Journal of Law and Health

Volume 36 | Issue 2 Note

5-1-2023

Face Off: Overcoming the Fifth Amendment Conflict Between Cybersecurity and Self-Incrimination

Zachary E. Jacobson
Cleveland State University College of Law

FACE OFF:
OVERCOMING THE FIFTH AMENDMENT CONFLICT BETWEEN CYBERSECURITY AND SELF-INCRIMINATION

Zachary E. Jacobson

TABLE OF CONTENTS

I. INTRODUCTION

The average lifespan of a smartphone is 2.75 years.[1] As time progresses, more of the 290 million smartphone users in the United States[2] will be pushed towards using more secure biometric encryption methods such as face ID and fingerprint ID, already found on many smart devices.[3] Cybercriminals might not struggle to overcome a simple 4-6 digit password on an individual's smartphone, but it is considerably more difficult for hackers to replicate an individual's fingerprint or the complexities of a person's face.[4] While an individual's phone is far more secure from cybercriminals thanks to biometric encryption, it runs the risk of being quite easily compromised should that person have an encounter with law enforcement.[5]

In a majority of jurisdictions, the Fifth Amendment protects an individual from being compelled to declare one's password to unlock his or her personal smart device.[6] On the other hand, no such universal protection is granted to individuals who refuse to present their fingerprint or face scan in order to open a biometrically encrypted device.[7] In this legal setting, a smart device with the 6-digit password of "1-1-1-1-1-1" is more constitutionally protected from government intrusion than the most recent biometric encryption found on most cutting edge smart devices.

Say for example you and your crazed conspiracy-loving Uncle Jeff go to buy the most popular model of smartphone in the United States, the iPhone 12 Pro.[8] You and Jeff each purchase an iPhone 12 Pro and begin setting up your respective devices. As you set up your device, you are prompted with an opportunity to set up facial recognition as well as a password. You select your password and begin scanning your face in order to biometrically encrypt your phone. Jeff sets up a password but refuses to set up a FaceID profile because of his fears of what the government or aliens might do with it. You both complete the setup of your phones but later, you are both implicated in an illegal gambling organization thanks to one of Jeff's conspiracy buddies. Law enforcement obtains valid warrants to search both, your and Jeff's, new iPhones in connection to the gambling. Law enforcement attempts to get Jeff to open his phone, but he refuses – law enforcement must leave Jeff's phone be because they cannot compel Jeff to say or type his password. However, if you were to refuse, it is likely that you could be found in contempt of court

---

[1] *Average lifespan (replacement cycle length) of smartphones in the United States from 2014 to 2025*, STATISTA, https://www.statista.com/statistics/619788/average-smartphone-life/ (last visited Nov. 4, 2021).

[2] *Smartphones in the U.S. – Statistics & Facts*, STATISTA, https://www.statista.com/topics/2711/us-smartphone-market/#dossierKeyfigures (last visited November 4, 2021)..

[3] Diego Poza, *What Is Biometric Authentication? 3 Trends for 2021*, AUTH0 (Oct. 22, 2021), https://auth0.com/blog/3-critical-trends-in-biometric-authentication-in-2019/.

[4] Louis Columbus, *Why Your Biometrics Are Your Best Password*, FORBES, (Mar. 8, 2020, 12:38 PM) https://www.forbes.com/sites/louiscolumbus/2020/03/08/why-your-biometrics-are-your-best-password/?sh=202bf3596c01.

[5] Kendall Howell, *The Fifth Amendment, Decryption, and Biometric Passcodes*, LAWFARE, https://www.lawfareblog.com/fifth-amendment-decryption-and-biometric-passcodes (last visited Nov. 27, 2017).

[6] Paul Rosenzweig, *Courts, the Fifth Amendment, and Biometric Encryption*, WONDRIUM DAILY, https://www.wondriumdaily.com/courts-the-fifth-amendment-and-biometric-encryption/ (last visited Sept. 20, 2021).

[7] *Id.*

[8] *Smartphones in the U.S. – Statistics & Facts*, *supra* note 2.

because you do not have a guaranteed Fifth Amendment privilege in your biometrically encrypted iPhone.[9]

The circumstances of this hypothetical scenario demonstrate a conflict between an individual's interest in securing their phone from cybercriminals against an individual's interest in the Fifth Amendment protection against self-incrimination. This note will begin to reconcile this conflict by observing it through the lens of cybersecurity, examining modern cases regarding the compulsion of biometric features in order to argue that such acts are testimonial and thus protected under the Fifth Amendment privilege against self-incrimination, and that the foregone conclusion doctrine should be limited in its application to biometric encryption cases. Part II of this note will provide meaningful background on an individual's right against self-incrimination under the Fifth Amendment and a brief history on encryption, authentication, and biometrics within the law. Part III of this note will examine two recent cases in which courts determined whether the compelled application of biometric features is a testimonial act. A comparison between the cases will indicate that courts should determine that the application of biometric features is testimonial in nature. Part IV will explore the application of the foregone conclusion doctrine, compare and contrast two different types of applications, and address how it should be applied within the context of the Fifth Amendment.

II. ORIGINS AND DEVELOPMENT OF THE FIFTH AMENDMENT PRIVILEGE AGAINST SELF-INCRIMINATION

The origin of the privilege against self-incrimination predates the Constitution and can be found within English Common law.[10] After the American Revolution, James Madison spearheaded several proposed amendments during a speech to the House of Representatives.[11] The Grand Jury Clause, Double Jeopardy Clause, Self-Incrimination Clause, Due Process Clause, and the Takings Clause all made it into the final draft of the Constitution.[12] The final draft of Fifth Amendment states that no person "shall be compelled in any criminal case to be a witness against himself."[13]

Since the states ratified the Constitution, the courts have been presented with complex legal issues regarding the Fifth Amendment that the Framers could have never anticipated. *Boyd v. United States* was the first Supreme Court case to take on the issue of self-incrimination in 1885.[14] In *Boyd*, the Supreme Court held that requiring a man to surrender his personal books and papers was unconstitutional under the Fifth Amendment.[15] The Supreme Court rationalized its holding by stating that it was wrong for the government to violate "the sanctity of a man's home and the privacies of life," and the

[9] United States v. Wright, 431 F.Supp.3d 1175, 1186 (D. Nev. 2020) (noting a difference in circuit decisions regarding the testimonial nature of biometrics).

