Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 31 *XXXI*
Number 4

Article 5

2021

Abridging the Fifth Amendment: Compelled Decryption, Passwords, & Biometrics

Raila Cinda Brejt
Fordham University School of Law, rbrejt@law.fordham.edu

Abridging the Fifth Amendment: Compelled Decryption, Passwords, & Biometrics

Cover Page Footnote

J.D. Candidate, Fordham University School of Law, 2021; M.A., New York University, 2012; B.S., City University of New York, Brooklyn College, 2010. Thank you to Professor Daniel J. Capra for your advice and insightful comments. Additionally, thank you to the Fordham Intellectual Property Law Journal Executive Board, especially Sara Mazurek, for your feedback, time, and encouragement throughout this process.

Abridging the Fifth Amendment: Compelled Decryption, Passwords, & Biometrics

Raila Cinda Brejt*

Technological developments change the way we perform tasks by creating more efficient solutions to old problems and giving rise to opportunities not previously possible. Advances in communications technology have made the world feel smaller and more accessible. These changes also affect the methodology of both criminal activity and the investigative procedures of law enforcement. Our fundamental rights are challenged as judges and state actors try to strike the perfect balance between longstanding values and contemporary problems. This Note considers the Fifth Amendment challenges that arise when law enforcement attempts to obtain evidence from a criminal defendant's encrypted device. This Note will argue that the application of the foregone conclusion doctrine of the Fifth Amendment should require the government to show independent knowledge of the contents of the device that they seek prior to courts granting decryption compulsion orders of the criminal defendant's personal device. Biometric decryption should be considered the same as password encryption and distinguished from the physical act exceptions to the protections of the Fifth Amendment. To preserve the protections of the Fifth Amendment, we must resist the development of ambiguous and abridged doctrines that carry the potential to swallow our fundamental rights.

* J.D. Candidate, Fordham University School of Law, 2021; M.A., New York University, 2012; B.S., City University of New York, Brooklyn College, 2010. Thank you to Professor Daniel J. Capra for your advice and insightful comments. Additionally, thank you to the Fordham Intellectual Property Law Journal Executive Board, especially Sara Mazurek, for your feedback, time, and encouragement throughout this process.

INTRODUCTION

Computers, tablets, and smart phones are museums of their owners' minds as these devices record the users' social media, shopping,

and online dating habits while tracking location, health information, political affiliation, and so on.[1] The longer a person owns and utilizes their device, the more information the device has stored about the user. But users like to think they can keep their information away from the hands of others by encrypting it. In most circumstances, this should be sufficient. However, in the event that a person has a run-in with the law, it may become more complicated.

Professors Orin Kerr, of Berkley Law, and Bruce Schneier, security technologist, note that encryption technology has become widespread in recent years.[2] In the event that the government seeks evidence from a suspect's decrypted device, government investigators need to find an encryption workaround to convert the encrypted data from the encrypted digital devices to a decrypted and readable format.[3] Kerr and Schneier discuss six types of encryption workarounds;[4] this Note will focus solely on what they refer to as "compelling the key,"[5] wherein the government orders an individual to decrypt a device that is suspected or known to be under the dominion of a particular individual.[6] This method of decryption implicates Fifth Amendment jurisprudence, which is currently inadequate for protecting criminal defendants, as the doctrine is not fully fleshed out.

---

1 Riley v. California, 573 U.S. 373, 396 (2014) ("Mobile application software on a cell phone, or 'apps,' offer a range of tools for managing detailed information about all aspects of a person's life. There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life. There are popular apps for buying or selling just about anything, and the records of such transactions may be accessible on the phone indefinitely. There are over a million apps available in each of the two major app stores; the phrase 'there's an app for that' is now part of the popular lexicon. The average smart phone user has installed 33 apps, which together can form a revealing montage of the user's life.").

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

3 *Id.* at 990–91.

4 *Id.* at 996.

5 *Id.* at 1000.

6 *Id.*

Furthermore, the usage of biometrics,[7] in place of a password, adds to the complexity of modernizing the Fifth Amendment privilege. Biometric decryption technology has existed for some time, but on September 19, 2013, Apple Inc.'s sale of the iPhone 5 provided biometric decryption technology to the average consumer.[8] Unfortunately, our Fifth Amendment rights are at risk until it is legally determined how they interact with law enforcements' methodologies. It is important that the Fifth Amendment be construed liberally to protect defendants from the depreciation of their constitutional rights against self-incrimination.[9]

Part I of this Note will introduce the current binding precedent, as well as some gaps which lower courts have attempted to fill in. Part II considers the *State v. Stahl* case, with some of its problematic progeny, showing how radically the foregone conclusion doctrine can be misconstrued. Part III advocates that a password should not be considered a foregone conclusion based solely on showing ownership of the device and that the government must show independent knowledge of the evidence they seek prior to acquiring a compulsion order. To properly safeguard criminal defendants' constitutional rights, courts must adopt the narrowest interpretation of any doctrine which puts the defendants' rights in jeopardy.

---

[7] Maria Korolov, *What Is Biometrics? 10 Physical and Behavioral Identifiers That Can Be Used for Authentication*, CSO (Feb. 12, 2019, 6:00 AM), https://www.csoonline.com/article/3339565/what-is-biometrics-and-why-collecting-biometric-data-is-risky.html [https://perma.cc/3M8A-M4XT] (defining biometrics as "physical or behavioral human characteristics…[which] can be used to digitally identify a person to grant access to systems, devices or data" including fingerprint ID and facial recognition).

[8] Kara Goldman, *Biometric Passwords and the Privilege Against Self-Incrimination*, 33 CARDOZO ARTS & ENT. L.J. 211, 212 (2015).

[9] Gouled v. United States, 255 U.S. 298, 304 (1921) ("It has been repeatedly decided that [the Fifth Amendment] should receive a liberal construction, so as to prevent stealthy encroachment upon or 'gradual depreciation' of the rights secured by [it], by imperceptible practice of courts or by well-intentioned but mistakenly over-zealous executive officers.").

I. WHERE IT ALL BEGINS: CONTEXT FOR THE CLASH OF TECHNOLOGY AND THE LAW

A. Encryption, Passwords, and Biometrics

The government will often seek to obtain evidence from a suspect's digital device to link the suspect to the crime.[10] These digital devices—such as computers, tablets, and cell phones—carry a vast array of information that can reveal a rather intimate understanding of the user's hobbies, views, and relationships.[11] However, any content that is stored on digital devices can be encrypted.[12] Encryption utilizes an algorithm to convert information into a format that cannot be read or accessed.[13] Decryption involves causing the algorithm to be performed in the reverse to unscramble the data and make it readable to the device holder.[14] The device's encryption key must be triggered to reverse the algorithm.[15] This key is established and preprogrammed into the device by the device manufacturer.[16] The device user does not know the preprogrammed decryption key in the device's operating system, which controls the encryption process; rather, users who wish to encrypt their device can set their own password which serves to trigger the device to provide the decryption key.[17] Once the user enters their password into the digital device, the password decrypts the key, which in turn decrypts the actual content on the digital device.[18] Therefore, in order to access data stored on an encrypted digital device, a device holder must know the device's password.

Consumers can use their physical biometric features to avoid entering the password to decrypt their various devices equipped with these capabilities.[19] Biometric feature decryption utilizes scans of

---

10 Riley v. California, 573 U.S. 373, 379 (2014).
11 *Id.* at 396–97.
12 Kerr & Schneier, *supra* note 2, at 993.
13 *Id.*
14 *Id.*
15 *Id.* at 994–95.
16 *Id.*
17 *Id.* at 994.
18 *Id.* at 994–95.
19 United States v. Sealed Warrant, 2019 U.S. Dist. LEXIS 147836, at *11 (N.D. Cal. Aug. 16, 2019).

the user's face, eye, or fingerprint.[20] In order to set up biometric decryption, the user must first set a password on the device.[21] When presented with the correct biometric features, these features trigger the digital device to utilize the user-established password to decrypt the device's decryption key, which subsequently decrypts the digital device.[22]

B. "I Plead the Fifth": Fifth Amendment Protections

The goal of the right against self-incrimination is "to avoid confronting the witness with the 'cruel trilemma' of self-accusation, perjury or contempt."[23] The essence of the cruel trilemma is forcing the defendant to "communicate an express or implied assertion of fact or belief" where the defendant's choices are limited to "truth, falsity, or silence" and suffering the consequences of their choice.[24]

To avoid confessions obtained by cruel treatment,[25] the Fifth Amendment of the United States Constitution protects a person from being compelled to act as a "witness against himself."[26] The three elements of the Fifth Amendment privilege are: "(1) compulsion of a (2) testimonial communication that is (3) incriminating."[27] Traditionally, the Fifth Amendment privilege has served to prohibit the government from compelling a criminal defendant to take the stand and say things against their own penal interest or to force them to incriminate themselves.[28]

---

20 *Id.* at 12.

21 Michael Price & Zach Simonetti, *Defending Device Decryption Cases*, 43 CHAMPION 42, 42 (2019).

22 *Id.*

23 *In re* Martin-Trigona, 732 F.2d 170, 174 (2d Cir. 1984) (quoting Murphy v. Waterfront Comm'n of N.Y. Harbor, 378 U.S. 52, 50 (1964)).

24 Pennsylvania v. Muniz, 496 U.S. 582, 597 (1990).

25 Couch v. United States, 409 U.S. 322, 328 (1973).

26 U.S. CONST. amend. V.

27 United States v. Authement, 607 F.2d 1129, 1131 (5th Cir. 1979) (interpreting Fisher v. United States, 425 U.S. 391 (1976)).

28 *Couch*, 409 U.S. at 327.

