


4-11-2018

Privacy, Screened Out: Analyzing the Threat to Individual Privacy Rights and Fifth Amendment Protections in *State v. Stahl*

Jesse Coulon
Boston College Law School, jesse.coulon@bc.edu

Follow this and additional works at: <http://lawdigitalcommons.bc.edu/bclr>

 Part of the [Communications Law Commons](#), [Computer Law Commons](#), [Constitutional Law Commons](#), [Evidence Commons](#), [Privacy Law Commons](#), and the [Science and Technology Law Commons](#)

Recommended Citation

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 (2018), <http://lawdigitalcommons.bc.edu/bclr/vol59/iss9/13>

This Comments is brought to you for free and open access by the Law Journals at Digital Commons @ Boston College Law School. It has been accepted for inclusion in Boston College Law Review by an authorized editor of Digital Commons @ Boston College Law School. For more information, please contact nick.szydowski@bc.edu.

PRIVACY, SCREENED OUT: ANALYZING THE THREAT TO INDIVIDUAL PRIVACY RIGHTS AND FIFTH AMENDMENT PROTECTIONS IN *STATE v. STAHL*

Abstract: Courts across the United States have applied Fifth Amendment protections to passcodes, as long as those passcodes are not a foregone conclusion. In order for a court to determine that a passcode is a foregone conclusion, and thus not testimonial in nature, the prosecution must show that they knew the existence, possession, and authenticity of the evidence that would be discovered by the compelled passcode, before the passcode is compelled. The foregone conclusion doctrine was established, and had been used, to balance the need of law enforcement to gather incriminating evidence while still protecting defendants' Fifth Amendment rights. In 2016, the Florida Second Court of Appeals took the foregone conclusion doctrine to an extreme in *State v. Stahl*, by expanding the foregone conclusion doctrine and finding that evidence must be significantly testimonial in order for it to be protected by the Fifth Amendment. If other courts follow the *Stahl* decision, it would mean the end of the balance that the foregone conclusion has provided as well as all Fifth Amendment protections to encryption.

INTRODUCTION

Courts have had to reinterpret Fifth Amendment protections against self-incrimination as communication technology has evolved.¹ The increased speed of modern decryption technology and the proliferation of smartphone usage has left individual courts to interpret an antiquated Supreme Court doctrine.² Today, individuals are increasingly reliant upon their

¹ See Matthew J. Weber, Note, *Warning—Weak Password: The Courts' Indecipherable Approach to Encryption and the Fifth Amendment*, 2016 U. ILL. J.L. TECH. & POL'Y 455, 456–57 (stating that as cell phones, computers, and the internet have become entwined in every aspect of daily life, courts have had to interpret what technological communications are protected by the Fifth Amendment); see also U.S. CONST. amend. X (stating that “[n]o person . . . shall be compelled in any criminal case to be witness against himself”); Erin Sales, Note, *The “Biometric Revolution”: An Erosion of the Fifth Amendment Privilege to Be Free from Self-Incrimination*, 69 U. MIAMI L. REV. 193, 197 (stating that since the passage of the Fifth Amendment, the purpose and meaning of the Amendment has become increasingly unclear as technology has evolved).

² See Weber, *supra* note 1, at 457, 460 (stating that the traditional approach taken by courts, which holds that the Fifth Amendment protects against an individual incriminating themselves by being compelled to produce testimonial evidence, has become more difficult for modern courts to apply as individuals do more and more on their encrypted electronic devices); see, e.g., *State v. Stahl*, 206 So. 3d 128, 136 (Fla. Dist. Ct. App. 2016) (finding that when a phone has a passcode and is registered to a defendant, the State can compel the password to the phone because it is a

smartphones, computers, and other portable electronic devices for tasks including online banking, dating, and communications.³ As these technologies have been integrated into almost every aspect of modern daily life, telephone and computer companies have made encryption technology easier for customers to use and devices more difficult for unauthorized users to access.⁴ These factors have created an environment in which law enforcement often must obtain the passwords for electronic devices directly from the owner in order to access those devices.⁵

The two seminal Supreme Court cases that courts look to when determining whether an individual has a Fifth Amendment right to refuse to give their passcodes to law enforcement are *Fisher v. United States*, decided in

foregone conclusion that the defendant knows that password); *Commonwealth v. Baust*, 89 Va. Cir. 267, 271 (Va. Cir. Ct. 2014) (finding that the only way a passcode could be determined to be a foregone conclusion would be if the government already knew the passcode).