[10] *Fifth Amendment – Rights of Persons*, GOVERNMENT PUBLISHING OFFICE 1272, 1302 (1992), https://www.govinfo.gov/content/pkg/GPO-CONAN-1992/pdf/GPO-CONAN-1992-10-6.pdf.
[11] *James Madison's Proposed Amendments to the Constitution,* CENTER FOR LEGISLATIVE ARCHIVES (1789), https://www.archives.gov/files/legislative/resources/education/bill-of-rights/images/handout-2.pdf. f
[12] U.S. CONST. amend. V.
[13] *Id.*
[14] Boyd v. United States, 116 U.S. 616 (1886).
[15] *Id.* at 634-35.

violation of a private citizen's property necessitated protection under the Fifth Amendment privilege against self-incrimination.[16]

In *Blau v. United States,* the Supreme Court established that the privilege against self-incrimination protected testimony that itself would support a conviction but also protected testimony that led to a "link in the chain of evidence needed" to support the conviction.[17] *Blau's* holding means that both the compelled responses that directly support conviction *and* any response that has an evidentiary link in the chain of evidence needed to support conviction receive protection.[18] The Supreme Court further established its rationale for the privilege against self-incrimination in *Ullman v. United States*.[19] The court noted that "too many…view this privilege as a shelter for wrongdoers. They too readily assume that those who invoke it are either guilty of crime or commit perjury in claiming privilege," and " the privilege against self-incrimination serves as a protection to the innocent as well as to the guilty, and we have been admonished that it should be given a liberal application."[20] While a liberal interpretation of the privilege against self-incrimination might hinder government efforts and allow some guilty people to escape, the privilege serves a greater purpose in protecting citizens from abuse by law enforcement.[21]

The case that defined the privilege against self-incrimination as we know it today was *Fisher v. United States.*[22] The Fisher court held that a case must meet three requirements in order to implicate the privilege against self-incrimination.[23] An individual must (1) be compelled by the government, (2) to give a testimonial communication, (3) that is incriminating.[24] The litigation originated from an IRS summons that required attorneys to produce incriminating documents related to income tax accusations against their own clients and the attorneys asserted their privilege against self-incrimination.[25] At question was the testimonial nature of the production of documents.[26] The *Fisher* court specified that the Fifth Amendment protects against compulsion of testimony, and that testimony is not limited to verbal or written communications.[27] The court concluded that the act of handing over papers in response to a summons implicitly testified that the documents existed, they were in the Defendants' possession, and the papers surrendered were the specific documents the IRS was requesting, thus making them testimonial in nature.[28]

Fisher also established what is known as the foregone conclusion doctrine.[29] The foregone conclusion doctrine states that when the testimonial aspect of compelled testimony "adds little or nothing to the sum total of the Government's information…no constitutional rights are touched."[30] The *Fisher* court determined that the existence of the incriminating documents was a foregone conclusion as the government was not relying

---

[16] *Id.* at 630.
[17] Blau v. United States, 340 U.S. 159, 161 (1950).
[18] *Id.*
[19] Ullmann v. United States, 350 U.S. 422 (1956).
[20] *Id.* at 426-27.
[21] *Id.* at 428.
[22] Fisher v. United States, 425 U.S. 391 (1976).
[23] *Id.* at 401.
[24] *Id.*
[25] *Id.* at 394-95.
[26] *Id.* at 394.
[27] *Id.* at 410-11.
[28] *Id.* at 414.
[29] *Id.* at 411.
[30] *Id.*

exclusively on the "truthtelling" of the taxpayer to prove the existence of the documents.[31] The result here is that the evidence that is compelled goes from protected to unprotected because the government could show courts that the evidence provided at issue has already been established and would provide little or nothing to the case at hand.[32] Courts are quite ambiguous as to the burden of proof required to establish that a conclusion is foregone.[33]

The foregone conclusion doctrine was expanded upon in *United States v. Hubbell*.[34] Hubbell was subpoenaed in relation to the Whitewater investigation, invoked the privilege against self-incrimination, and refused to state whether or not he had the documents that the Independent Council had requested.[35] Hubbell was granted immunity and supplied the documents but was indicted on tax and fraud charges.[36] The district court initially dismissed the charges because the evidence against Hubbell was derived from his immunized act, but the appellate court overturned the decision in order to determine whether the government had enough alternative proof or knowledge of the documents provided by Hubbell that his compelled production was a foregone conclusion.[37] The Supreme Court held even though the nature of the documents may not be protected, the act of producing them is testimonial because the act of production indicated Hubbell had control over the documents and acknowledged their existence.[38] The Court further reasoned that the Fifth Amendment protection against self-incrimination also includes compelled statements that lead to incriminating evidence, even though the statements themselves were not incriminating.[39] The government in *Hubbell* made no effort to show that it had specific knowledge of the documents it asked Hubbell to produce and Hubbell would have had to use "the contents of his own mind" in identifying the documents in the subpoena, and thus the government could not establish a foregone conclusion.[40] While *Hubbell* specified the scope of the foregone conclusion doctrine, it failed to distinguish the evidentiary threshold the government must establish before a court in order to show a foregone conclusion.[41]

A. Encryption, Biometrics, and Their Place in the Law

The almost universal technique for providing confidentiality and privacy for transmitted or stored electronic data is through encryption, which utilizes an encryption algorithm to secure data so that only individuals with decryption keys can access the data.[42] The practice of encryption can be traced back as early as the Kingdom of Egypt in 1900 BC, when spies would send protected information to others by encoding it through the use of predetermined codes.[43] Contemporarily, most smartphones utilize either Full Disk Encryption (FDE), which encrypts all data, applications, and services on one's device or