1. Establishing the Foregone Conclusion Doctrine – The Trilogy

Fifth Amendment protections are not limited to speech. According to the Supreme Court, compelled actions can be considered testimonial communications.[29] In *Fisher v. United States*,[30] the Court considered whether compelling an attorney to provide his client's tax paperwork to the Internal Revenue Service ("IRS") constituted compelled self-incrimination in conflict with his Fifth Amendment right.[31] The right against producing one's own incriminating papers is supported by longstanding jurisprudence.[32] The preexisting documents are not protected, but the action of having to provide them against yourself is.[33] However, the *Fisher* Court concluded that neither the attorney nor the client's Fifth Amendment right allowed for denying an enforcement action by the IRS.[34] The Court held that asserting the Fifth Amendment privilege is specific to barring the "use of 'physical or moral compulsion' exerted on *the person*."[35] The Fifth Amendment only prevents incrimination by the defendant's own compelled testimonial communications.[36] Here, the subpoenaed documents were prepared by the defendant's accountant and therefore, did not constitute testimonial declarations against the defendant taxpayer—rather, it was merely a surrender.[37]

The *Fisher* Court observed that the very act of production can be communicative by admitting possession, control, and the existence of the produced items.[38] The key inquiry of the potentially communicative nature of compelled production concerns the context of the production.[39] To determine if compelled production becomes testimonial and therefore conflicts with the defendant's Fifth

---

29 *See generally* Fisher v. United States, 425 U.S. 391 (1976).
30 *Id.*
31 *Id.*
32 Boyd v. United States, 116 U.S. 616, 630 (1886).
33 *Fisher*, 425 U.S. at 407.
34 *Id.* at 405, 414.
35 *Id.* at 397 (quoting Perlman v. United States, 247 U.S. 7, 15 (1918)) (emphasis added).
36 *Fisher*, 425 U.S. at 409.
37 *Id.*
38 *Id.* at 410; *see also In re* Grand Jury Proceedings, 771 F.2d 143, 145 (6th Cir. 1985).
39 *See* United States v. Schlansky, 709 F.2d 1079, 1083 (6th Cir. 1983), *cert. denied*, 465 U.S. 1099 (1984).

Amendment right, it is pertinent to determine whether producing the evidence signifies a link in the evidentiary chain by providing the government with information they did not previously have.[40]

There are certain long-standing exceptions that are exempt from the Fifth Amendment's protection, such as: having blood drawn for a blood-alcohol test;[41] being compelled to provide voice and handwriting samples;[42] and being compelled to try on clothing or appear in front of the jury.[43] Additionally, the required records exception[44] and the corporate records exception[45] also remove compliance with a governmental demand for documents outside the protections of the Fifth Amendment.

Two Supreme Court cases furthered *Fisher*'s doctrine of the communicative nature of producing documents. In the first case, *United States v. Hubbell*, the Court utilized *Fisher*'s "foregone conclusion" doctrine.[46] This doctrine applies when the witness' production of the documents provided evidence that the government already had knowledge of, thus, the witness does not provide any additional information to the government.[47] When the existence, location, and authenticity of the property in question is already a foregone conclusion, the Fifth Amendment does not apply because it is a matter of surrender rather than testimony.[48] The *Hubbell* Court found that the government cannot pursue charges against an individual who produced documents after receiving immunity because without this production the government had no other source or

---

40 *See, e.g.*, *id.* at 1084.

41 *E.g.*, Schmerber v. California, 384 U.S. 757, 762 (1966).

42 *E.g.*, Gilbert v. California, 388 U.S. 263, 266–67 (1967).

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

44 *E.g.*, United States v. Doe *(In re* Grand Jury Subpoenas Dated September 9, 2011), 2011 U.S. Dist. LEXIS 156979, at *19–20 (E.D.N.Y. Dec. 30, 2011) (discussing the required records exception, which is triggered when an individual engages in an activity that has a mandatory record-keeping requirement which obligates the individual to have these records).

45 *E.g.*, *In re* Grand Jury Subpoenas Duces Tecum dated June 13, 1983 & June 22, 722 F.2d 981, 986–88 (2d Cir. 1983) (discussing the corporate records exception, which compels officers of a corporation to provide the corporation's records if subpoenaed by the government).

46 United States v. Hubbell, 530 U.S. 27, 44–45 (2000).

47 Doe v. United States (*In re* Grand Jury Subpoena), 383 F.3d 905, 910 (9th Cir. 2004).

48 *See id.*

knowledge of the existence and location of these documents.[49] To sustain such an indictment subsequent to a grant of immunity for the production of these documents, the government would have to show a "wholly independent" source from which it obtained the same evidence.[50]

In the second case, *Doe v. United States*, the Court notes that the Fifth Amendment protects the contents of an individual's mind from compelled disclosure.[51] This case involved the government's interest in gaining information about the defendant's offshore bank accounts.[52] To obtain this information, the bank required the government to provide a consent form signed by the defendant.[53] The defendant asserted that compelling his signature on a consent form would be a violation of his Fifth Amendment right.[54] In a famous footnote responding to an argument from the dissenting Justice Stevens, the majority contrasts the particular type of consent directive the defendant is being compelled to sign with being compelled to provide the "combination to [a] wall safe."[55] Subsequently, in *Hubbell*, this statement made its way into the text of the majority opinion which Justice Stevens authored.[56]

2. What is "Foregone" in the Foregone Conclusion Doctrine?

To address the changing Fifth Amendment inquiries, courts have utilized the language in *Hubbell* to develop elements to the foregone conclusion test.[57] This test requires the government to have prior knowledge of the "location, existence, and authentic[ity]" of the

---

49 *See Hubbell*, 530 U.S. at 44–45.

50 *Id.* at 45 (quoting Kastigar v. United States, 406 U.S. 441, 460 (1972)).

51 Doe v. United States, 487 U.S. 201, 210–11 (1988).

52 *Id* at 202–03.

53 *Id.*

54 *Id.* at 204.

55 *Id.* at 210 n.9 ("In our view, such compulsion is more like 'be[ing] forced to surrender a key to a strongbox containing incriminating documents' than it is like 'be[ing] compelled to reveal the combination to [petitioner's] wall safe.'").

56 United States v. Hubbell, 530 U.S. 27, 43 (2000).

57 *See* Jesse Coulon, *Privacy, Screened Out: Analyzing the Threat to Individual Privacy Rights and Fifth Amendment Protections in* State v. Stahl, 59 B.C. L. REV. E. SUPP. 225, 234 (2018).

evidence it seeks.[58] These three elements act as barriers against governmental compulsion of evidence from an individual. If the government can show sufficient prior knowledge of the evidence's location and existence, and can independently prove its authenticity, then compelling the defendant to produce this evidence is not self-incriminating and, therefore, permissible under the Fifth Amendment since the government already knew about it.[59]

The standard for the government's showing of prior knowledge to establish the foregone conclusion is the "reasonable particularity" standard. The language of this standard originates from a Second Circuit case which the *Hubbell* Court utilized to demonstrate that the government was unable to establish knowledge of what documents they sought from Hubbell.[60] When the case was granted certiorari, the Supreme Court agreed with the D.C. Circuit's conclusion that the government failed its burden of showing adequate prior knowledge based on their overbroad request.[61] Therefore, it would violate Hubbell's Fifth Amendment right to be compelled to provide documents to the government because he would essentially be doing the work of incriminating himself for them.[62]

3. It's Complicated: Differing Opinions

Applying the foregone conclusion doctrine can be complicated. Currently, there is no binding precedent on how to apply its so-called elements, and the reasonable particularity standard is largely undefined. This has led courts to examine the issue from a variety of angles, attempting to balance the needs of the government with the Fifth Amendment rights of the accused. Below is an attempt to

---

58 *See id.* at n.50; *Hubbell*, 530 U.S. at 32 ("The question the District Court should have addressed was the extent of the Government's independent knowledge of the documents' existence and authenticity, and of respondent's possession or control of them.").

59 *Hubbell*, 530 U.S. at 44–45.

60 United States v. Hubbell, 167 F.3d 552, 579 (D.C. Cir. 1999) ("[W]e agree with the Second Circuit that the government must establish its knowledge of the existence, possession, and authenticity of subpoenaed documents with 'reasonable particularity' before the communication inherent in the act of production can be considered a foregone conclusion.").

61 *Hubbell*, 530 U.S. at 29–30, 44–45.

62 *Id.* at 45.

summarize some of the current arguments in Fifth Amendment jurisprudence for compelling decryption of a digital device.

a) Possession: Whose Phone Is It Anyway?

Every detail must be considered when analyzing actions for their testimonial nature. The Florida Fourth District Court of Appeals has held that compelled decryption is not a foregone conclusion because decryption acts as a communication.[63] In a case where the government was seeking the decryption of a phone retrieved from a household with several individuals, the District Court for the Northern District of Illinois, Eastern Division noted that being able to open the phone communicated possession and control over the device.[64] Therefore, compelling individuals to use their fingerprint to try to open a phone "tacitly concedes" ownership, unless the government can show prior knowledge of whose phone it is.[65] If, once opened, the device contains evidence of the owner's illegal activity, then opening the phone incriminates the opener and is, therefore, testimonial.

b) What Is a Password?

Typically, the password itself is not direct evidence. Analogizing the text of the *Hubbell* decision that "compelled testimony that communicates information that may 'lead to incriminating evidence' is privileged even if the information itself is not inculpatory,"[66] the District Court for the Eastern District of Michigan, Southern Division held that requesting a password is not seeking evidence, but rather seeking a *fact that leads to the evidence*.[67]

---

63 *See* G.A.Q.L. v. State, 257 So. 3d 1058, 1061–62 (Fla. Dist. Ct. App. 2018).

64 *See In re* Single-Family Home & Attached Garage, 2017 U.S. Dist. LEXIS 170184, at *3–4 (N.D. Ill. Feb. 21, 2017), *rev'd on other grounds*, *In re* Search Warrant Application, 279 F. Supp. 3d 800 (N.D. Ill. 2017); *accord In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1016 (N.D. Cal. 2019) (stating that "a successful finger or thumb scan confirms ownership or control of the device.").

65 Fisher v. United States, 425 U.S. 391, 410 (1976) (explaining that compliance with a subpoena "tacitly concedes" the existence of the evidence sought).

66 United States v. Kirschner, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) (quoting Doe v. United States, 487 U.S. 201, 208 n.6 (1988)).