³ Weber, *supra* note 1, at 458; Arron Smith, *Record Shares of Americans Now Own Smartphones, Have Home Broadband*, PEW RESEARCH CTR. (Oct. 3, 2017), <http://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology> [<https://perma.cc/F29Q-GJRR>] (stating that as of January 2017, 77% of Americans own a smartphone, a figure that has more than doubled since 2011, and that this trend is expected to continue with 92% of younger adults owning smartphones).

⁴ See *Stahl*, 206 So. 3d at 128 n.1 (finding that all Apple products running iOS 8 or later have an encryption key that is tied to the user's passcode, which Apple does not possess).

⁵ See *id.* (stating that as iPhone users download the iOS 8 or newer operating system, law enforcement officials will not be able to access those phones without owners providing their passcodes). As of September 2014, technology giant Apple implemented the iOS 8 operating system for its devices. *Apple Announces iOS 8 Available September 17*, Apple Newsroom (Oct. 3, 2017), <https://www.apple.com/newsroom/2014/09/09Apple-Announces-iOS-8-Available-September-17> [<https://perma.cc/P474-LSUW>]. The main purpose of the iOS 8 operating system update was to ensure the privacy of Apple's customers by removing Apple's ability to unlock its customers' phones by retrieving their passcodes. See *Stahl*, 206 So. 3d at 128 n.1 (finding that Apple will no longer perform data extractions in response to warrants for iOS systems because the data is now protected by an encryption key tied to the owner of the phone's passcode, which Apple no longer has access to); see also Craig Timber, *Apple Will No Longer Unlock Most iPhones, iPads for Police, Even with Search Warrants*, WASH. POST (Feb. 18, 2018), https://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html?utm_term=.5f2a48ad3398 [<https://perma.cc/DG6G-8LVH>] (stating that Apple's iOS 8 will prevent the company from unlocking customer's iPhones or iPads). Practically, what this means is Apple does not have the ability to access these passcodes, so it can no longer provide a phone's passcode to law enforcement when served subpoenas for them. *Id.*; John L. Potapchuk, *A Second Bite at the Apple: Federal Courts' Authority to Compel Technical Assistance to Government Agents in Accessing Encrypted Smartphone Data Under the All Writs Act*, 57 B.C. L. REV. 1403, 1404 (2016) (stating that Apple's iOS 8 operating system and the Google Android's operating system developed during the same time period, which collectively compose over ninety-six percent of the operating systems on the market, have encryption capabilities believed to be impossible to break without the owner's passcode); Lily Hay Newman, *Here's How to Keep Apple from Sharing Your iPhone Data with the Police*, Slate (Feb. 18, 2018), http://www.slate.com/blogs/future_tense/2014/09/18/if_you_use_a_passcode_in_ios_8_apple_won_t_be_able_to_give_your_personal.html [<https://perma.cc/Q393-D5EU>] (stating that Apple, with its iOS 8 operating system, will no longer be able to comply with warrants requesting the company to unlock its customers' iPhones).

1976, and *Doe v. United States*, decided in 1988.⁶ Both cases were decided prior to the ubiquitous nature of technology today and prior to the proliferation of smartphones in our society.⁷ This has left state governments and individual courts to determine the extent to which individuals have a Fifth Amendment right of refusal to provide law enforcement their passcodes, even when law enforcement officers have secured a warrant to search their encrypted devices.⁸ Courts have answered this question in a variety of different ways with a range of results, but no court prior to the Florida Second District Court of Appeals in 2016, in *State v. Stahl*, has completely stripped away an individual's Fifth Amendment right to refuse to give law enforcement the password to a personal encrypted device.⁹

⁶ See *Doe v. United States*, 487 U.S. 201, 218–19 n.9 (1988) (establishing that a combination to a wall safe, which courts have interpreted as equivalent to a passcode, is considered testimonial because recalling the passcode forces a defendant to reveal a product of his mind); *Fisher v. United States*, 425 U.S. 391, 411–14 (1976) (determining that when the government knows the location, existence, and authenticity of evidence with reasonable particularity, that evidence loses its Fifth Amendment protections because the act of producing that evidence adds little to nothing to the government's case).