---

[31] *Id.*
[32] *Id.* at 412.
[33] Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. LAW REV. 767, 774 (2019).
[34] United States v. Hubbell, 530 U.S. 27 (2000).
[35] *Id.* at 30-31.
[36] *Id.*
[37] *Id.* at 31-32.
[38] *Id.* at 36-37.
[39] *Id.* at 44-45.
[40] *Id.* at 43.
[41] *Id.* at 45.
[42] WILLIAM STALLINGS & LAWRIE BROWN, COMPUTER SECURITY PRINCIPLES AND PRACTICE, 31-32 (4th ed. 2018).
[43] *A Brief History of Cryptography*, CYPHER RESEARCH LABORATORIES, http://www.cypher.com.au/crypto_history.htm (last visited Nov. 8th, 2021).

File Based Encryption (FBE), which encrypts large quantities of files or data within the phone individually.[44] In order to access an FDE or FBE encrypted device's data and applications, users must provide some form of authentication in order to demonstrate they are the authorized user and the data can then be decrypted into a discernable form.[45] Authentication can be password-based, such as the 4-6 digit numerical passwords offered on Apple devices.[46] Authentication can also take place through biometrics, which authenticate a user based upon "his or her unique physical characteristics."[47] This type of authentication identifies complex patterns found in one's fingerprints, hand geometry, facial characteristics, retina, etc.[48] Biometric authentication offers several advantages over password-based encryption. Biometric passwords provide high levels of security and assurance because biometric information is exclusive to each individual person, it provides a fast and easy user experience through seamless and effortless use, and it is difficult to fake or replicate.[49] Due to these advantages the smartphone industry is shifting towards biometric encryption, and it is estimated that by 2024, 66% of smartphone owners will use biometrics for authentication.[50]

As mentioned above, *Fischer* and *Hubbell* established that the Fifth Amendment protects people from being forced to incriminate themselves when the government compels testimony of the defendant's own mind. This privilege does not traditionally apply to acts of production for real or physical biometric evidence.[51] Most courts and scholars agree that compelled disclosure or statement of passwords is testimonial, and that requiring individuals to disclose a password is a Fifth Amendment violation.[52] However, courts vary greatly when it comes to compelled entry of passwords. The Massachusetts Supreme Court has held that one can be compelled to unlock their phone if it is their phone and there is reason to suspect they know the password, while the Indiana Supreme Court has held that the government cannot make an individual unlock their phone unless the investigators already know the incriminating information on the phone.[53] Some courts do not distinguish clearly between compelled disclosure of password by a statement and compelled unlocking

---

[44]Tyler Campbell, *Mobile Device Encryption*, INFORMATION SECURITY – A SHARED RESPONSIBILITY, https://infosec.conncoll.edu/uncategorized/mobile-device-encryption/ (May 24, 2022).

[45] STALLINGS & BROWN, *supra* note 42, at 64.

[46] *Id.* at 66.

[47] *Id.* at 67.

[48] *Id.* at 88.

[49] ANN CAVOUKIAN & ALEX STOIVOV, BIOMETRICS THEORY, METHODS, APPLICATIONS, 655-56 (Nikolaos Boulgouris ed., 2010).

[50] *By 2024, How Many Smartphone Owners Will Use Biometrics?*, PAYMENTSJOURNAL, https://www.paymentsjournal.com/by-2024-how-many-smartphone-owners-will-use-biometrics/ (last accessed Nov. 20th, 2021).

[51] *See Schmerber v. California*, 384 U.S. 757 (1966) (holding that the ordered withdrawal of blood from a suspect does not violate the Fifth Amendment guarantee against self-incrimination since the results of the blood test were neither testimony or communicative in nature); *see also Gilbert v. California*, 388 U.S. 263 (1967) (holding the taking of handwriting exemplars does not violate the Fifth Amendment's protections against self-incrimination as it identifies a physical characteristic); *see also United States v. Dionisio*, 410 U.S. 1 (1973) (holding that compelling a defendant to provide a voice recording did not violate the Fifth Amendment's protection against self-incrimination if used solely to measure physical aspects of the voice).

[52] Orin Kerr & Laurent Sacharoff, *Compelled Decryption: Criminal Law & Procedure Practice Group Teleforum*, THE FEDERALIST SOCIETY, https://fedsoc.org/events/compelled-decryption (last visited May 23, 2022); *see also*, Commonwealth v. Davis, 220 A.3d 534 (Pa. 2019).

[53] Commonwealth v. Jones, 117 N.E.3d 702 (Mass. 2019); Seo v. State, 148 N.E.3d 952 (Ind. 2020).

of a device, despite precedent indicating otherwise.[54] State courts and federal courts have conflicting opinions regarding whether the Fifth Amendment permits the compelled application of biometric features to unlock an encrypted device.[55] While both state and federal courts have weighed in on compulsion of disclosing a password, inputting a password, and application of biometric features to unlock an encrypted device, the Supreme Court has not weighed in directly on any of these issues.[56]

III. COMPARISON OF FEDERAL DISTRICT COURT CASES

While federal district courts have only begun to litigate cases regarding the compulsion of biometrically encrypted devices, district courts have already reached different rulings.[57] The United States District Court of Nevada held that biometric authentication was testimonial, while The United States District Court for the Eastern District of Kentucky held that compelled biometric authentication was not testimonial.[58] This note will compare the rationale from both district court cases in order to argue that biometric authentication should be considered testimonial.

