[235] or voice samples;[236] providing saliva, hair, or blood samples;[237] or providing the key to a strong box.[238] Courts prohibiting compelled biometrics ignore the technical realities of biometric passwords and Supreme Court precedent.[239]

First, courts that prohibit compelled biometrics ignore the fact that biometric passwords are typically used in conjunction with alphanumeric passcodes, rather than in lieu of alphanumeric passcodes.[240] This shows a technical misunderstanding of biometric technology because electronic devices generally cannot be programmed with biometric passwords without first programming a passcode.[241] Often a passcode is required even after the biometric feature has been programmed, such as when the device is first turned on.[242]

Second, biometric passcodes are not testimonial communications because they do not require defendants to make use of their minds'

232. *See id.* at 411 (holding that the State need only establish the defendant's ownership of the evidence, the defendant's control or possession of the evidence, and the evidence's authenticity for the foregone conclusion exception to apply).

233. *See id.*

234. *See* State v. Andrews, 243 N.J. 447, 466 (2020).

235. Although an individual's voice and handwriting are types of communication, not "every compulsion of an accused to use his voice or write compels a communication within the cover of the privilege. A mere handwriting exemplar, in contrast to the content of what is written, like the voice or body itself, is an identifying physical characteristic outside its protection." *See* Gilbert v. California, 388 U.S. 263, 266–67 (1967).

236. *See* United States v. Dionisio, 410 U.S. 1, 5–6 (1973) ("It has long been held that the compelled display of identifiable physical characteristics infringes no interest protected by the privilege against compulsory self-incrimination.").

237. *See* Schmerber v. California, 384 U.S. 757, 761 (1966).

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

239. *See In re* Search Warrant No. 5165, 470 F. Supp. 3d 715, 731 (E.D. Ky. 2020) ("Where other district courts have prohibited compelled biometrics, they have favored a pragmatic (rather than legalistic) approach.").

240. *See id.*

241. *See id.*

242. *See id.*

contents.[243] Although entering passcodes can potentially lead to incriminating evidence, the fact remains that a nontestimonial act of production cannot trigger the Fifth Amendment's privilege against self-incrimination merely because it *could* lead to incriminating evidence.[244] The Supreme Court's requirement that the compelled communication be "testimonial" in order for the Fifth Amendment privilege to apply differs from the requirement that the communication be "incriminating."[245] Therefore, courts that prohibit compelled biometrics falsely equate the "testimonial" and "incriminating" requirements of the Fifth Amendment's self-incrimination clause.[246]

Third, the argument that the act of unlocking a phone with a fingerprint scan "far exceeds" the physical evidence generated from a traditional fingerprinting is "simply untrue."[247] The fact that unlocking a phone happens much faster than running a fingerprint through a biometric database or conducting an expert analysis "is of no consequence in the Fifth Amendment analysis."[248] When deciding whether an act is testimonial or not, the governing case law does not consider the power or immediacy of the incriminating inference drawn.[249]

Lastly, the argument that using biometrics makes refuting device ownership impossible has two flaws.[250] First, although a key to a lockbox is more likely to be borrowed, found, or stolen[251] than a fingerprint that unlocks a phone, the person whose fingerprint unlocks a device could still refute ownership.[252] The distinction between key and fingerprint speaks only "to the incriminatory nature of the possession of the object" and not to the testimonial nature of the compulsion.[253] Although possessing the fingerprint that opens a locked device might have a more incriminating implication than possessing a key that opens a strongbox, the level of

243. *See id.* at 732 ("Although the conclusion reached in *Oakland* and others has practical justifications, the decision never resolves how the physical act of placing your finger on a screen, for example, communicates the mental thoughts and impressions of a target to convert such actions into testimonial acts.").

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

245. *See In re* Search of [Redacted] Washington, 317 F. Supp. 3d 523, 536 (2018).

246. *See In re* Search Warrant No. 5165, 470 F. Supp. 3d 715, 731 (E.D. Ky. 2020).