⁷ See *Weber*, *supra* note 1, at 458 (finding that we are now more reliant than ever before on technology—we use it to pay our bills, make purchases at grocery stores, check bank accounts, and we perform many of these activities through our smartphones).

⁸ See *id.* at 460 (stating that courts have differed on how to best handle the compulsion of passcodes, which could be incriminating, when the defendant providing that passcode is the only way to access that defendant's electronic device); see also FLA. STAT. ANN. § 933.07 (West 2001 & Supp. 2012) (stating that a judge must find that there is probable cause to believe that the evidence that is being searched for will be located where the search warrant is being issued in order to issue a search warrant); MASS. GEN. LAWS ch. 276, § 1 (2016) (stating that a judge must find that there is probable cause to believe that the evidence being searched for “is in a house, place, vessel or vehicle or in the possession of the person anywhere within the commonwealth and territorial waters thereof”); *Stahl*, 206 So. 3d at 136 (finding that when a phone has a passcode and is registered to a defendant the State can compel the password to the phone because it is a foregone conclusion that the defendant knows that passcode); *Baust*, 89 Va. Cir. at 267 (finding that the only way that a passcode could be a foregone conclusion would be if the government already knew the passcode); *Newman*, *supra* note 5, at 195 (stating that courts have lacked consistency when deciding if compelling the production of an individual's passcode violates that individual's Fifth Amendment rights).

⁹ See *United States v. Apple MacPro Computer*, 851 F.3d 238, 248 (3d Cir. 2017) (determining that because the government could show through forensics that there were photographs on the defendant's hard drive consistent with child pornography and the hard drive was taken from the defendant's possession, the government met the requisite requirements of the foregone conclusion doctrine, so the defendant's passcode could be compelled); *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335, 1346–47 (11th Cir. 2012) (finding that the government did not know with reasonable particularity that there was child pornography on the defendant's hard drive, so the government could not compel the defendant to relinquish the passcode to the hard drive); *Stahl*, 206 So. 3d at 136 (finding that knowledge that a cellphone is registered to a defendant and that the phone has a passcode are enough to establish that the passcode is a foregone conclusion and to compel the defendant to surrender that passcode).

Part I of this Comment will present the two seminal Supreme Court cases that provide the precedent for all password protection cases.¹⁰ Part II will lay out the facts and holding of the *Stahl* case.¹¹ Part III will show how both federal and state courts before *Stahl* have applied the foregone conclusion doctrine as a balancing test between individual privacy rights and state interests.¹² Finally, Part IV will analyze how the court in *Stahl* incorrectly applied the foregone conclusion doctrine, by finding that every passcode is a foregone conclusion when a phone is shown to be registered to an individual and has a passcode, and the potential consequences of other courts adopting the *Stahl* interpretation.¹³

I. SEMINAL CASES THAT HAVE CREATED THE FRAMEWORK FOR ALL FIFTH AMENDMENT PROTECTIONS RELATING TO ENCRYPTION

Courts dealing with cases involving encryption technology look at two seminal Supreme Court cases, *Doe v. United States* and *Fisher v. United States*, for precedent and guidance when ruling on passcode compulsion cases.¹⁴ Although these two opinions were written before the proliferation of encryption technology, their respective establishment of what evidence is considered testimonial and what evidence is considered a foregone conclusion in a password context is still considered precedential law today.¹⁵

In *Doe*, the Supreme Court established the fundamental distinction between being compelled to hand over a key that unlocks a safe with incrimi-

¹⁰ See *infra* notes 14–36 and accompanying text.

¹¹ See *infra* notes 37–63 and accompanying text.

¹² See *infra* notes 64–89 and accompanying text.

¹³ See *infra* notes 90–102 and accompanying text.