67 *See id.*

Therefore, providing a password can be a testimonial communication because it leads to other evidence.[68]

Courts often characterize a password as knowledge, thereby making it "contents of the mind."[69] This characterization prevents passwords from being a foregone conclusion and are, therefore, testimonial. In another case, *Pollard v. State*, the court notes that the method of providing the password, whether defendant enters it into the phone, writes it down, or says it, does not negate that it is a product of the defendant's mind.[70]

c) Types of Encryption

Some courts distinguish between passwords and biometric decryption.[71] These courts assert that using a fingerprint to decrypt a digital device is merely a physical act and therefore is as good as a foregone conclusion.[72] In contrast, since the government does not know the password, decryption via password is not a forgone conclusion.[73]

In Minnesota, the *Diamond* court argued that the physical act of providing a fingerprint is no different than other longstanding manners of compelling the suspect to perform a physical act to confirm or deny his guilt.[74] As previously mentioned, there are established exceptions to the Fifth Amendment, such as allowing for blood draws or making a court appearance to be identified by the victim.[75] The court found that unlocking a phone via fingerprint is no more testimonial than these longstanding physical exceptions.[76]

---

68 *See id.*

69 *See, e.g.*, *id* (quoting *Doe*, 487 U.S. at 211); Commonwealth v. Baust, 89 Va. Cir. 267, 271 (Va. Cir. Ct. 2014).

70 Pollard v. State, 287 So. 3d 639, 653 (Fla. 2019), *denied motion for rehearing and certified questions to* 2019 Fla. App. LEXIS 18978 (Dist. Ct. App. Dec. 23, 2019).

71 *See Baust*, 89 Va. Cir. at 271; *but see In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1016 (N.D. Cal. 2019).

72 *See, e.g.*, United States v. Barrera, 415 F. Supp. 3d 832, 839 (N.D. Ill. Nov. 22, 2019).

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

74 *See* State v. Diamond, 890 N.W.2d 143, 151 (Ct. App. Minn. 2017).

75 *See supra* Section I.B.1.

76 *Id.*

d) Waiver: Once Revealed, It Is No Longer a Secret

In Vermont, the *Boucher* court found that if an individual has already shown files to the government, thereby confirming the existence, location, and authenticity of these files, the Fifth Amendment protection is waived.[77] The government's knowledge of files that the defendant has already confirmed makes them foregone.[78] Boucher complied with a preliminary search of his computer, which contained child pornography, but later refused to provide the password.[79] Since the existence of these files on his computer was already a foregone conclusion, providing the password no longer carried any testimonial value.[80] This voluntary production as waiver has been held to be true even in a case where the defendant was in custody and had not been given her Miranda rights.[81]

e) Rejected Distinctions

i. Voluntarily Created Files Can Still Be Testimonial

In an Eleventh Circuit case, the defendant rebutted the government's argument that files created voluntarily are not testimonial because they were not created to be incriminating.[82] The Court held that the government's argument missed the issue of whether the act of production, not the contents, was communicative.[83] Here, the court required the government to show that it had knowledge of

---

77 *In re* Grand Jury Subpoena (Boucher), 2009 U.S. Dist. LEXIS 13006, at *9–10 (D. Vt. Feb. 19, 2009).

78 *Id.*

79 *Id.* at 9.

80 *Id.* at 9–10; Commonwealth v. Gelfgatt, 468 Mass. 512, 524 (2014) (finding that the defendant's post-arrest interview informed the government that his transactions and communications utilized his computers and affirmed his ownership of the computers, thereby making any communication from decrypting them a foregone conclusion).

81 United States v. Oloyede, 933 F.3d 302, 309 (4th Cir. 2019); *but see* United States v. Green, 272 F.3d 748, 753 (5th Cir. 2001) (finding that once an individual has invoked his right to counsel, any subsequent interrogation results in testimonial and inadmissible self-incrimination).

82 United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1342 (11th Cir. 2012).

83 *Id.*

some of the contents of the device rather than merely knowing that the defendant can decrypt it.[84]

ii. Decryption Is Not Assembly

Another rejected distinction is that decryption actually forces the defendant to assemble the data together for the government.[85] Unlike when Hubbell was required to collect thousands of documents, biometric decryption cannot be considered testimonial by claiming it is an act of assembly since this process is accomplished by a single tap of defendant's finger.[86] The U.S. District Court for the District of Columbia found that the difference in cognitive exertion involved in the assembly process distinguished whether it was testimonial.[87]

f) Effort Involved May Make a Difference

Similarly to above, the Eleventh Circuit held that a defendant was not required to produce an unencrypted hard drive.[88] The court found that it was testimonial that rather than seeking decryption of a device, the government sought to require the defendant to produce a copy of the unencrypted hard drive.[89] A later court noted that producing an unencrypted hard drive is more cognitively demanding than the act of biometrically decrypting a device, thereby causing production of an unencrypted hard drive to not be a foregone conclusion.[90]

g) Scope of Reasonable Particularity

The *Hubbell* Court considered the government's request for "any and all" documents to be an indication that the government did not have enough knowledge of the defendant's incriminatory possessions to rise to the level of a foregone conclusion.[91] Knowing that an individual keeps business records is insufficient for showing with

---

84 United States v. Spencer, 2018 U.S. Dist. LEXIS 70649, at *6 (N.D. Cal. Apr. 26, 2018) (interpreting *Doe* (*In re* Grand Jury Subpoena), 670 F.3d at 1347).

85 *In re* Search of [Redacted], 317 F. Supp. 3d 523, 537–38 (D.D.C. 2018).

86 *Id.* at 538.

87 *Id.*

88 *See generally Doe* (*In re* Grand Jury Subpoena), 670 F.3d.

89 *Id.* at 1346.

90 State v. Diamond, 890 N.W.2d 143, 150 (Ct. App. Minn. 2017).

91 United States v. Hubbell, 530 U.S. 27, 38 (2000).

reasonable particularity that he has the documents the government is seeking.[92] Such an overbroad statement cannot be the basis for a foregone conclusion because answering such a request would show that the defendant believed the documents he produced were actually what the government sought. Compliance with such a request implicitly communicates the defendant's belief that these documents reveal their guilt and waive the defendant's option to deny knowledge of what the government is seeking.

Other courts have determined that the government's lack of specificity for the files it seeks is actually a Fourth Amendment issue,[93] while simultaneously noting that "it is nonsensical to ask whether the government has established with 'reasonable particularity' that the defendant is able to decrypt a device."[94] The *Spencer* court noted that the reasonable particularity standard is ill-suited for the yes or no inquiry of whether the defendant can open his phone; rather, such a standard is more logically tailored to determining if the government has shown enough prior knowledge to meet its burden of showing the device's contents are a foregone conclusion not worthy of the Fifth Amendment's protection.[95]

II. A CRY FOR HELP: WHEN DOCTRINE IS MISCONSTRUED

A. Dangerous Interpretations: State v. Stahl

In 2014, the Floridian police arrested Aaron Stahl on charges of video voyeurism for attempting to capture video footage up a woman's skirt with his cell phone.[96] When police located and arrested him, he did not have his cell phone on him.[97] Once arrested, he agreed to have his phone searched but then withdrew his consent.[98] He had already identified the phone—an iPhone 5—and

---

92 Doe v. United States (*In re* Grand Jury Subpoena), 383 F.3d 905, 911–12 (9th Cir. 2004).

93 United States v. Spencer, 2018 U.S. Dist. LEXIS 70649, at *7–8 (N.D. Cal. Apr. 26, 2018).

94 *Id.* at 8.

95 *Id.* at 9.

96 State v. Stahl, 206 So. 3d 124, 127 (Fla. Dist. Ct. App. 2016).

97 *Id.*

98 *Id.* at 128.

confirmed that it could be found at his residence.[99] However, when police discovered the phone was password protected,[100] the Fifth Amendment analysis began, and it went awry.

The *Stahl* court focused on the testimonial element of the Fifth Amendment right.[101] It found that the production of a password does not constitute a testimonial communication and therefore, the state can compel decryption of a password encrypted device.[102] *Stahl* classifies biometrics as mere physical acts to classify biometric decryption as nontestimonial.[103] Such reasoning fails to recognize that mere physical acts serve to utilize the defendant's physical qualities as evidence, rather than having the defendant supply access to evidence.

The *Stahl* court asserts two lines of reasoning which decrease the burden of the foregone conclusion doctrine. First, *Stahl* reduced the government's burden to showing independent knowledge of the existence, authenticity, and possession of the phone's password, rather than having to show independent knowledge *of the evidence that is encrypted on the phone*.[104] Second, the court found that if the foregone conclusion doctrine applies to passwords, the passwords must be considered self-authenticating, thereby both removing authentication as an element of the doctrine and simultaneously causing the defendant's act of decryption to be communicative of the authenticity of the content on the device.[105] The *Stahl* court also struggled to determine how a password is actually defined within its abridged version of the doctrine. At different points in the opinion, the court regarded passwords as a source of evidence,[106] but subsequently considered the password to be the evidence that must be foregone for the government to compel decryption.[107] Each of these problematic findings will be discussed below.

---

99 *Id.*
100 *Id.*
101 *Id.* at 132.
102 *Id*. at 134.
103 *Id*. at 135.
104 *Id*. at 136.
105 *Id.*
106 *Id*. at 134.
107 *Id.* at 135–36.

1. Passwords as Nontestimonial Communications

The *Stahl* court found that producing a password was a nontestimonial communication.[108] The Fifth Amendment privilege only protects against compulsion of testimonial communications, while nontestimonial materials can be compelled.[109] Therefore, the testimonial status of a password determines whether the Fifth Amendment protects encrypted devices.

Many courts find that something is testimonial if it utilizes the contents of the individual's mind.[110] But the *Stahl* court noted that the *Hubbell* Court spoke of "extensive" use of the contents of the mind.[111] This led *Stahl* to assert that the content being sought must be of "testimonial significance" to be testimonial.[112] Therefore, the *Stahl* court concluded that because the password being sought does not alone have testimonial significance, it is a nontestimonial communication.[113] This reasoning prevented Stahl from asserting his Fifth Amendment right, and allowed the government to compel the unlocking of his iPhone.

The issue with *Stahl*'s analysis is that it misses the *Hubbell* Court's point of juxtaposing the notion of the "extensive" use of the contents of the mind with a reiteration of *Doe*'s famous footnote, showing that physical keys are different than keys stored in one's memory.[114] This juxtaposition served to show that extensive usage of one's cognitive abilities to collect hundreds of documents is more similar to being compelled to provide a wall safe combination than the non-cognitively demanding act of handing over a physical key to open a box.[115] It is a typical and commonplace convention of speech to follow a conceptual statement with an example to help

---

108 *Id*. at 134.

109 *Id.* at 131.

110 *Id.* at 133–34.

111 *Id.* (quoting United States v. Hubbell, 530 U.S. 27, 43 (2000)).