247. There are only two possibilities when a defendant uses a biometric identifier to unlock a device. If the match is positive, the device permits access. If the match is negative, the device does not permit access. Therefore, the information revealed by a positive biometric match does not "far exceed" the physical evidence generated by a traditional positive fingerprint match, except the result's instantaneous nature. *See id.* at 732–33.

248. *See id.* at 733.

249. *See In re* Search Warrant Application, 279 F. Supp. 3d 800, 805 (N.D. Ill. 2017) ("If the act does not inherently contain a communication from the person, then no testimony has been obtained from the person.").

250. *See In re* Search of [Redacted] Washington, 317 F. Supp. 3d at 536.

251. *See id.* at 535–36.

252. *See id.*

253. *See id.* at 535–36 n.9.

"incriminatory power" has no relevance in determining the compulsion's testimonial status.[254] Second, because an iPhone can store up to five fingerprints, the implicit inference drawn from a defendant unlocking one does not necessarily assume the defendant's exclusive control or access to the phone.[255] Therefore, a defendant unlocking a device does not axiomatically equate to ownership and can still be refuted.[256]

C. Advocating for a Uniform Rule of Law

Courts must apply the Fifth Amendment's privilege against self-incrimination uniformly to prevent absurd results[257] and to uphold due process and equal protection.[258] A Supreme Court ruling allowing the government to compel defendants to unlock their devices with both alphanumeric passcodes and biometric indicators would achieve both of these policy goals.[259]

Forever preventing the government from compelling the decryption of password-protected devices would lead to arbitrary and absurd results.[260] The determining factor in whether the government could compel a defendant to unlock an encrypted device would be whether the defendant protected the device using a fingerprint key or an alphanumeric password.[261] The method of unlocking should not be determinative of whether the Fifth Amendment will be implicated.[262]

---

254. *See id.* 535–36.

255. United States v. Barrera, 415 F. Supp. 3d 832, 840 (N.D. Ill. 2019).

256. *See id.*

257. *See* discussion *infra* pp. 603–04.

258. *See* discussion *infra* pp. 604–06.

259. *See* discussion *infra* pp. 606–07.

260. *See* United States v. Spencer, No. 17-cr-00259-CRB-1, 2018 U.S. Dist. LEXIS 70649, at *5 (N.D. Cal. Apr. 26, 2018).

261. *See id.* "Similarly, accepting the analogy to the combination-protected safe, whether a person who receives a subpoena for documents may invoke the Fifth Amendment would hinge on whether he kept the documents at issue in a combination safe or a key safe." *Id.* However, this distinction should not impact the legal outcome because either way, unlocking the safe does not require producing the combination to the State. *See id.*

262. *See id.* at *5–6.

Without a uniform rule of law from the United States Supreme Court, state courts[263] and federal courts[264] apply the provisions of the United States Constitution differently. The inconsistent application of the Fifth Amendment to similarly situated individuals violates equal protection and due process.

For example, two Florida counties—located just approximately 137 miles from each other—apply the United States Constitution to criminal defendants in different ways.[265] In Sarasota County, the act of providing a passcode is not a testimonial communication, and even if it were, the foregone conclusion exception applies;[266] however, in Orange County, the foregone conclusion exception does not apply to compelled oral testimony.[267] Accordingly, Florida residents' constitutional rights vary depending on their county.[268]

---

263. *See* Pollard v. State, 287 So.3d 649, 657 (Fla. Dist. Ct. App. 2019). The First District held that compelling a defendant to disclose a passcode to a cellphone is a testimonial communication. *See id.* Furthermore, the State cannot invoke the foregone conclusion exception unless the state can describe with reasonable particularity the information it seeks to access on a specific cellphone. *See id.* On the assumption that the foregone conclusion exception applies to core testimonial communications, such as a compelled oral disclosure of a password, it is not applicable in this case because the state failed to identify with particularity and certainty what information existed beyond the password-protected cellphone wall; mere inference that evidence may exist is not enough. *See id. But see* State v. Stahl, 206 So.3d 124, 134 (Fla. Dist. Ct. App. 2016). The Second District held that the act of providing a cellphone password is not a testimonial communication protected by the Fifth Amendment. *See id.* The court further reasoned that even if it were a testimonial communication, the foregone conclusion exception would apply because the state could prove, with reasonable particularity, that the passcode exists, is within the accused's possession or control, and is authentic. *See id.* at 136; G.A.Q.L. v. State, 257 So.3d 1058, 1061–62 (Fla. Dist. Ct. App. 2018). The Fourth District held that requiring a defendant to disclose his cell phone's passcode violated his Fifth Amendment rights because the password was a testimonial communication. *See id.* The court further reasoned that the foregone conclusion exception does not apply because the state failed to show with reasonable particularity knowledge of the evidence within the phone. *See id.* at 1059; Garcia v. State, 302 So.3d 1051, 1057 (Fla. Dist. Ct. App. 2020). Florida's Fifth District Court held that compelling a defendant to orally provide the passcode to his smartphones constitutes a testimonial communication protected under the Fifth Amendment and that the foregone conclusion exception does not apply to compelled oral testimony. *See id.*