¹⁴ See *Doe v. United States*, 487 U.S. 201, 210 n.1 (1988) (establishing that a combination to a wall safe, which courts have interpreted as the equivalent of a passcode, is considered testimonial because recalling the passcode forces a defendant to reveal a product of his mind); *Fisher v. United States*, 425 U.S. 391, 411 (1976) (finding that even if evidence is testimonial, it can still be compelled if the government knows with reasonable particularity the location, possession, and authenticity of that evidence); see also *State v. Stahl*, 206 So. 3d 128, 136 (Fla. Dist. Ct. App. 2016) (narrowing the Fifth Amendment protections of *Fisher* and *Doe* by finding that when a phone has a passcode and is registered to a defendant, the government can compel the password to the phone because it is a foregone conclusion that the defendant knows that password); *Commonwealth v. Baust*, 89 Va. Cir. 267, 271 (Va. Cir. Ct. 2014) (widening the Fifth Amendment protections of *Fisher* and *Doe* by finding that the only way a passcode could be deemed a foregone conclusion would be if the government already knew the passcode).

¹⁵ See *Doe*, 487 U.S. at 210; *Fisher*, 425 U.S. at 411; *United States v. Greenfield*, 831 F.3d 106, 127 (2d Cir. 2016) (following *Fisher*, by finding that the district court was incorrect in finding that the defendant's production of documents was a foregone conclusion because the government did not prove the existence, location, and authenticity of the documents at the time of the issuance of the subpoena); *United States v. Green*, 272 F.3d 748, 753 (5th Cir. 2001) (following *Doe* in finding that compelling a defendant to open combination locks with illegal firearms inside violated his Fifth Amendment rights because giving over the combinations is a testimonial act).

nating evidence inside and being compelled to provide the combination to unlock that same safe.¹⁶ The defendant in *Doe* was the target of a grand jury investigation into whether he had fraudulently manipulated the receipts for oil cargo and unreported income.¹⁷ As part of this investigation, the banks where Doe's accounts were located were subpoenaed to produce Doe's account information; however, they refused to provide this information without Doe's consent.¹⁸ Doe argued that consenting to allow his banks to send the government his account information would violate his Fifth Amendment rights.¹⁹ The Supreme Court found that compelling the target of a grand jury investigation to authorize foreign banks to disclose records of his accounts, without identifying those documents or acknowledging their existence, did not implicate the Fifth Amendment because it did not require him to make a testimonial communication.²⁰ The Court found that compelling an individual to authorize a bank to disclose the records of his accounts was akin to forcing a defendant to surrender the key to a safe with incriminating evidence inside of it.²¹ The act of surrendering a key is not protected by the Fifth Amendment because it does not force an individual to reveal the contents of his mind.²² If, in lieu of a key, the warrant tried to compel an indi-

¹⁶ See *Doe*, 487 U.S. at 210 n.9 (finding that being compelled to give a combination to a wall safe is testimonial because it forces that individual to express the contents of his mind, while surrendering a key to a strongbox is not testimonial because it does not force an individual to express the contents of his mind).

¹⁷ *Id.* at 203.

¹⁸ *Id.* The banks where Doe's accounts were located were in the Cayman Islands and Bermuda. *Id.*

¹⁹ *Id.* at 208 (arguing that consenting to allow his bank to send the government his account information is a testimonial act because it is a statement of the defendant that could lead to potentially incriminating evidence against him).

²⁰ *Id.* at 217–18 (finding that the defendant authorizing his bank to disclose his records did not express that he had any control over the accounts, or that the banks were correct that these accounts belonged to him, just that he was authorizing his bank to turn over information that, in the bank's opinion, belonged to the defendant).

²¹ *Id.* at 210; see Nicholas Soares, *The Right to Remain Encrypted: The Self-Incrimination Doctrine in the Digital Age*, 49 AM. CRIM. L. REV. 2001, 2005 (stating that the Supreme Court has distinguished between physical acts of surrender and acts that force a defendant to divulge the contents of their mind, by finding that the former does not invoke Fifth Amendment protections while the latter does).