In *United States v. Wright*, Wright was indicted on two counts of possessing child pornography and moved to suppress the evidence, which was obtained when his phone was unlocked by being held to his face before a warrant had been administered.[59] Wright argues that the forcible extraction of his biometric data violated his Fifth Amendment right because it is testimonial as it reflects that he had sufficient control over the phone that he could unlock it with his face and reveals the contents of his mind.[60] The government argues that it was not testimonial because it was nothing more than the compelled display of identifiable characteristics and so there is no violation.[61] The *Wright* court acknowledges a split in court decisions regarding this issue before deciding that precedent concluding that biometric authentication is testimonial is more compelling.[62] The court distinguishes two key differences between a biometric unlock and a submitting to fingerprinting or a DNA swab.[63] A biometric feature is the same as a passcode in that it tells law enforcement that an individual has access to the device, and since passcodes are testimonial, biometrics should be too.[64] Secondly, unlocking a phone with one's face is the equivalent of testimony, in that the individual has unlocked the phone before and thus had some level of control over the phone.[65] The issue of a foregone conclusion did not present itself because the government did not present evidence that the Defendant had ownership or capability of opening the phone beforehand.[66]

In *In re Search Warrant No. 5165*, the United States applied for a search warrant requesting to compel any individual present during the execution of the warrant to provide

---

[54] *See generally* State v. Andrews,234 A.3d 1254 (N.J. 2020).
[55] United States v. Barrera, 415 F.Supp.3d 832, 838 (N.D. Ill.2019).
[56] *United States v. Wright*, 431 F.Supp.3d 1175, 1186 (D. Nev. 2020).
[57] *Id.* (noting a difference in circuit decisions regarding the testimonial nature of biometrics).
[58] *Id.* at 1188; In re Search Warrant No. 5165, 470 F.Supp.3d 715, 729 (E.D. Ky. 2020).
[59] *Wright* at 1179.
[60] *Id.* at 1186.
[61] *Id.*
[62] *Id.* at 1186-87.
[63] *Id.* at 1187.
[64] *Id.*
[65] *Id.* at 1188.
[66] *Id.*

biometrics in order to access seized electronic devices.[67] When the constitutionality of compelled biometrics came to issue, the court acknowledged a divide in district courts and appointed an amicus curiae who argued with the prosecutor before the court.[68] The court concluded that being forced to supply biometrics is not testimonial, emphasizing that in order to be testimonial an accused's communication itself must explicitly or implicitly relate a factual assertion or disclose information.[69] The court emphasizes that language is testimonial if the production of documents "was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox."[70] The court concludes that "a face, finger, or iris is a physical item that can be physically produced without any mental impression, communication, or admission of *mens rea* from the target" and is more akin to a key than a combination to a wall safe.[71] The court argues that the application of biometric features can be done in a person's sleep and does not require any revelation of information stored in a person's mind.[72] The court draws a comparison between signing a consent form and applying a biometric authentication, stating "the consent form may have ultimately led to the discovery of incriminating evidence obtained from another source—evidence that the prosecution could not have obtained without Doe's signature on the form. The use of biometrics may ultimately lead to incriminating evidence, but one does not hold thoughts or mental states in one's thumbprint."[73] The court also states that the provision of biometrics in other situations such as a blood sample or providing a handwriting or voice sample is not considered testimonial.[74] The facts of a foregone conclusion were not before the court.[75]

The court in *Wright* seems willing adopt a cybersecurity lens when it states that a biometric feature has the same function as a password.[76] Some argue that they are not functionally similar because there are times in which a smart device might not accept a biometric authentication in lieu of a passcode authentication.[77] This is just a security feature to ensure the device is not accessed by people without the authorization of the primary user.[78] An example of this includes the iPhone, which does not allow biometric authentication after it has been restarted, the device has not been unlocked for a period of time, or there have been unsuccessful attempts to unlock the device with biometric authentication.[79] Ultimately, the device attempts to give the user the option to use either authentication method for convenience and security.[80] Others argue that just because the authentication methods are functionally similar does not mean that makes biometric authentication testimonial, and that this is only a practical solution. While the result from *Wright* would be practical, the court also goes on to argue that the biometric is testimonial in nature because the presentation of a face is akin to acknowledging ownership or access

---

[67] In re Search Warrant No. 5165, 470 F.Supp.3d 715, 719 (E.D. Ky. 2020) (citing *U.S. v. Hubbel*, 530 U.S. 27, 43 (2000)).
[68] *Id.* at 727.
[69] *Id.* at 729.
[70] *Id.* at 728.
[71] *Id.* at 729.
[72] *Id.*
[73] *Id.* at 730.
[74] *Id.*
[75] *Id.*
[76] Wright, 431 F.Supp.3d at 1187.
[77] In re Search Warrant No. 5165 at 731-32.
[78] *About Face ID advanced technology*, Apple, (Apr. 27, 2022) https://support.apple.com/en-us/HT208108.
[79] *Id.*
[80] *Id.*

to the phone.[81] Linking an individual to a particular location using their DNA or fingerprint is considerably different than accessing a device that stores a wealth of private information about a person. Evidence does not need to be verbal or written to be testimonial and here, the link in the chain of evidence is that Wright owned or had access to a phone that contained child pornography.[82]

The court in *In re Search Warrant* failed to take into account that the implicit link required is the extreme likelihood individuals like Wright owned or had access to a phone that contained child pornography when he was compelled to open it with his face.[83] The *In re* court puts a high amount of emphasis on the analogizing of passcodes to the contents of a person's mind and of biometric features to physical keys.[84] While physical keys can be surrendered to the government, biometric features are less distinguishable from a person and cannot be so readily separated. The *In re* court likely considered this when it pointed out that application of biometric features can be done in a person's sleep and so no content of mind could possibly be used in their application.[85] While this may be true for now, many smartphone devices also take countermeasures against this.[86] For example, the iPhone's facial scanning software looks for eye movement and screen focus before unlocking, indicating that it is the intention of the manufacturer that the person be conscious and privy to the fact that they are unlocking their phone and that involuntary user biometric authentication may be erased in the future.[87] The *In re* decision is also heavily influenced by precedent that biometrics in other situations such as blood samples or handwriting/voice samples are not considered to be testimonial.[88] The common feature that biometrics have in all previous case precedent is that they all communicate aspects of an individual's identity.[89] Biometric authentication goes beyond the scope of identification and as stated before, implicitly implies ownership or access to the device.[90]