264. *See* United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1352–53 (11th Cir. 2012) (holding that compelling passwords violates the Fifth Amendment when the reasonable particularity standard is not met). *But see* United States v. Apple Mac Pro Comput., 851 F.3d 238, 248 (3d Cir. 2017) (holding that requiring a defendant to produce his lawfully seized devices in a fully unencrypted state did not violate the Fifth Amendment and that the foregone conclusion exception applied).

265. The 137 mile difference between the two counties is approximately a two-and-a-half-hour drive. *See* GOOGLE MAPS, https://bit.ly/2OZPPid (last visited Feb. 21, 2021).

266. *See Stahl*, 206 So.3d at 136.

267. *See Garcia*, 302 So.3d at 1057.

268. *See id.*; *Stahl*, 206 So.3d at 136.

Like Florida, Illinois' appellate courts also disagree on the issue.[269] In Cook County, the court found a defendant in direct civil contempt of court when she failed to unlock her cellular phone in defiance of a court order.[270] However, in Rock Island County,[271] the court held that compelling a defendant to disclose the passcode to his cell phone would violate his Fifth Amendment right against self-incrimination.[272] Like Florida, these inconsistent interpretations of the Fifth Amendment's privilege against self-incrimination result in Illinois residents' constitutional rights changing every time they cross county lines.[273]

In the federal system, similar inconsistencies exist. In the Ninth Circuit, defendants cannot be compelled to provide a passcode or use a biometric feature to unlock an electronic device.[274] However, in the Eleventh Circuit, the Fifth Amendment is not implicated for a nontestimonial act of production like providing a fingerprint.[275] The Eleventh Circuit requires law enforcement to prove with reasonable particularity that the information sought is a foregone conclusion for devices protected by alphanumeric passwords.[276] Yet another standard exists in the Fourth Circuit, in which the government need only prove that the defendant was the sole user or possessor of the device to compel decryption.[277]

---

269. *See* People v. Johnson, 90 N.E.3d 634, 640–41 (Ill. App. Ct. 2017); People v. Spicer, 125 N.E.3d 1286, 1292 (Ill. App. Ct. 2017).

270. Although the Appellate Court of Illinois for the First District did not specifically consider whether compelling a defendant to unlock a phone or to provide a passcode is a violation of the Fifth Amendment, the trial court found that the compulsion fell within the foregone conclusion exception, and the Appellate Court acknowledged their holding. *See Johnson*, 90 N.E.3d at 636.

271. Rock Island County is approximately 168 miles from Cook County, which is less than a 3-hour drive. *See* GOOGLE MAPS, https://bit.ly/37Bt7U2 (last visited Feb. 21, 2021).

272. *See Spicer*, 125 N.E.3d at 1292. The court reasoned that revealing the passcode was testimonial and that the foregone conclusion exception did not apply. *See id.* According to the court, the focus of the foregone conclusion exception is not on the passcode itself but on the information the passcode protects. *See id.* Therefore, the State needed to establish with reasonable particularity what the contents of the phone were, which it did not do. *See id.*

273. *See id.*; *Johnson*, 90 N.E.3d at 640–41.

274. *See In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1018 (N.D. Cal. 2019) ("The Government may not compel or otherwise utilize fingers, thumbs, facial recognition, optical/iris, or any other biometric feature to unlock electronic devices.").