112 *Id.* at 133–34 (quoting Doe v. United States, 487 U.S. 201, 211 n.10 (1988)).

113 *Id.* at 133–35.

114 *Hubbell*, 530 U.S. at 43 ("It was unquestionably necessary for respondent to make extensive use of 'the contents of his own mind' in identifying the hundreds of documents responsive to the requests in the subpoena….The assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox.").

115 *Id.*

visualize the content of the preceding sentence. By using *Hubbell*'s "extensive usage of the mind" out of context of the subsequent statement, the *Stahl* court misapplied *Hubbell*'s case language. Severing "extensive" from the wall safe combination example attempts to make producing a password into an insignificant, and thus, nontestimonial communication. At the extreme, this mistaken interpretation permits compelled decryption to be subject to governmental compulsion like any other type of physical evidence—despite a password's existence as contents of the mind.

2. To Be the Evidence or to Provide the Evidence

The *Stahl* court confuses two important ideas: (1) the defendant's characteristics being classified as the evidence and (2) the government utilizing the defendant's physical characteristics as a vehicle to obtaining other evidence.[116] In coming to the conclusion that passwords are nontestimonial, the *Stahl* court asserts that it is necessary to prevent biometrically encrypted cell phones from receiving less protection under the Fifth Amendment than passwords.[117] The court then sought to ensure that neither format of encryption received Fifth Amendment protection. Their argument hinges on their assumption that biometric decryption does not convey more than an unprotected mere physical act.[118]

Under longstanding Fifth Amendment jurisprudence, an accused may be forced to do certain physical acts to confirm or deny their guilt, such as providing blood samples or voice exemplars.[119] If these compelled acts were not permitted under the Fifth Amendment, Justice Holmes noted, a court would not even be allowed to bring the defendant in to be viewed by a jury.[120] However, conflating the physical acts permitted by Fifth Amendment jurisprudence—of being the physical evidence against oneself with

---

116 *Stahl*, 206 So. 3d at 135; *but see Doe*, 487 U.S. at 211 n.10 (utilizing the phrase "testimonial significance" to explain the distinction between serving as the physical evidence and physically complying with a compulsion order to provide a source of evidence).

117 *Stahl*, 206 So. 3d at 135.

118 *Id.*

119 *Id.*

120 Schmerber v. California, 384 U.S. 757, 763 (1966).

biometric decryption—misunderstands the goal of using the defendant as evidence against oneself when there would be no other alternative.

Forcing the defendant to unlock a phone is not about *being* the evidence, it is about directly supplying the evidence. This additional step between being the evidence and personally supplying the evidence, regardless of the format of decryption, results in a testimonial action "furnish[ing] a link in the chain of evidence."[121] Unless the ownership and content on the device has already been shown to be a foregone conclusion through independent means, compelled biometric decryption communicates the defendant's relationship with the device and its contents.

In *Doe*, the government carefully crafted the consent directive to avoid being testimonial; the directive did not assert any facts by requesting information on any accounts Doe "may" be associated with, without specifying from which bank, and by adding the additional layer of protection of requiring independent authentication.[122] The *Doe* defendant was not revealing possession with this signature; rather the signature served to allow the government to obtain access to documents from a third-party that may result in relevant evidence, which the government would subsequently have to authenticate independently.[123] This distinguishes Doe's physical act of signing the directive from the direct and personal surrender of evidence provided by biometric decryption, which communicates that the evidence on the device was placed there by the individual with matching physical features.[124]

It is important to note that the above analysis is not applicable if the government already knew the phone contained illicit content and had probable cause to believe the suspect had committed the crime.

---

121 United States v. Hubbell, 530 U.S. 27, 38 (2000) (quoting Hoffman v. United States, 341 U.S. 479, 486 (1951)) ("'The privilege afforded not only extends to answers that would in themselves support a conviction…but likewise embraces those which would furnish a link in the chain of evidence.'").

122 Doe v. United States, 487 U.S. 201, 215 (1988).

123 *Id.*

124 Aric Jenkins, *Could an 'Evil Twin' Trick Your iPhone's Facial Recognition?*, TIME (Sept. 13, 2017), https://time.com/4940176/apple-iphone-x-face-id-facial-recognition/ [https://perma.cc/Q89G-5MDH].

If biometric decryption served to merely confirm ownership over the device, then compelled biometric decryption *would* be the same as being classified as physical evidence against oneself.

3. Reducing the Foregone Conclusion Burden

The *Stahl* court diminished the foregone conclusion doctrine to only require the government to prove with reasonable particularity that a password exists, the password is within the defendant's control, and it is authentic.[125] *Stahl*'s focus is on the vessel, the device holding the evidence, but the Fifth Amendment's protection is for protecting the defendant from having to produce their own self-incriminating evidence. The foregone conclusion was established for the limited circumstances in which the government can independently show it already knew of the evidence in the defendant's possession,[126] not that the defendant has access to a source of *potential* evidence.

The *Stahl* court accomplished this outrageous misreading of the foregone conclusion doctrine by misunderstanding the circumstances in *Boucher*,[127] where the defendant voluntarily allowed the government to search and discover child pornography on his computer and, therefore, made his possession of illicit content a foregone conclusion.[128] The government's previous search of the contents of the computer acts as independent knowledge of the device's content, making the illicit content a foregone conclusion and nullifying the testimonial nature of providing the password to the computer.

Boucher is easily distinguishable from *Stahl*, where the government was attempting to access Stahl's phone to try and prove he in fact committed a crime.[129] Knowing Boucher's encrypted computer contains child pornography is different than knowing that Stahl's phone is password encrypted. The officers investigating Stahl did not have any independent means for knowing the contents of his phone and wanted access to its decrypted files to obtain the initial

---

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

126 Doe v. United States (*In re* Grand Jury Subpoena), 383 F.3d 905, 910 (9th Cir. 2004).

127 *Stahl*, 206 So. 3d at 136.

128 *In re* Grand Jury Subpoena (Boucher), 2009 U.S. Dist. LEXIS 13006, at *9 (D. Vt. Feb. 19, 2009).

129 *Compare Boucher*, 2009 U.S. Dist. LEXIS 13006, at *9, *with Stahl*, 206 So. 3d at 127.

evidence.[130] By only requiring proof that Stahl has the password to his own phone, the *Stahl* court drastically reduced the government's burden envisioned by the *Hubbell* Court for the foregone conclusion doctrine.[131]

Comparing *Stahl* to *Hubbell*, the *Hubbell* Court held that the government's overbroad demand for thousands of documents showed that the government had not met its burden for the foregone conclusion exception to the production of self-incriminating evidence.[132] A sweeping compulsion of business records, without any specificity, evidences that the government failed to independently identify what they were seeking from Hubbell.

The government did not want Stahl's password for the sake of knowing the password; the password served as a vehicle to a potential avenue for evidence. When the *Stahl* court held that if the government can prove that the defendant has the password to his phone then the password is a foregone conclusion, this is the equivalent of saying that if the government knew Hubbell owned papers then all of his papers were a foregone conclusion to be freely collected by the government. The Supreme Court held the opposite by invalidating a claim for the foregone conclusion doctrine because the overbroad demand signified the government's inability to articulate which documents they wanted.[133]

4. Removing Elements of the Foregone Conclusion Doctrine

The *Stahl* decision removes the authenticity element from the foregone conclusion doctrine by determining that passcodes are self-authenticating.[134] According to *Stahl*, if the government, with

---

130 *See generally Stahl,* 206 So. 3d at 127.

131 United States v. Hubbell, 530 U.S. 27, 45; *Stahl*, 206 So. 3d at 135 (contradicting itself, having stated the correct burden of proof at the beginning of the opinion: "However, even the testimonial communication implicit in the act of production does not rise 'to the level of testimony within the protection of the Fifth Amendment' where the State has established, through independent means, the existence, possession, and authenticity of the documents.").

132 *Hubbell*, 530 U.S. at 45.

133 *Id.* ("The Government cannot cure this deficiency through the overbroad argument that a businessman such as respondent will always possess general business and tax records that fall within the broad categories described in this subpoena.").

134 *Stahl*, 206 So. 3d at 136.

reasonable particularity, determines a device belongs to the defendant and a password exists that the defendant can unlock the device with, then the contents of the device are authentic. This reduces the government's burden for the foregone conclusion exception to the Fifth Amendment; it only needs to prove the existence and location elements.

Additionally, determining a password's authenticity based on whether or not it opens the device is backwards;[135] such a process forces the defendant to authenticate the password him/herself by showing the password opens the device.[136] Not only does this self-authenticating test[137] appear to remove an element of the foregone conclusion doctrine, but it actually makes the action of entering the password retroactively communicative (of its own authenticity), and therefore testimonial, as it provides the government with information they did not know before (that the password is authentic).[138] Furthermore, authenticity is a distinct rule of the admissibility of evidence and acts as a potential defense for criminal defendants that should not be eradicated.[139]

5. Inconsistent Usage of Passwords as Two Separate Things

Finally, the *Stahl* court simultaneously considered a password to be two opposing concepts. Earlier in the decision, the password is merely a means to evidence and therefore, it is non-testimonial because it is insignificant.[140] Later in the decision, the court argues under the assumption that the password *is* evidence.[141] For the

---

135 *Id.* ("If the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic.").

136 Pollard v. State, 287 So. 3d 649, 656 (Fla. Dist. Ct. App. 2019); People v. Spicer, 125 N.E.3d 1286, 1292 (Ill. App. Ct. 2019).

137 *Stahl*, 206 So. 3d at 136.

138 *Spicer*, 125 N.E.3d at 1292.

139 FED. R. EVID. 901 & 902; FLA. STAT § 90.901 (2012).

140 *Stahl*, 206 So. 3d at 134 ("[A]lthough the passcode would allow the State access to the phone, and therefore to a source of potential evidence, the State has a warrant to search the phone—the source of evidence had already been uncovered.").

141 *Id.* at 135–36 ("That is, by implicitly admitting the existence of the evidence requested and that it is in the accused's possession the accused 'adds little or nothing to the sum total of the Government's information'" and "[t]o know whether providing the passcode implies testimony that is a foregone conclusion, the relevant question is whether the State has

purposes of the foregone conclusion, it is essential that the court resolve this inconsistency by acknowledging that a password is rarely itself evidence, but rather a method of access to evidence.