The primary counter argument to the establishment that biometric authentication is testimonial is that it is too limiting to law enforcement in its ability to access encrypted devices. It is important to distinguish that making biometric authentication testimonial does not totally eliminate the government's access to biometrically encrypted devices. The first option at the government's disposal is the use of the foregone conclusion doctrine to prove that it has enough evidence to establish a defendant's ownership and access to a device that the conclusion is foregone and there is no constitutional issue.[91] A second option for law enforcement is procuring incriminating biometrically encrypted evidence from third parties

---

[81] Wright, 431 F.Supp.3d at 1187-88.
[82] *See generally* Fisher v. United States, 425 U.S. 391 (1976); Blau v. United States, 340 U.S. 159, 161 (1950).
[83] In re Search Warrant No. 5165, 470 F.Supp.3d 715, 727 (E.D. Ky. 2020).
[84] *Id.* at 728-29.
[85] *Id.* at 729.
[86] *About Face ID advanced technology*, *supra* note 79.
[87] *Id.*
[88] In re Search Warrant No. 5165 at 730.
[89] Schmerber v. California, 384 U.S. 757 (1966) (holding that the compulsion of the biometric blood sample does not violate the Fifth Amendment interest against self-incrimination because it is a non-testimonial act); Gilbert v. California, 388 U.S. 263, 87 (1967) (holding one's voice and handwriting are means of communication but compulsion of an accused to use his/her voice or writing constitutes a non-testimonial act).
[90] Wright, 431 F.Supp.3d at 1187-88.
[91] Fisher v. United States, 425 U.S. 391, 411 (1976).

such as Meta.[92] Law enforcement also has access to continuously improving decryption options such as Cellebrite.[93]

A. The Direction of the Constitution and Privilege Against Self-Incrimination

Since the introduction of the privilege against self-incrimination, federal courts have shown a willingness to expand the privilege as the law has developed. This can be seen in *Hoffman v. United States* when the Court emphasized this privilege, stating "(the Bill of Rights) was added to the original Constitution in the conviction that too high a price may be paid even for the unhampered enforcement of the criminal law and…other social objects of a free society should not be sacrificed."[94] The *Hoffman* court demonstrates that a person's privilege from self-incrimination outweighs the United States' interest in unhindered law enforcement.[95] This is indicative that an individual's interest in protection from compulsion of biometric authentication should also bear considerable weight. The court in *Hoffman* illustrates this further by calling for a "liberal construction in favor of the right it was intended to secure."[96] The court reiterates this interpretation in *Ullman v. United States*. [97] In *Ullman*, the court expanded the privilege against self-incrimination, holding that "constitutional protection must not be interpreted in a hostile or niggardly spirit."[98] *Ullman* emphasized that it was better for an occasional crime to go unpunished through strict enforcement of the privilege than to allow the prosecution to build a strong case using compelled disclosures.[99]

The Supreme Court also takes the privacy rights of citizens into consideration with advancing technologies in *Kyllo v. United States*.[100] In *Kyllo*, law enforcement used a thermal imaging camera to scan the defendant's home and found evidence sufficient for a search warrant that lead to the discovery of marijuana.[101] The Supreme Court held that the use of a thermal imaging camera was a search of the home and emphasized its desire to not leave citizens and their privacy at the mercy of advancing technology.[102] This idea was reaffirmed in *Carpenter v. United States*, which stated that "rule(s) the Court adopts 'must take account of more sophisticated systems that are already in use or development.'"[103] The *Carpenter* court held that due to the overwhelming amount of personal information on cellphones, search warrants must be issued to search them and further rationalized that the court must protect the privacy rights of individuals as "(s)ubtler and more far-reaching

---

[92] Seo v. State, 109 N.E.3d 418, 439 (Ind. Ct. App. 2018) (opinion vacated by Seo v. State, 148 N.E.3d 952 (Ind. 2020)).
[93] Thomas Brewster, *The Feds Can Now (Probably) Unlock Every iPhone Model In Existence – UPDATE*, FORBES (Feb. 26, 2018 10:20 AM), https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/?sh=28655159667a.
[94] Hoffman v. United States, 341 U.S. 479, 486 (1951).
[95] *Id.*
[96] *Id.*
[97] Ullmann v. United States, 350 U.S. 422 (1956).
[98] *Id.* at 426.
[99] *Id.* at 427.
[100] Kyllo v. United States, 533 U.S. 27 (2001).
[101] *Id.* at 29-30.
[102] *Id.* at 33-34.
[103] Carpenter v. United States, 138 S.Ct. 2206, 2210 (2018) (citing Kyllo v. United States, 533 U.S. 27, 36 (2001)).

means of invading privacy become available to the government".[104] While both of these cases contend with Fourth Amendment issues, they demonstrate the Supreme Court's willingness to protect citizen's privacy rights against the government utilizing new technologies. This willingness could easily be extended to include the strict confines of the privilege against self-incrimination and the Fifth Amendment.

The culmination of Fourth and Fifth Amendment case precedents lay the foundation for extending the privilege against self-incrimination to the compulsion of biometrically encrypted devices. Given the "considerable weight" given to the privilege against self-incrimination, the courts' propensity to prioritize the rights of the innocent over the values of the police, and this court's willingness to take technology into consideration when deliberating on the privacy rights of citizens, it is natural that the protection against self-incrimination be expanded to include the burgeoning technology of biometric authentication.