²² *Doe*, 487 U.S. at 210 n.9. The Supreme Court found in *Fisher* that if something is not a product of a defendant's mind, it is not protected by Fifth Amendment privilege, even if what is being compelled would lead to incriminating evidence. See *Fisher*, 425 U.S. at 409. The Court found that the Fifth Amendment does not apply to all compelled production of incriminating evidence; it only applies when the government is compelling testimony that is a testimonial communication. *Id.* The Court mentions circumstances where it has found that the compulsion of incriminating evidence is not testimonial because the evidence is not communicative in nature. *Id.* The examples the Court has provided when it has found that compulsion of incriminating evidence is not testimonial are: blood samples, *Schmerber v. California*, 384 U.S. 757, 763–64 (1966); handwriting exemplars, *Gilbert v. California*, 388 U.S. 263, 265–67 (1967); voice exemplars, *United*

vidual to provide a combination to open that same safe, that combination would be protected under the Fifth Amendment privilege.²³ Forcing an individual to surrender a passcode would be demanding them to express the contents of their mind, making the action testimonial.²⁴ Courts have generally interpreted, prior to the Second Court of Appeals in *State v. Stahl*, that if a combination to a wall safe is testimonial, then so is a passcode to an encrypted device.²⁵

Another seminal case regarding Fifth Amendment protections in the digital era is *Fisher v. United States*.²⁶ The defendants in *Fisher* were being investigated for possible civil and criminal liability under federal income tax laws by the Internal Revenue Service (IRS).²⁷ The IRS issued a subpoena to compel documents that were used to prepare the defendants' tax returns that the defendants had obtained from their accountants.²⁸ The defendants appealed the subpoena, stating that being compelled to hand over these documents to the government would violate their Fifth Amendment

States v. Wade, 388 U.S. 218, 222–23 (1967); and wearing clothing of the person who committed the crime, *Holt v. United States*, 218 U.S. 245 (1910). *Id.*

²³ See *Doe*, 487 U.S. at 210 n.9 (determining that compelling the defendant to authorize his bank to disclose information relating to his account was more like giving over a key to a safe, since complying with the warrant did not force him to give up a product of his mind). The Court emphasized this difference, because in order for an act to be protected by the Fifth Amendment it must be testimonial, and in order for an act to be testimonial, a defendant must be compelled to perform an act that forces him to give up a product of his mind. *Id.*

²⁴ *Id.*; see also Soares, *supra* note 21, at 2004 (stating that the Supreme Court has found that evidence is testimonial, and thus induces Fifth Amendment protections, if that evidence is a compelled communication that forces the defendant to reveal the contents of his or her mind).

²⁵ See *Doe*, 487 U.S. at 210 n.9 (establishing that a combination to a safe is protected by Fifth Amendment protections); see also *United States v. Apple MacPro Computer*, 851 F.3d 238, 248 (3d Cir. 2017) (finding that because the government was able to show through forensics that there were photographs on the defendant's hard drive that were consistent with child pornography, and because the hard drive was taken from the defendant's possession, the government met the requisite requirements of the foregone conclusion doctrine and the defendant's passcode could be compelled); *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335, 1346–47 (11th Cir. 2012) (finding that the government did not know with reasonable particularity that there was child pornography on the defendant's hard drive, so the government could not compel the defendant to turn over the passcode to the hard drive).

²⁶ See *Fisher*, 425 U.S. at 412; see Fern Kletter, Annotation, *Construction and Application of "Foregone Conclusion" Exception to Fifth Amendment Privilege against Self-Incrimination*, 25 A.L.R. Fed. 3d Art. 10 (2017) (finding that the foregone conclusion doctrine has been used to compel passcodes to encrypted devices).