The *Stahl* court risks the integrity of the foregone conclusion doctrine and the protections of the Fifth Amendment with its erroneous reasoning and findings. Providing a password is a testimonial communication as it utilizes contents of the mind to decrypt a digital device and is not a mere surrender. Biometric decryption is not the same as physical acts of *being* the evidence against one's self. To utilize the foregone conclusion doctrine, the government must carry its burden of independent knowledge of the data it seeks from the device it wants decrypted. The defendant's successful decryption of a device cannot retroactively authenticate the content of the device. Ultimately, passwords are not evidence themselves, but rather they are a link to a source of evidence.

B. Stahl*'s Progeny*

1. When *Stahl*'s Holding Traveled Beyond the Floridian Borders

While some courts are not convinced by *Stahl*'s abridged version of the foregone conclusion doctrine,[142] other courts are employing it.[143] The *Stahl* holding and its reasoning has permeated Fifth Amendment jurisprudence in several states.

In *State v. Andrews*, the New Jersey court used *Stahl*'s abridged foregone conclusion doctrine as support for its statements that

established that it knows with reasonable particularity that the passcode exists, is within the accused's possession or control, and is authentic.").

[142] G.A.Q.L. v. State, 257 So. 3d 1058, 1063 (Fla. Dist. Ct. App. 2018) (disagreeing with its sister court of appeals that the foregone conclusion is strictly for getting the contents of the phone, not the password); Pollard v. State, 287 So. 3d 649, 651 (Fla. Dist. Ct. App. June 20, 2019), *review dismissed and motion denied as moot by* No. SC20-110, 2020 Fla. LEXIS 522, at *1 (Mar. 25, 2020) (noting that the government has to carry its burden for the foregone conclusion exception *before* it unlocks the phone, which means authenticity cannot be proven afterwards by showing the phone opens when defendant puts his password in); Seo v. State, 148 N.E.3d 952, 970 (Ind. 2020).

[143] State v. Andrews, 457 N.J. Super. 14, 27 (Super. Ct. App. Div. 2018); State v. Johnson, 576 S.W.3d 205, 226 (Mo. Ct. App. 2019); State v. Pittman, 300 Or. App. 147, 161–62 (2019); Commonwealth v. Jones, 481 Mass. 540, 548 (2019).

providing a password does not constitute a testimonial communication because the government already knows the password exists and the government only needs to show that the defendant has the password to his device.[144] On appeal to New Jersey's Supreme Court, *Andrews* once again leaned on *Stahl*'s reasoning for support[145] citing *Stahl* for two components of its abridged approach to the foregone conclusion doctrine: 1) the government's knowledge with reasonable particularity of the existence and defendant's possession of the password, as opposed to focusing on the evidence sought from the device;[146] and 2) *Stahl*'s declaration that, for digital devices, the authenticity prong of the foregone conclusion doctrine should be assumed.[147]

Aside from fostering other New Jersey cases,[148] *Andrews*' holding has since been used as support in a Missouri case,[149] and is mentioned in an Ohio case,[150] spreading the influence of *Stahl*'s holding further. Oregon takes it a step further, drastically abridging the Fifth Amendment by disregarding the elements of the foregone conclusion doctrine altogether.[151]

2. Scary New Trends as *Stahl*'s Reasoning Continues to Spread

The scary reality of *Stahl*'s holding is exacerbated when subsequent courts loosen the doctrine even further. In *State v. Pittman*, the defendant appealed a contempt order from her refusal to provide her phone password in relation to an investigation of defendant's

---

144 *Andrews*, 457 N.J. Super. at 27, 29.

145 State v. Andrews, 243 N.J. 447, 475–76 (2020).

146 *Id.*

147 *Id.* at 481.

148 *In re* State's Application, No. A-4509-18T2, 2020 N.J. Super. Unpub. LEXIS 1708, at *8 (Super. Ct. App. Div. Sept. 11, 2020) (applying *Andrews*' foregone conclusion doctrine by showing that Max owned the phone, the phone was password protected because the state could not open it, and the password self-authenticates); State v. Anthony, No. A-0714-19T4, 2020 N.J. Super. Unpub. LEXIS 1737, at *1–2 (Super. Ct. App. Div. Sept. 18, 2020).

149 State v. Johnson, 576 S.W.3d 205, 227–28 (Mo. Ct. App. 2019), *cert. denied*, 140 S. Ct. 472, 205 L. Ed. 2d 286, 2019 U.S. LEXIS 6651 (U.S. 2019).

150 *In re* M.W., 2018-Ohio-5227, ¶¶ 60–63 (Ohio Ct. App. 2018).

151 State v. Pittman, 300 Or. App. 147, 149 (2019), *rev'd and remanded on different grounds by* State v. Pittman, 376 Ore. 498 (2021).

involvement in a single-vehicle accident with a tree.[152] The government sought to compel the defendant to open her phone to acquire evidence that the defendant was under the influence of an illicit substance when she was involved in the accident.[153] Pittman was held in contempt of court for entering her password wrong twice.[154]

Pittman utilized *Stahl*'s holding that passwords are nontestimonial to abandon the foregone conclusion doctrine when compelling decryption of a device that the government had already lawfully seized by warrant.[155] The court stated that the government's possession of the device is the equivalent of the government's possession of the data on the device, despite its encrypted format.[156] Neither the Court of Appeals of Oregon,[157] nor the Supreme Court of Oregon[158] attempts to employ the elements of the foregone conclusion doctrine.

Further, the Supreme Court of Oregon established precedent that the State can waive the testimonial aspects of decrypting a device without first requiring the State to show prior knowledge of the contents of the device.[159] The court accomplished this by allowing the state to "not use defendant's act of unlocking the phone as evidence; [the State] would only use it to gain access to the phone."[160] This is contrary to *Fisher*'s finding that the existence of, and access to, evidence is testimonial in and of itself.[161] According to *Pittman* the "testimonial aspects of the act have constitutional significance,

---

152 *Pittman*, 300 Or. App. at 149.

153 *Id*. at 150.

154 *Id*. at 151–52.

155 *Id*. at 161 ("The state did not need to establish, however, that the contents of the iPhone were a foregone conclusion.").

156 *Id*.

157 *See generally Pittman*, 300 Or. App.

158 *See generally* State v. Pittman, 376 Or. 498 (2021).

159 *Id.* at 523–26 ("[T]he state informed the court that it would not use defendant's act of unlocking the phone as evidence; it would use it only to gain access to the phone…[we] permit an order compelling a defendant to unlock a cell phone so long as the state…is prohibited from using defendant's act against defendant, except to obtain access to the contents of the phone.").

160 *Id*. at 523–24.

161 Fisher v. United States, 425 U.S. 391, 411 (1976) ("Surely the Government is in no way relying on the "truthtelling" of the taxpayer to prove the existence of or his access to the documents.").

which we must address; the access that the act provides does not."[162] This reasoning ignores the fact that if the government does not have prior knowledge of the existence of the evidence, then the evidence itself becomes testimonial by communicating its own existence.

The existence of the evidence and the defendant's access to it are communicative of a relationship between the evidence on the digital device and the defendant.[163] The *Fisher* Court allowed the government to demand the production of the tax documents because the government already knew these documents existed in the possession of a third-party, the defendants' attorneys.[164] *Pittman* correctly asserts that the evidence is not protected[165] but the *Pittman* court is wrong to think the government can waive the testimonial nature of opening the device to provide evidence the government did not previously know of. Without prior governmental knowledge of the existence of the evidence, the evidence's own existence is testimonial as it speaks against its owner and communicates the defendant's access to it. Therefore, the existence of the evidence should be protected until the government can show knowledge that the evidence's existence is a foregone conclusion. The existence, the access, the relationship between defendant and the evidence, etc.[166] are the communicative and testimonial aspects that the foregone conclusion element exists to protect.

The *Pittman* case further demonstrates the delicate nature of formulating exceptions to constitutional rights. Any concessions are likely to be further loosened over time, whether by the development of new circumstances or by misinterpretations in the applicability of the exception. And when the doctrine is loose enough, the courts may discard it altogether. For the viability of constitutional rights over time it is vital that exceptions to the rule be narrowly construed. The manner in which *Stahl* and its progeny flippantly turn over all

---

162 *Pittman,* 376 Or. at 525.

163 *Fisher*, 425 U.S. at 410 ("The act of producing evidence in response to a subpoena nevertheless has communicative aspects of its own, wholly aside from the contents of the papers produced. Compliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer.").

164 *Id*. at 411.

165 *Pittman,* 376 Or. at 525.

166 *Fisher*, 425 U.S. at 410.

encrypted digital devices does injustice to the careful protections that have surrounded the Fifth Amendment for years.[167]

The compulsion orders themselves are likely to lead to novel complications.[168] If suspects claim that they do not know or cannot remember their passwords, courts will have to consider when to punish the individuals for defying a compulsion order.[169] It would be a miscarriage of justice if individuals were held in contempt for genuinely not knowing a password. If the penalty for being held in contempt is less than the sentence for the crime the defendant is accused of, the defendant may engage in a cost-benefit analysis and strategically choose non-compliance.[170] The government must then show that the defendant willfully refused to comply or else the defendant may avoid any consequence for their noncompliance.[171] This could push courts and legislatures to escalate the penalty for being held in contempt. But it will be a struggle for the courts to determine whether the defendant was willfully noncompliant. The court sought to hold the *Pittman* defendant in contempt for providing the wrong password to the device and chose not to provide a written discussion of how it determined that Pittman was willful in her noncompliance.[172]

Further, hasty application of exceptions to constitutional rights will subject criminal defendants to arbitrary differences in their rights. The distinction between biometrics and alphanumeric passwords is particularly inconspicuous to lay people who will not realize that their legal rights change based on how they encrypt their devices. The recent court cases about compelled biometric

---

167 *See* Commonwealth v. Jones, 481 Mass. 540, 547 (2019) (Lenk, J., concurring); *see also* Pollard v. State, 287 So. 3d 649, 653–54 (Fla. Dist. Ct. App. 2019) (questioning *Stahl*'s reasoning for the sake of individual autonomy, concerns of governmental overreach, and the original understanding of the Fifth Amendment).

168 Kerr & Schneier, *supra* note 2, at 1004–05.

169 *Id*.

170 *Id*.

171 *Id*.