IV. A CYBERSECURITY VIEW OF BIOMETRIC ENCRYPTION AND AUTHENTICATION

The goal of cybersecurity is to ensure the confidentiality, integrity, and availability of data and systems for the user.[105] In order to ensure this exists on devices like smartphones, specialists employ encryption to limit access to the data and systems and authentication to verify that the person accessing the device is the intended individual accessing the data.[106] As stated above, there are multiple means of authentication, each with their own strengths and weaknesses. The cybersecurity industry must compete with the user's desire for smooth and expedient access to their devices, while still ensuring that they are more secure.[107] Biometric technologies have advanced to a point where there is a balance of both security and convenience.[108] In order to better secure the privacy of a smart device from the government, an individual must encode it with a password– but this is in direct conflict with the goals of cybersecurity by forcing users to utilize a less secure method of encryption and authentication. This juxtaposition demonstrates the sacrifice of "social objects of free society" that the court in *Hoffman* was attempting to prevent.

The assertion that password authentications are testimonial while biometric authentications are non-testimonial is further confounded by the fact that on many smartphones, they serve the same functional purpose: authentication so that users may access the decrypted data.[109] Not only do biometric and password-based authentication serve the same purpose, but they are oftentimes interchangeable.[110] iPhones allow an individual to utilize biometric authentication through Face ID or passcode authentication at the user's discretion.[111] The testimonial nature of the production of smartphone data should not change just because the method of authentication does. The individual is still authenticating their use and likely possession or knowledge of the material on the smartphone.

---

[104] *Id.* at 2223 (citing Olmstead v. United States, 277 U.S. 438, 473-474 (1928) (Brandeis, J. dissenting)).
[105] STALLINGS & BROWN, supra note 42, at 3.
[106] *Id.* at 31.
[107] *Id.* at 66-67.
[108] Nikolaos V. Boulgouis, et al. BIOMETRICS THEORY, METHODS, AND APPLICATIONS 655 (IEEE Press, 2010).
[109] In re Search of a Residence in Oakland, 354 F.Supp.3d 1010, 1015 (N.D. Cal. 2019).
[110] *About Face ID advanced technology*, *supra* note 79.
[111] *Id.*

Although only tangentially related, varying pieces of legislation on the state level indicate that the public values privacy when it comes to biometrics and smart devices as well. Illinois' Biometric Privacy Information Act (BIPA) was the first piece of legislation that demonstrated the trend toward biometric privacy laws in the United States.[112] BIPA was enacted in response to public concerns regarding the rapidly growing use of biometric technology in commercial transactions.[113] BIPA applies to many common biometric identifiers such as retina/iris, fingerprints, voiceprints, facial scans, etc. and requires targeted entities to take protective measures in securing an individual's biometric features in order to be compliant with the act.[114] The statute even requires that companies treat these biometric identifiers in a similar fashion to passcodes, account numbers, pin numbers, or other types of unique identifying information.[115] BIPA has served as a model for other state laws and four other states have adopted legislation modeled on BIPA, while 27 other states have BIPA-modeled legislation pending as of June 2021.[116] While the determination for biometric encryption to be considered testimonial does not hinge upon whether state legislatures have enacted statutes protecting biometric features, it is still indicative of a public interest in biometrics and their relation to privacy interests.

Smartphones have only become more interconnected into our everyday lives and as they continue to do so, they also begin to function more like a part of or extension of our minds.[117] They have become a critical part of our memories as they can record pictures, set reminders, and we use them to accomplish a number of mental tasks and solve problems. To the extent the Fifth Amendment protects a private mental sphere in connection with criminal investigations, at least, it should have a special application to these special devices.[118]

A. *The Foregone Conclusion Doctrine and Fifth Amendment*

As mentioned above, the foregone conclusion doctrine was first introduced in *Fisher v. United States*.[119] Courts have disagreed on whether or when the foregone conclusion doctrine applies to a case and how it contends with other constitutional protections.[120] The issue at the center of the foregone conclusion doctrine is whether to treat the compelled disclosure of a password differently than a compelled decryption, such as an individual being compelled to present their face or fingerprint to unlock a biometric encryption. This has been interpreted in two distinct ways by different state supreme courts.

The Supreme Court of Massachusetts has held that the only testimony at issue when considering the foregone conclusion doctrine is whether or not the defendant knows

---

[112] 740 ILL. COMP. STAT. 14/5 (2008).
[113] *See* 740 ILL. COMP. STAT. 14/5(b) (2008).
[114] *See id.* 14/15.
[115] *See id.* 14/15(e)(2).
[116] Christopher Ward, Kelsey Boehm, *Developments in Biometric Information Privacy Laws*, FOLEY & LARDNER LLP (Jun. 17, 2021), https://www.foley.com/en/insights/publications/2021/06/developments-biometric-information-privacy-laws.
[117] Bryan H. Choi, *The Privilege Against Cell Phone Incrimination*, 97 TEXAS L. REV. ONLINE 73, 75 (2019).
[118] Riley v. California, 573 U.S. 373, 403 (2014).
[119] Fisher v. United States, 425 U.S. 391, 411 (1976).
[120] Nicole Hager, *SCOTUS Asked If 5th Amendment Bars Compelling Defendants to Unlock Electronic Devices*, THE FEDERALIST SOCIETY (Feb. 22, 2021), https://fedsoc.org/commentary (search for "SCOTUS Asked"; then scroll to find article link).

the password.[121] In *Jones*, the defendant came under suspicion for sex trafficking and prostitution and an investigation was launched.[122] Police identified a cell phone that they suspected the defendant used to communicate with sex trafficking victims and conduct the prostitution business.[123] A search of one of the victim's cell phones revealed conversations with an individual whose contact name matched the defendant's, discussing prostitution and sex trafficking at length. The defendant was arrested, two cell phones were recovered, and search warrants for the cell phones were granted, but the investigation was halted because the phones were password encrypted.[124] The Commonwealth of Massachusetts filed a motion to compel the defendant to decrypt the phone by inputting his password, arguing that compelling the defendant to enter the password would not reveal any information that the Commonwealth did not already know.[125] After the motion was denied, the Commonwealth renewed its motion and presented further evidence arguing the defendant's knowledge of the password was a foregone conclusion based on cell site location information records, specific telephone numbers, and even a statement the defendant made to police officers during his booking, in which he identified the phone.[126] After this was denied the case advanced to the Supreme Court of Massachusetts to determine the applicability of the foregone conclusion doctrine.[127] The court notes that:

> "The commonwealth may, however, compel testimonial acts of production without violating a defendant's rights under the fifth amendment or art. 12 where "facts conveyed [by the act] already are known to the government, such that the individual 'adds little or nothing to the sum total of the Government's information.' In these circumstances, because the facts implicitly disclosed through the act or production are already known to the commonwealth."[128]

The court acknowledges the foregone conclusion doctrine's origin in compelled production of documents and extends the foregone conclusion doctrine to production of passwords encrypting electronic devices, so long as the Commonwealth establishes that it already knows the testimony that is implicit within the act of production. [129] The court asserts that in the case of compelled decryption the only fact conveyed by the act is that the defendant knows the password and can access the device and thus the only thing that the Commonwealth needs to prove is that the defendant knows the password to decrypt the cell phone before his knowledge of the password can be deemed a foregone conclusion.[130] The court concludes that the factual record put before the court by the Commonwealth met its burden, proving that the defendant's knowledge of the phone password was a foregone conclusion and the defendant must be compelled to input the password by motion.[131]

Alternatively, the Supreme Court of Indiana found that unlocking a device implies the additional testimony of admitting one's ability to control the device and the contents

---

[121] Commonwealth v. Jones, 481 Mass. 540, 551 (2019).
[122] *Id*. at 543.
[123] *Id*. at 544.
[124] *Id*. at 545.
[125] *Id*.
[126] *Id*.
[127] *Id*. at 545-46.
[128] *Id*. at 546.
[129] *Id*.
[130] *Id*.
[131] *Id*. at 556.

found within.[132] The defendant in the Indiana case, Katelin Seo, was under investigation for stalking and harassing a minor after he told police he received texts and calls from her number and other unassigned phone numbers.[133] The defendant was eventually arrested, but she refused to provide her phone password, even after a warrant was issued to compel her to unlock her device or be found in contempt of court.[134] At a hearing, the defendant argued that forcing her to unlock her iPhone would violate her Fifth Amendment right against self-incrimination. While she appealed the contempt ruling against her, she entered into a plea agreement with the state, pleading guilty to one count of stalking.[135] The Supreme Court of Indiana heard her remaining appeal regarding the contempt of court.

The Court notes that embedded within the Fifth Amendment is the principle that "the state produce evidence against an individual through 'the independent labor of its officers, not by the simple, cruel expedient of forcing it from his own lips.'"[136] The court specifies that not all compelled incriminating evidence is protected and that it must be testimonial because "an accused's communication must itself, explicitly or implicitly relate a factual assertion or disclose information."[137] The defendant argues that forcing her to unlock her iPhone for law enforcement is a form of self-incrimination, while the state argues that it already knows the implicit factual information that the defendant would convey by unlocking her phone, thus making the act a foregone conclusion.[138] The Court found in favor of the defendant, holding that the compelled production of an unlocked smartphone is "testimonial and entitled to Fifth Amendment protection–unless the State demonstrate the foregone conclusion exception applies."[139] The Indiana Supreme Court goes on to rationalize that giving law enforcement an unlocked smartphone communicates to the government a plethora of information such as "that the suspect knows the password; the files on the device exist; and the suspect possesses those files."[140] Previous case law establishes that the act of producing documents can imply critical information within a case, and the foregone conclusion exception must be considered against these broad communicative aspects. "In this way, the act of production doctrine links the physical act to the documents ultimately produced."[141] The court analogized entering the password to unlock an encrypted device to the physical act of handing over documents and reasoned that the files on an encrypted phone are the same as documents that are physically produced.[142] The court ruled that the state must prove that (1) the suspect knows the password, (2) the files on the device exist, and (3) the suspect possessed those files; otherwise, the act of production is not a foregone conclusion and Fifth Amendment protections apply.[143] The Court here concludes that even if the state had shown that the defendant knew the password to her smartphone, they failed to demonstrate that any particular files on the device existed, or that she possessed those files, and thus the defendant's act of production would provide the state with information it did not already

---

[132] Seo v. State, 148 N.E.3d 952, 955 (Ind. 2020).
[133] *Id*. at 953.
[134] *Id*. at 954.
[135] *Id*.
[136] *Id*. at 954-55.
[137] *Id*. at 955.
[138] *Id*.
[139] *Id*.
[140] *Id*.
[141] *Id*. at 957.
[142] *Id*. (citing Commonwealth v. Jones, 481 Mass. 540, 565 (2019)).
[143] *Id*.

know.[144] To rule alternatively would "sound 'the death knell for a constitutional protection against compelled self-incrimination in the digital age.'"[145]

The Supreme Court of Indiana goes on to state its concerns with extending the foregone conclusion exception to the compelled production of an unlocked smartphone.[146] The Court references case precedent in which the foregone conclusion doctrine was applied but was limited in the scope to the documents at issue, such as tax documents and case documents, which differ greatly from the vast amount of information available within a smartphone, where there is no way to limit the amount of data obtained.[147] The Court further remarked on the complexities of advancing technology and the foregone exclusion exception.