²⁷ *Fisher*, 425 U.S. at 394. The Supreme Court decided two separate cases in *Fisher*, both involving the IRS attempting to compel accountant working papers from the defendants. *Id.*

²⁸ *Id.* at 395. The papers were subsequently given by the defendants to their attorneys with the hope of invoking attorney client privilege, however the Court found this argument unpersuasive. *Id.* at 395, 401–06.

rights because handing over the documents was a testimonial act.²⁹ The Supreme Court found it unnecessary to determine if providing the documents to the government was a testimonial act.³⁰ The Court held that a subpoena issued by the IRS seeking the defendants' accountant's working papers used in the preparation of tax returns could be compelled even if they were protected by Fifth Amendment privilege because their existence was a foregone conclusion.³¹ The government already knew that the tax returns existed, where they were located, and that they were authentic, so producing these documents to the IRS would "add little or nothing" to the government's case.³² The production of the documents adds little or nothing to the government case because the actual production of the documents, which otherwise would tacitly concede the existence of the documents being compelled, loses all prejudicial effect to the defendant, because the government already knows the location, authenticity, and existence of the documents.³³ When testimonial evidence that would normally be protected by the Fifth Amendment adds little or nothing to a case against a defendant, no constitutional rights are violated.³⁴ The compulsion of evidence that adds little or

²⁹ *Id.* at 395. The Court found that responding to the subpoena may invoke Fifth Amendment protections; however, it was unnecessary for the Court to decide if it did because the papers were foregone conclusion, voiding any possible Fifth Amendment protections. *Id.* at 411–12.

³⁰ *Id.* at 411–12 (finding that testimonial evidence that normally would be protected by the Fifth Amendment loses its Fifth Amendment protections when the government already knows the existence, location, and authenticity of the evidence, so that the actual production of the documents adds little to nothing to the government's case).

³¹ *Id.* at 410–13. The Court found that the working papers were testimonial not due to the nature of the documents, but rather because producing the documents to the government has a communicative aspect by itself, which makes the production of the documents testimonial. *Id.* The working papers that were subpoenaed were not created by the defendant and do not contain any communicative declarations that would make them testimonial. *Id.* Instead they are testimonial because the act of production can be testimonial when it concedes the existence of the papers and that they are in the possession of the defendant. *Id.*

³² *See id.* at 411 (finding that when the government knows the location, authenticity, and existence of evidence, the act of producing that evidence is no longer testimonial in nature). The government knew the location of the documents because they knew the defendant transferred the papers to his attorney. *Id.* at 394. The government verified the possession and authenticity of the documents through independent evidence. *Id.* at 394, 411. Due to the government's prior knowledge of the defendant's tax documents being compelled, the defendant's actual handing over of the documents to the government would add little to nothing to the government's case. *Id.* at 411.

³³ *Id.* at 411; *see* Kletter, *supra*, note 26, at 10 (stating that Fifth Amendment protections do not apply to evidence when the location, existence, and authenticity of the evidence is already known, so that even if the act of production conveys a fact regarding the existence, location, or authenticity of the evidence, that fact is already a foregone conclusion).

³⁴ *See Fisher*, 425 U.S. at 411 (finding that when the production of evidence adds little or nothing to the government's case, that production loses its Fifth Amendment protections). When the government knows the location, existence, and authenticity of evidence, that evidence loses its testimonial nature. *Id.* When this happens, the act of handing over the evidence is no longer a testimonial act, but instead an act of surrender. *Id.*

nothing to a case against a defendant is not seen as a question of testimony, but as one of surrender.³⁵ If the government is aware of the testimonial aspect of the evidence they are compelling, and the government is not attempting to prove the testimonial evidence through the order, then compulsion of the evidence does not violate Fifth Amendment protections.³⁶

II. STAHL'S DIVERGENT INTERPRETATION OF THE FOREGONE CONCLUSION DOCTRINE

Section A of this Part will discuss the trial court's ruling in *State v. Stahl*.³⁷ Section B will discuss the Florida Second District Court of Appeals ruling in *Stahl*.³⁸

A. Trial Court's Ruling in Stahl

In December 2016, the Second District Court of Appeals of Florida in *State v. Stahl* granted the State of Florida's motion to compel the defendant's passcode to his iPhone 5.³⁹ In *Stahl*, a woman shopping in a store caught the defendant attempting to film underneath her skirt.⁴⁰ The defendant was later caught, arrested, and charged with video voyeurism.⁴¹ During his arrest, the defendant told the Sarasota County Police that he did not have his cellphone on him and that it was located at his house.⁴² The police ob-

³⁵ See *id.* (finding that the government already knew the location, authenticity, and existence of the documents being requested, making the production of those documents no longer testimonial); *supra* note 33.