172 State v. Pittman, 300 Or. App. 147, 152 (2019) (rejecting the defendant's argument, without a written discussion, that the State did not show defendant's entering of the wrong password was willful non-compliance).

decryption have been discussed by technology news outlets.[173] It seems unfair to reward people under the law with their Fifth Amendment right for having access to legal news, following technology-related news, or for their preference on how to decrypt their device. Such a nuanced distinction is unfair. It creates inequitable results for criminal defendants that do not know that biometric decryption means their bodies can be used against them if the government wants access to their device. Many mobile phones,[174] tablets,[175] and some personal computers[176] are equipped with biometric decryption technology. This problem will only get worse as newer formats of decryption arise—leading to unpredictable results.

3. Scholarly Considerations for Finding a Solution

Scholars have offered their opinions on how to resolve the ambiguities in the applicability of *Fisher*'s foregone conclusion doctrine to compelled decryption. There is some consensus that the government cannot compel the defendant to write down or orally provide their password to an encrypted device.[177] Being compelled to provide the password orally or in written format would force a criminal defendant to reveal the contents of his or her mind.[178] Additionally, the foregone conclusion doctrine is built upon the act of producing something that was voluntarily created by the defendant

---

[173] *See* Lily Hay Newman, *Why Cops Can Force You to Unlock Your Phone with Your Face*, WIRED (Oct. 1, 2018), https://www.wired.com/story/police-unlock-iphone-face-id-legal-rights/ [https://perma.cc/Q8XH-HAZB].

[174] GLOBAL NEWSWIRE, *Global Consumer Biometrics Market Research Report 2020-2025* (Mar. 18, 2020), https://www.globenewswire.com/news-release/2020/03/18/2002724/0/en/global-consumer-biometrics-market-research-report-2020-2025.html [https://perma.cc/3TP6-UQLE] ("According to the Credit Suisse report, in 2018, the shipment of smartphones with fingerprint sensors worldwide stood at 1,082 million units.").

[175] *See* Xiomara Bianco, *Best Tablets with Fingerprint Sensors*, CNET (Apr. 5, 2017), https://www.cnet.com/news/best-tablets-with-fingerprint-sensors/ [https://perma.cc/9JZ7-ZE6N].

[176] *See* David Nield, *How to Log into Your Computer with Your Fingerprint or Face*, POPULAR SCI. (Apr. 24, 2018), https://www.popsci.com/computer-login-fingerprint-face/ [https://perma.cc/96YA-6P7N].

[177] Laurent Sacharoff, *What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr*, 97 TEX. L. REV. ONLINE 63, 64 (2019) [hereinafter *What Am I Really Saying*].

[178] *Id*. at 68.

prior to the government's involvement, preexisting the compulsion, rather than writing something down in response to the compulsion.[179] The question remains: can a court compel the criminal defendant to enter the password into the device to decrypt it?[180] In such circumstances, the defendant does not reveal the password but decrypts the device and provides the decrypted device to the government to search.[181]

First it must be determined what the act of decryption communicates.[182] While some scholars feel that decryption only reveals the defendant's knowledge of the password, others argue that decryption potentially communicates the defendant's dominion and ownership of the device and their knowing possession of the files on the device.[183] This point of contention is at the center of the issue of applying the foregone conclusion doctrine.[184]

Professor Laurent Sacharoff of the University of Arkansas School of Law points out that *Doe* would consider production to be testimonial for "implicit statements of fact."[185] This requires us to consider all the potential inferences that come from requiring a defendant to decrypt his or her device, including knowledge, possession of the device and its files, and authenticity.[186] According to Sacharoff, if decryption only reveals knowledge of the password, then for the decryption to be a foregone conclusion, the government need only show that the defendant knows the password.[187] However, if decryption reveals ownership of the device or possession of the files, then the government must first reveal independent knowledge of the files it seeks from the device.[188] Since the password is never

---

179 Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 FORDHAM L. REV. 203, 236 (2018) [hereinafter *Unlocking the Fifth Amendment*].

180 *What Am I Really Saying*, *supra* note 179, at 65.

181 *Id*. at 68.

182 *Id*. at 67.

183 *Id*.

184 *Id*.

185 *Id.* at 70 (quoting Doe v. United States, 487 U.S. 201, 209 (1988)).

186 *Id.* at 70–71.

187 *Id*. at 67.

188 *Id*.

produced and provided to the government because it is contents of the mind, the password itself cannot be the thing that is foregone.[189]

Some scholars feel the Fifth Amendment analysis here is altogether misplaced. If not, Professor Orin Kerr argues, then the Fifth Amendment protections provide an elevated protection, in comparison to Fourth Amendment protections, to defendants who encrypt their devices.[190] Kerr notes that once law enforcement obtains a warrant to search a house, they can search the house and the same should be true of digital devices.[191] Kerr advocates for a bright line rule that if the government can show that the defendant knows the password to the decrypted device and that they have the device and a court order, the defendant should not be able to assert a Fifth Amendment privilege.[192] This will prevent criminal defendants from hindering the effects of a search warrant by hiding behind a password.[193] Kerr feels that encryption technology is not an appropriate place for Fifth Amendment rules to apply because these rules will act as barriers on top of the Fourth Amendment protections already in place.[194]

Some scholars take a different approach: rather than pitting the value of one amendment against the other, we need to consider compelled decryption of a device seized by a warrant as a hybrid Fourth and Fifth Amendment question requiring its own unique analysis.[195] This approach would only allow the state to retrieve the specific files that they can describe with reasonable particularity prior to the defendant's compelled decryption.[196]

Some scholars are starting to take the view that perhaps such a flippant disregard for biometric encryption misses some important considerations.[197] The act of biometric decryption communicates the

---

189 *Id*. at 68.

190 Orin Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767, 794 (2019).

191 *Id.*

192 *Id.* at 783.

193 *Id.* at 794.

194 *Id*. at 796.

195 *Unlocking the Fifth Amendment*, *supra* note 181, at 250–51.

196 *Id.*

197 Price & Simonetti, *supra* note 21, at 42.

defendant's sole ownership and dominion over the device as well as exclusive control and ownership of the files on the device.[198]

III. SOLUTIONS FOR THE FIFTH AMENDMENT: SETTING BOUNDARIES FOR THE FOREGONE CONCLUSION DOCTRINE

A. Stop Stahl-*ing: The Future of the Fifth Amendment*

Ideally, legislature should establish guidelines to provide the proper balance of protecting criminal defendants from compelled decryption in the scenarios where the act of decryption retains its testimonial nature and is not a foregone conclusion. However, in the absence of such efforts, the Supreme Court should grant certiorari to the next case on topic to clarify the doctrine.

1. Take a Case-by-Case Approach

It must be determined what the act of decryption communicates. Realistically, the act of decryption communicates different things in different scenarios. As Professor Sacharoff points out this may depend upon what the government is looking to gain from the compelled decryption.[199] A different analysis may be necessary when the government knows the digital device has been used for illegal activity and seeks to confirm ownership; or when the government is seeking evidence from the device; or when the government is seeking content on the device to lead to a different source of evidence.

A case-by-case approach is superior to Professor Kerr's suggestion for a bright line rule because the foregone conclusion may apply differently in different scenarios. Kerr's recommendation for a bright line rule rests on his assertion that unlocking a device only implicitly communicates knowledge of the password.[200] This disregards the other testimonial qualities of decryption such as dominion over the phone, ownership of the files on the phone and the authenticity of the files.[201] *Stahl*'s assertion that passwords are self-

198 *Id.*
199 *What Am I Really Saying*, *supra* note 179, at 67.
200 Kerr, *supra* note 192, at 779.
201 *What Am I Really Saying*, *supra* note 179, at 67.

authenticating[202] is an indication that the courts will utilize the password's entry to communicate more than mere knowledge of the password. Cases may occur where decryption of the password will only reveal knowledge of the password. However, a one-size fits all approach misses the mark of preventing criminal defendants from having to provide testimony against themselves.

2. Passwords Are Vehicles, They Are Not the Foregone Evidence

The Court should find that passwords are not evidence but rather a means to obtain the evidence. The foregone conclusion should not apply to passwords because it is not the evidence the government seeks.[203] The concept of passwords is not new to Fifth Amendment jurisprudence. Both the *Doe*[204] and *Hubbell*[205] cases acknowledged passwords can come between the government and evidence but felt that while physical keys can be surrendered, cognitively memorized combinations cannot be compelled. The holding in *Hubbell* turned on the fact that the government could not independently state what papers it sought.[206] The Court felt the government should have provided a specific demand, guiding the defendant to the documents they sought, to show they already knew of these documents to warrant their surrender.[207] The foregone conclusion doctrine is supposed to apply to evidence that the government already knows about, thereby removing the sting of compelling the defendant to provide it to the government. If the government merely has to know that the defendant has the password to their own phone in order to be able to compel him/her to provide it so they can search for evidence, that is likely to leave quite the sting.

This protection is especially important for crimes where possession of certain digital content is an element of the crime, as opposed to when the government is seeking evidence that helps investigate a different crime. For crimes where possession of digital content is an

---

202 State v. Stahl, 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016).
203 G.A.Q.L. v. State, 257 So. 3d 1058, 1063 (Fla. Dist. Ct. App. 2018).
204 Doe v. United States, 487 U.S. 201, 210 n.9 (1988).
205 United States v. Hubbell, 530 U.S. 27, 43 (2000).
206 *Id.* at 44–45.
207 *Id.*

element of a crime, the foregone conclusion exception must be used even more stringently and only once the government can show, from an independent source, that the defendant is guilty. Perhaps for such crimes, compelling the individual to open their phone should only be used for sentencing purposes.

3. Criminal Defendants Are Entitled to the Proper Functioning of Both the Fourth & Fifth Amendment

The boundaries of the Fourth and Fifth Amendment should not be blurred. While the Fourth Amendment is concerned with privacy,[208] the Fifth Amendment is concerned with avoiding compulsion leading to the cruel trilemma.[209] Despite the challenges of obtaining evidence in modern society and for modern crimes, the autonomy to not be coerced to implicitly say "I did it" by actions is not merely an added inconvenience to Fourth Amendment searches. Careful consideration of, among other things, all the possible testimonial qualities that can be expressed, the way data is stored, the types of information that can be stored without the user's knowledge, and the evidentiary methods by which files can be authenticated and assigned to the users, is necessary to determine the impact of new technology on the doctrine's application to the rights of criminal defendants. Fifth Amendment protections must prevail as long as the compelled action provides any testimony. Therefore, compelled decryption must be subject to the extra burden of the elements of the foregone conclusion doctrine. Professor Kerr and Professor Sacharoff diverged on the topic of how these two amendments are both at work.

a) Taking the Fourth Amendment Too Far

Professor Kerr argues that if the government can show that the suspect knows their password, then there should be no Fifth Amendment privilege against compelled decryption.[210] Kerr reasons that defendants should not be permitted to employ the Fifth Amendment as an additional burden to the government's Fourth Amendment

---

208 Fisher v. United States, 425 U.S. 391, 400 (1976).

209 *Id.*; Pennsylvania v. Muniz, 496 U.S. 582, 596–97 (1990).