> "[I]f officers searching a suspect's smartphone encounter an application or website protected by another password, will they need a separate motion to compel the suspect to unlock that application or website? And would the foregone conclusion exception apply to that act of production as well? Suppose law enforcement opens an application or website and the password populates automatically. Can officers legally access that information? Or what if a suspect has a cloud-storage service—like iCloud or Dropbox—installed on the device, which could contain hundreds of thousands of files. Can law enforcement look at those documents, even though this windfall would be equivalent to identifying the location of a locked storage facility that officers did not already know existed?"[148]

The Court stated that its last concern revolved around applying the foregone conclusion doctrine to a novel dilemma that was completely unforeseen when the doctrine was created. The Indiana Supreme Court points out that *Fisher*, which created and applied the foregone conclusion doctrine, was decided in 1976, almost 46 years ago from today. Cell phones were not widely used in 1976.[149] The Court concluded that forcing the defendant to unlock her iPhone for law enforcement would violate her Fifth Amendment right against self-incrimination and reversed the trial courts order finding her in contempt.[150]

While both the Massachusetts Supreme Court and the Supreme Court of Indiana are still arguing over whether requiring an individual to input his password is protected by the Fifth Amendment, these same arguments could be applied when an individual is compelled by a court to input biometric information into an encrypted smart device. In an attempt to disentangle the messy subject of the Fifth Amendment and the foregone conclusion doctrine, the Supreme Court of Massachusetts in *Commonwealth v. Jones* seems to posit a fairly simple rule: if the state can show independently that a person knows the password to a smart device, the government can compel that person to enter the password.[151] However, the rule should not be whether the government can show that the suspect knows the password to the device, the better rule is the one applied in *Seo v. State*. Whenever a person opens their smart device, be it by password or biometric authentication,

---

[144] *Id*. at 958.
[145] *Id*.
[146] *Id*. at 959.
[147] *Id*. at 959-60.
[148] *Id*. at 960-61.
[149] *Id*. at 961.
[150] *Id*. at 962.
[151] Commonwealth v. Jones, 481 Mass. 540, 557 (2019).

there is a distinct link between the act of opening the phone for law enforcement and the data found on the device. The physical act testifies about the data within. The person implicitly communicates they possess or control the data found on the device. If the person can open the device, it is extremely likely that the device is their own, and if the person owns the device, the files on it are likely their own too, which is extremely prejudicial if the government has not yet established this as fact. The implicit nature of these acts is largely ignored in *Commonwealth v. Jones*, in what appears to be an attempt to maintain practices or an interpretation of balance in the law. If the *Jones* ruling were followed, it would shift power towards the government, giving them the ability to search very personal and private data that did not even exist twenty years ago, let alone when *Fisher* was decided.

As stated in *Seo*, the nature of smart devices means that the information available from smartphones is expansive and provides "the proverbial 'key to a man's kingdom.'"[152] These realities are recognized when law enforcement needs to state with reasonable particularity what they believe they will identify on the smartphone that is of legal relevance and be limited to using just that. This rationale should be applied just the same to cases involving the foregone conclusion doctrine. The government should be required to demonstrate that an individual knows the password to the smart device, explain with reasonable particularity what they expect to find on the device, and that the data was in the individual's possession. A reasonable particularity requirement would also satisfy the issue of unbridled phone access brought forward in *Seo*.

Additionally, one aspect which has not been addressed yet is the burden of proof required to establish a foregone conclusion. While courts have started to apply the foregone conclusion doctrine within the context of compelled decryption, only one court has stated the standard of proof the government bears to establish that a defendant's knowledge of the password to decrypt an electronic device is a foregone conclusion under the Fifth Amendment.[153] This is separate from the reasonable particularity standard mentioned above, as a court is unable to ask whether the government has established with reasonable particularity if the defendant knows the password to the device in question. While some evidence can be described with specificity, this metric cannot be applied to a defendant's ability to decrypt. The court in *Spencer* indicates that the appropriate burden is clear and convincing evidence.[154] The *Spencer* court posits that a high burden of proof for the foregone conclusion is important so that the Fifth Amendment is not trampled upon.[155] While the burden of clear and convincing evidence is a strong standard, courts deciding the issue of evidentiary burdens for the foregone conclusion doctrine may want to rule that the evidentiary standard is beyond a reasonable doubt because this is the standard of evidence most often applied in criminal proceedings. Furthermore, the Supreme Court in *Fisher* was the first (and only) court to find that the testimony implicit in an act of production was a foregone conclusion.[156] The government failed to show that a foregone conclusion was met in other Supreme Court decisions.[157] The Supreme Court's unwillingness to apply the

---

[152] Seo v. State, 148 N.E.3d 952, 960 (Ind. 2020) (citing *United States v. Djibo*, 151 F. Supp. 3d 297, 310 (E.D.N.Y. 2015)).
[153] United States v. Spencer, No. 17-cr-0025-CRB-1, 201 WL 1964588, at *8 (N.D. Cal. Apr. 26, 2018).
[154] *Id*.
[155] *Id*.
[156] Fisher v. United States, 425 U.S. 391, 411 (1976).
[157] United States v. Doe, 465 U.S. 605, 614 (1984) (*Doe I*); United States v. Hubbell, 530 U.S. 27, 44 (2000).

foregone conclusion doctrine beyond the *Fisher* case may mean that they feel as though the burden of proof should be as high as beyond a reasonable doubt.

V. CONCLUSION

The Founders included the privilege against self-incrimination in the Constitution to protect individual privacy and ensure a fair judicial process.[158] Courts have failed U.S. citizens by neglecting to protect them from compelled unlocking of biometrically encrypted devices. This inaction has created a loophole that contradicts the framework of the privilege against self-incrimination. To correct this mistake courts should reconsider the trend they have set for the Constitution and the Fifth Amendment and consider adopting a forward-thinking cybersecurity lens to conclude that biometric authentication is testimonial. Courts should consider that biometric encryption is akin to a compelled password entry for the purposes of the foregone conclusion doctrine. The foregone conclusion doctrine should be applied in limited circumstances with a specific and high burden of proof so that the "jealous protection of the privilege against self-incriminating testimony" can be preserved.[159] Allowing law enforcement such easy access to smart devices narrows Fifth Amendment protections and the expansive foregone conclusion exception is contrary to both principles of cybersecurity and the spirit of the Fifth Amendment. Courts should move to remediate this at once. These liberties and values can only be guaranteed by courts that are willing to take on cases with issues revolving around biometric encryption, the Fifth Amendment, and the foregone conclusion doctrine.

[158] *Fifth Amendment - Rights of Persons*, *supra* note 10, at 1302.
[159] Fisher v. United States, 425 U.S. 391 (1976).