275. *See* United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1345 (11th Cir. 2012).

276. *See id.*

277. *See* United States v. Gavegnano, 305 F. App'x 954, 956 (4th Cir. 2009).

The inconsistent interpretations of the Fifth Amendment result in a denial of due process[278] and equal protection[279] for criminal defendants in similarly situated circumstances.[280] Although "[e]qual protection does not require that all persons be dealt with identically," the distinction between people must "have some relevance to the purpose for which the classification is made."[281] The Fifth Amendment privilege against self-incrimination should not extend more protection to individuals who use alphanumeric passcode than to individuals who use biometric passcodes.[282] No government interest is substantially furthered by the differential treatment between alphanumeric passcode users and biometric passcode users.[283] Therefore, these laws violate equal protection and due process.

IV. CONCLUSION

To prevent absurd results and to ensure that all criminal defendants receive the same treatment under the Fifth Amendment privilege against self-incrimination, the Supreme Court should resolve the current federal circuit, state, and sub-state splits and rule definitively on the compelled decryption issue.[284] Passwords and biometric security bypasses should not be interpreted as testimonial communications, especially when the foregone conclusion exception applies.[285]

Traditional passwords are not inherently testimonial or inherently incriminating.[286] Even if some testimonial implication could be drawn from a defendant decrypting a device, the foregone conclusion exception should be satisfied when law enforcement can prove that the defendant has ownership or control over the encrypted device and knows the

278. "No person shall . . . be deprived of life, liberty, or property, without due process of law . . . ." U.S. Const. amend. V. Due process prevents the government from unfairly or arbitrarily convicting or punishing someone. *See* CHRISTOPHER WOLFE, THE RISE OF MODERN JUDICIAL REVIEW: FROM CONSTITUTIONAL INTERPRETATION TO JUDGE-MADE LAW 372–73 (1986).

279. "No State shall . . . deny to any person within its jurisdiction the equal protection of the laws." U.S. Const. amend. XIV, § 1.

280. *See* State v. Stahl, 206 So.3d 124, 135 (Fla. Dist. Ct. App. 2016); *see also* Equal Protection Clause, BLACK'S LAW DICTIONARY (11th ed. 2019) (defining "Equal Protection Clause" as "[t]he 14th Amendment provision requiring the states to give similarly situated persons or classes similar treatment under the law").

281. Baxstrom v. Herold, 383 U.S. 107, 111 (1966).

282. *See Stahl*, 206 So.3d at 135.

283. *See* Police Dep't of Chi. v. Mosley, 408 U.S. 92, 95 (1972) (holding that the crucial question in equal protection cases is whether an appropriate government interest is substantially furthered by the differential treatment between groups).

284. *See supra* Section III.C.

285. *See supra* Sections III.A, III.B.

286. *See supra* Sections II.D.1.a, III.A.

password.[287] The reasonable particularity standard articulated by the Eleventh Circuit arbitrarily requires the State to establish evidence beyond what is required by the governing Supreme Court case law.[288]

Biometric passwords do not constitute testimonial communications and, therefore, do not trigger the Fifth Amendment privilege against self-incrimination.[289] Because biometric passwords do not require defendants to use the contents of their minds or convey any knowledge they might have, the compelled unlocking of a biometric-protected device is nontestimonial.[290] No threshold of incriminating evidence can replace the requirement that a communication be testimonial in order to trigger the Fifth Amendment privilege against self-incrimination.[291]

Strong encryption protects data in the modern world.[292] However, a legal system that would allow the Aaron Stahls of the world to avoid detection and punishment for their crimes does not bear contemplation.[293] Compelling criminal defendants to decrypt their devices provides courts with both a feasible and constitutionally permissible means to promote digital security and facilitate justice.[294]

287. *See supra* Section II.D.1.c.
288. *See supra* Section III.A.
289. *See supra* Sections II.C, III.B.
290. *See supra* Sections II.C, III.B.
291. *See supra* Section II.C.
292. *See supra* Section II.A.
293. *See supra* Part I.
294. *See supra* Sections II.A, III.

***