210 Kerr, *supra* note 192, at 783.

burdens of finding probable cause and acquiring a search warrant.[211] Kerr states that if the government can show that the phone is in the defendant's possession and the phone responds to a phone number known to belong to the defendant, then the foregone conclusion should apply.[212]

This does not reach the level of particularity that the Supreme Court has utilized in prior Fifth Amendment cases considering the testimoniality of producing incriminating evidence. So far, the three Supreme Court cases on point consist of two occasions where the government acquired the documents they sought from a third party,[213] and therefore, did not require the defendant to provide evidence against himself, and more recently, where the Court decided not to expand the doctrine to avoid governmental overreach when they could not specify what evidence they wanted.[214] The government must therefore, carry a heavier burden than showing the defendant possessed the digital device.

One way to think about the divide between the Fourth and Fifth Amendment in the context of compelled production is the difference between the government's right to take and the right to demand the defendant to provide. If the government has probable cause and can obtain a proper warrant, they are entitled to take possession of, or seize, and search according to the parameters set forth on the warrant.[215] But this is entirely distinct from what the government can demand the defendant to provide. The government is not prohibited per se from demanding evidence from the defendant, but the government is limited from demanding anything that is testimonial or would provide the government with more than what they previously had.[216] This is tricky because the evidence itself is not protected,[217] it is the potential communication that is communicated when

---

211 *Id.* at 788.

212 *Id*. at 783.

213 *Fisher*, 425 U.S. at 409 (serving summonses on the attorneys of the individuals under investigation by the IRS); Doe v. United States, 487 U.S. 201, 215 (1988) (seeking to obtain a consent directive from defendant to obtain account records from the banks).

214 United States v. Hubbell, 530 U.S. 27, 44–45 (2000).

215 Chimel v. California, 395 U.S. 752, 762 (1969).

216 *Hubbell*, 530 U.S. at 34.

217 *Fisher*, 425 U.S. at 407.

providing the evidence that is protected for its testimonial potential.[218] The foregone conclusion doctrine arose to shrink this protection in instances when the production of the demanded evidence would not be testimonial.[219] This prevents the defendant from protecting evidence once the government already has some level of knowledge from an independent source that the evidence exists.[220]

Herein lies the value of the elements of the foregone conclusion doctrine. The government should not be able to guess that evidence is likely to exist and demand it. For the government to assert that the defendant must provide self-incriminating evidence against their will, the government must carry the burden of showing they knew of this evidence anyway.[221] This reduces the sting of being forced to testify against yourself; the government already knew you had this evidence, so providing it minimizes what you must do against your free will.

Kerr's comparison to the law enforcement officers that have a search warrant to search a house therefore does not work.[222] He never asserts that encrypting one's digital devices is wrong or illegal in any way.[223] If people can encrypt their devices, then even if this seems like a nuisance on top of the Fourth Amendment, the ability to decrypt digital devices is merely a consequence of the advancement of technology. And while encryption is utilized for privacy purposes, and therefore, would seem at first blush to be a Fourth Amendment problem,[224] the modern reality is that this is something the government has to demand from the defendant. Being that the act of decryption can be communicative, this brings in the Fifth Amendment.[225] Decryption creates a practical and legal wedge between the government's possession of the device and the government's possession of the data on the device. This is true despite the fact that if encryption did not exist, then the government would not

---

218 *Hubbell*, 530 U.S. at 36.
219 *Id.* at 44.
220 *Id.* at 44–45.
221 *Id.* at 45.
222 Kerr, *supra* note 192, at 794.
223 *See generally id.* at 767.
224 *Id.* at 787.
225 *What Am I Really Saying*, *supra* note 179, at 67.

need the defendant's assistance. Perhaps if encryption did not exist, people would not utilize their devices the same way and such evidence would not exist.

Additionally, Kerr's approach does not consider the full potential for "implicit statements of fact" that decryption might convey, aside from knowledge of the password.[226] Decryption also implies dominion over and possession of the device as well as access and possibly ownership over the evidence on the device.[227] These implications make decryption testimonial,[228] which makes it important to examine every situation individually and consider all possible implications. The protections of the Fifth Amendment must apply if decryption communicates something that the government did not previously know.

b) Restricting the Fourth Amendment Too Much

Professor Sacharoff's approach, by contrast, shortchanges the Fourth Amendment. He recommends that in compelled decryption cases, a potential solution against overbroad requests would be to limit the defendant's compelled decryption of the device to only provide the government access to the specific files the government can independently describe with reasonable particularity.[229] According to Sacharoff, this hybrid approach harmonizes the values of both the Fourth and Fifth Amendments rather than pitting them against each other.[230] Sacharoff acknowledges that this approach suffers shortcomings related to sentencing for possession-based crimes[231] but notes that it offers definite Fourth and Fifth Amendment protections through its "antifishing" limitations.[232]

Using the foregone conclusion doctrine to limit governmental access to only specific files is expanding the reasonable particularity

---

226 *Id.* at 70 (quoting Doe v. United States, 487 U.S. 201, 209 (1988)).

227 *Id.* at 67.

228 *See id*. at 70.

229 *See Unlocking the Fifth Amendment*, *supra* note 181, at 250–51.

230 *See id.* at 245.

231 *See id.* at 239–44 (noting that for possession-based crimes, the amount of illicit content may be a consideration in sentencing, such that limiting the government's access to the files it was able to describe independently may provide the defendant with a lower sentence than they actually deserve).

232 *Id.* at 245.

standard too far by requiring too much specificity. This is true because Sacharoff's proposal limits the government's ability to acquire evidence to the specific files that it must already know of.[233] *Fisher* permitted the government to request documents as unspecified as "[r]etained copies of reports and other correspondence between Tannebaum Bindler & Lewis and Dr. E. J. Mason during 1969, 1970 and 1971."[234] While some of the documents demanded in *Fisher* were referred to specifically, the above-quoted demand lacks specificity on what "reports and other correspondences" might refer to other than a footnote that narrowed this demand to "original letters sent from the accountant to the taxpayer."[235] This demand lacks specificity and is capable of referring to a small range of content, rather than one specific document, which shows that *Fisher* did not expect the foregone conclusion doctrine to limit the government in such an exacting manner.

Sacharoff's approach will not work for all the situations in which such compulsion orders can arise. The government could be seeking pictures saved to or created on the device, an audio clip from a longer recording, documents created or downloaded on the device or sections of a document, text messages, phone call history, social media access, browsing history, other internet engagement information, global positioning system information, etc. Alternatively, the government could be seeking to determine if the defendant deleted files, whether the device utilizes a certain application or program, or how many times the defendant accessed a certain application or program. The government may seek metadata, which has to be handled delicately because metadata is easily altered through normal usage of the device or retrieval of files.[236] For some of these potential types of evidence, it is not a specific file that the government seeks. It could be the data about the file, the lack of the file, only a selected portion of the file, information about the applications or programs on the device, etc. In such circumstances, a rule

---

233 *Id.*

234 Fisher v. United States, 425 U.S. 391, 394 (1976).

235 *Id.* at 413 n.13.

236 *See* Justin Boncaldo, *DFS 8: Metadata in Forensics*, BONCALDO'S FORENSICS BLOG, https://boncaldoforensics.wordpress.com/2019/02/16/dfs-8-metadata-in-forensics/ [https://perma.cc/U9MC-3E8T].

that requires the government to have specific knowledge to describe a file may place information off-limits to the government in a way that *Fisher* is not likely to have intended.

This approach also does not explain the extent to which the government must be able to describe the file it seeks. How would a situation be handled if the government has a witness that saw an illicit photo of a child on the defendant's device, but upon opening the device, the defendant has multiple photos that fit the description? The question then becomes which photo does the government get. Sacharoff's approach is oversimplified and would prove clunky in practice.

Additionally, while the desire to protect against overzealous forensic investigations is appreciable, the Fifth Amendment is not the right "place" for these concerns. This approach risks conflating the values of two amendments. The Fifth Amendment is not supposed to prevent fishing expeditions, as the Fifth Amendment does not protect privacy or evidence.[237] The Fifth Amendment protects against the testimonial nature of producing evidence.[238] The Fourth Amendment is supposed to manage privacy concerns by limiting the government's search of a seized device as prescribed by the search warrant.[239] When the privacy amendment itself is inadequate to prevent governmental fishing expeditions[240] another amendment cannot solve the problem. Once the foregone conclusion applies by the government's showing of independent knowledge, by reasonable particularity, of the files it seeks from the device, it is up to the protections of the Fourth Amendment to take over and limit the search to what is outlined on the search warrant. This is where Kerr's house comparison comes in;[241] once the government has access, we must trust that they will abide by the warrant. The Fifth Amendment is not a guardian to prevent abuses of the Fourth Amendment.

---

237 *See Fisher*, 425 U.S. at 407.

238 *See id.*

239 *See* Kerr, *supra* note 192, at 788.

240 *See Unlocking the Fifth Amendment*, *supra* note 181, at 251.

241 *See* Kerr, *supra* note 192, at 794.

4. Define the Standard of the Foregone Conclusion Doctrine

The Supreme Court needs to clarify what the reasonable particularity standard applies to. Aside from the lack of clarity regarding the level of certainty required to show reasonable particularity, it is also unclear what the government must show this standard in relation to. Reasonable particularity could apply to how specifically the government must be able to describe the evidence that it is seeking.[242] Alternatively, reasonable particularity could refer to the government's level of certainty of the existence, location, and authenticity of the evidence it seeks.[243]

The reasonable particularity standard should apply to the government's ability to show, with some level of certainty, their prior knowledge that relevant evidence exists. Requiring the government to be too specific in describing the evidence they are seeking will lead to a rule that is only applicable in some circumstances.[244] In *Fisher*, the government knew the types of documents they sought but they did not know enough to specifically describe each individual document.[245] If the level of specificity with which the government must demand particular pieces of evidence is too high, then the doctrine will lose its value to the government. Since the evidence itself is not protected, they need not already know the specifics of what the evidence will provide, but the government must know that it is exists, its location, and that it is authentic.

Considering this issue from the opposite perspective, in *Stahl*'s case, the government would have easily been able to describe what they expected to find on his iPhone by the nature of the crime he was accused of.[246] They were seeking files showing that he took inappropriate video and/or photographic content of a female customer in a store because that is the crime he was accused of.[247] In order for the government's burden to have any meaning under such

---

242 *See id.* at 775.

243 *See id.*

244 *See supra* Section g)

245 Fisher v. United States, 425 U.S. 391, 394 (1976) (seeking to obtain several types of tax documents, reports, and related correspondences between the taxpayers and their accountants).

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

247 *Id.* at 129.

circumstances, the government must show their investigative work provided them with some level of independent prior knowledge of the existence, location, and authenticity of the evidence they seek.

5. Clarify the Elements of the Foregone Conclusion Doctrine

The Supreme Court should also clarify whether or not possession falls within the elements of the foregone conclusion. Some courts have used possession as interchangeable with the location element.[248] This confusion stems from the fact that *Fisher* lists three ways the act of production could be communicative: (1) by admitting possession, (2) control, and (3) the existence of the produced items.[249] However, subsequent courts have confused these three communicative aspects of production with the three elements the government must show to carry its burden for application of the foregone conclusion doctrine: (1) existence, (2) location, and (3) authenticity.[250]

Possession, or more precisely dominion, should only be a component of the locational element. If the government cannot independently show that the defendant has some level of control over the device, then the government cannot threaten a contempt order to force defendant to open the device. However, this is not the sole burden of the location element; the government cannot merely state that they believe evidence to be "on defendant's digital device." The government retains the responsibility of producing some other information to prove that they have prior independent knowledge that a specified location on the device contains the evidence that government already knows, with reasonable particularity, to exist on the device. The locational element of the foregone conclusion carries the potential to be the proper place to address the "antifishing" Fourth Amendment concern[251] expressed by some scholars. A well outlined search warrant stating precisely how the device will be searched could constitute the locational element of the foregone conclusion doctrine and be the mechanism for harmonizing the

---

248 *See In re* Single-Family Home & Attached Garage, 2017 U.S. Dist. LEXIS 170184, at *3 (N.D. Ill. Feb. 21, 2017).

249 *Fisher*, 425 U.S. at 410.

250 *See Stahl*, 206 So. 3d 124, 130.

251 *See Unlocking the Fifth Amendment*, *supra* note 181, at 245.

Fourth and Fifth Amendment without losing the values behind either of them.

6. Protect the Authenticity Element of the Foregone Conclusion Doctrine

The Supreme Court should call out *Stahl*'s rejection of the need to authenticate digital content. If the password self-authenticates the contents of the device, then providing the password becomes testimonial by communicating the authenticity of the contents of the device.[252] To maintain *Stahl*'s self-authenticating password proposal, the government would have to independently prove authenticity of the content on the device prior to compelling the defendant to decrypt the device.[253] While authenticity has a low standard[254] as its "burden of proof is slight,"[255] authenticity should still be a valid evidentiary objection for defendants.

B. Biometrics Are Not Physical Acts, They Are Passwords!

Biometric decryption has taken a hard hit in modern Fifth Amendment jurisprudence.[256] However, the Supreme Court should contemplate the value of considering all encryption formats the same. The fact that biometrics are not contents of the mind does not mean biometric decryption cannot be testimonial.

It seems arbitrary and inequitable that an exception to the Fifth Amendment which prevents an individual from being compelled to unlock their device is afforded to those who use an alphanumeric passcode but not to those who use face ID or fingerprints to encrypt

---

[252] *Stahl*, 206 So. 3d at 136 (stating that the technology and the password are self-authenticating but this was based on the court's presumption that the password was what the foregone conclusion applied to rather than the contents of the device).

[253] *See* Kerr, *supra* note 192, at 773–74.

[254] *See* United States v. McGlory, 968 F.2d 309, 328–29 (3d Cir. 1992) (quoting United States v. Goichman, 547 F.2d 778, 784 (3d Cir. 1976)) ("The showing of authenticity is not on a par with more technical evidentiary rules….The only requirement is that there has been substantial evidence from which they could infer that the document was authentic.").

[255] McQueeney v. Wilmington Tr. Co., 779 F.2d 916, 928 (3d Cir. 1985).

[256] *See In re* Search Warrant Application, 279 F. Supp. 3d 800, 801 (N.D. Ill. 2017); Matter of White Google Pixel 3 XL Cellphone in a Black Incipio Case, 398 F. Supp. 3d 785 (D. Idaho 2019); Commonwealth v. Baust, 89 Va. Cir. 267, 267 (Va. Cir. Ct. 2014); United States v. Barrera, 415 F. Supp. 3d 832, 842 (N.D. Ill. Nov. 22, 2019).

their devices. Creating a Fifth Amendment distinction based on the format of decryption will create inequitable results for defendants that do not know that biometric decryption means their bodies can be used against them if the government wants access to their device.

If no bright line rule is established on this matter, newer formats of encryption will lead to unpredictable holdings. What about unlock patterns?[257] Unlock patterns represent both physical gestures and the memory of the user. Figuring out whether such a decryption method is a mental exercise or a physical action would be a waste of court time. With rapid technological advancements, we do not know what will come next. The legal system should strive to encourage innovation of technology rather than stifling it with the fear that new technology will expose individuals to differential rights. "It has been repeatedly decided that [the Fifth Amendment] should receive a liberal construction, so as to prevent stealthy encroachment."[258]

Moreover, one of *Doe*'s subtler footnotes paves the groundwork for understanding the difference between physical acts of being the evidence and being compelled to perform actions that leads to evidence.[259] Decrypting a device regardless of format is an additional step towards providing evidence against oneself. A defendant should not be compelled to provide the government with access to self-incriminating evidence unless it is actually a foregone conclusion. Therefore, the Court should distinguish decryption by biometrics from the physical acts of actually being the evidence, such as by providing blood samples or voice exemplars.[260]

Furthermore, in *Matter of Residence of Oakland*,[261] the court noted that biometrics are functionally the same as passwords

---

[257] An unlock pattern requires tracing a prespecified number of points which forms a pattern that unlocks the device.

[258] Fisher v. United States, 425 U.S. 391, 417 (1976) (quoting Gouled v. United States, 255 U.S. 298, 304 (1921)).

[259] Doe v. United States, 487 U.S. 201, 211 n.10 (1988) ("[T]he Court distinguished between the suspect's being compelled himself to serve as evidence and the suspect's being compelled to disclose or communicate information or facts that might serve as or lead to incriminating evidence.").

[260] *See* State v. Diamond, 890 N.W.2d 143, 150 (Ct. App. Minn. 2017).

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

because various security features of most cell phones can render biometric access functionless, necessitating password entry to open the device.[262] While providing fingerprints may have once been merely a physical act for identifying the defendant, the legal system must reexamine its understanding of this action now that fingerprints can provide "a direct link to communicative, as well as potentially incriminating information."[263] The same is true for other formats of biometric decryption.

Courts cannot ignore the communicative nature of biometric decryption. Once the device perceives the unique combination of physiological features of the device owner's face or fingerprint, it provides the user-chosen password[264] to decrypt the key which in turn decrypts the device. Biometric decryption identifies the encrypted device's owner by responding to their unique physiological features. Unlike a password-protected phone, biometric decryption typically can only be accomplished by the person with the specific features the encryption was established with.[265] This is communicative that the individual that biometrically decrypts the phone is likely the *only* person with control over the device and its contents. Password protected devices allow anyone who knows the password to utilize the device. Regardless of the format of encryption, decrypting the device still concedes the defendant possessed and controlled the device and its contents. The communication of confirming the owner's identity, sole access, and dominion over the device and its files makes compelled biometric decryption testimonial, unless the device's contents are otherwise a foregone conclusion. Therefore, biometric decryption should not flippantly be categorized as an unprotected physical act under the Fifth Amendment.

C. The Problems

Some speculate that stringent Fifth Amendment protections will lead the government to rely more heavily on the workaround

---

[262] *Id*. at 1015–16 (quoting the government's own concession that when the phone has been turned off, restarted, inactive, or has not been unlocked for a certain amount of time, only the password will open the device).

[263] *See* Goldman, *supra* note 8, at 211.

[264] *See* Price & Simonetti, *supra* note 21, at 42.

[265] *See* Jenkins, *supra* note 126.

methods of the Fourth Amendment, such as increased surveillance.[266] Such a threat is a viable concern, but the fact that the government can impede one right does not mean we should not protect another. The focus of this Note is to argue for strict adherence to the spirit of the Fifth Amendment; however, the Court may find that this sets a burden that is too high for the government in fighting certain possession-based digital crimes which the government has an undeniably strong interest in fighting, such as child pornography.

CONCLUSION

Currently, the foregone conclusion doctrine requires some clarification. The Supreme Court must address several issues in order to provide equitable and consistent results across all U.S. cases. Different scenarios will require a customized approach to address the particular potential implicit testimonial communications of each situation. Courts must acknowledge that passwords are not evidence, but a vehicle to access evidence. The Fourth and Fifth Amendment must be seen individually for the unique protections they each provide to criminal defendants. The foregone conclusion doctrine must be developed to determine when it applies, to what it applies to, the appropriate standard for its application, and what burden each element poses to the government. Biometrics should be treated the same as alphanumeric passwords under the law because of the testimonial features of compelled biometric decryption and to avoid disparate treatment under the law. The spirit of the bill of rights' protection of criminal defendants must be preserved. Ultimately, the challenges posed to law enforcement by the advancement in technology does not justify abridging a criminal defendant's Fifth Amendment right.

---

266 *See* Caren Myers Morrison, *The Intersection of Facebook and the Law: Symposium Article: Passwords, Profiles, and the Privilege Against Self-Incrimination: Facebook and the Fifth Amendment*, 65 ARK. L. REV. 133, 158 (2012).