³⁶ See DAVID M. NISSMAN & ED HAGEN, LAW OF CONFESSIONS, § 3:19, Westlaw (database updated June 2017) (stating that an act of production is not testimonial when the existence and the possession of the evidence sought are already known by the government).

³⁷ See *infra* notes 39–52 and accompanying text.

³⁸ See *infra* notes 53–63 and accompanying text.

³⁹ *State v. Stahl*, 206 So. 3d 128, 136 (Fla. Dist. Ct. App. 2016). When the State filed its motion to compel Stahl's passcode, the State understood that the newer versions of Apple's operating system would lock and erase the contents of the phone if there were ten failed attempts to enter the passcode. *Id.* at 128 n.1. Also, Apple would not run extractions on any phones with the iOS 8 or later operating system in response to search warrants because the files that the government would want to be extracted are protected by an encryptions key that is tied to the owner of the phone's passcode, which Apple does not have access to. *Id.* (citing *Privacy*, APPLE INC., <https://www.apple.com/privacy/government-information-requests/> [<https://perma.cc/BM4L-3KVA>]). At the time the State filed its motion to compel, it was unable to determine what iOS operating system was installed on Stahl's phone. *Id.*

⁴⁰ *Id.* at 127.

⁴¹ *Id.* at 128. Video voyeurism is defined in Florida as intentionally using or installing an imaging device to "secretly view, broadcast, or record a person, for their own amusement, entertainment, sexual arousal, gratification, profit, or for the purpose of degrading or abusing another person, who is dressing, undressing, or privately exposing the body, at a place and time when that person has a reasonable expectation of privacy, without that person's knowledge or consent." FLA. STAT. ANN. § 810.14 (West 2007).

⁴² *Stahl*, 206 So. 3d at 128.

tained a warrant to retrieve the phone from his house and search it, but they could not unlock it without the defendant's passcode.⁴³ The defendant refused to provide the police with his passcode and the State subsequently filed a motion to compel the defendant to provide his passcode.⁴⁴

The trial court denied the State's motion to compel and found that forcing the defendant to surrender the passcode would violate his Fifth Amendment privilege against self-incrimination.⁴⁵ The act of giving the passcode would, at the most rudimentary level, force a defendant to "use the contents of his mind" in compelling him to recall the passcode.⁴⁶ If the compulsion of evidence forces a defendant to use the contents of his mind, then that evidence is protected by the Fifth Amendment because it is incriminating and testimonial in nature.⁴⁷

The trial court also found the State could not compel disclosure of the passcode to the defendant's phone by means of the foregone conclusion doctrine.⁴⁸ The foregone conclusion doctrine, originally established in *Fisher*, allows courts to compel evidence that would ordinarily be protected under the Fifth Amendment because that evidence is already known by the State.⁴⁹ The State must satisfy the three prongs of the foregone conclusion

⁴³ *Id.*

⁴⁴ *Id.*

⁴⁵ *Id.*; see *Fisher v. United States*, 425 U.S. 391, 409–10 (1976). For defendants to invoke their Fifth Amendment protection against self-incrimination, they must show that they are being compelled to provide evidence against themselves, that the evidence is incriminating, and that the evidence is testimonial. *Fisher*, 425 U.S. at 409–10. For evidence to be testimonial in nature, the evidence must come from a defendant being compelled to perform an act that forces him to give up a product of his mind. *Id.*; see Soares, *supra* note 21, at 2004 (stating that the Supreme Court has found that evidence is testimonial, and thus induces Fifth Amendment protections, if that evidence is a compelled communication that forces the defendant to reveal the contents of his or her mind). If the evidence was given willingly or created willingly, it will not meet the testimonial requirement. *Fisher*, 425 U.S. at 409–10. Just because evidence is incriminating does not make it testimonial. *Id.*

⁴⁶ *Stahl*, 206 So. 3d at 131.

⁴⁷ *Id.*; see *Doe v. United States*, 487 U.S. 201, 201 n.9 (1988) (finding that forcing a defendant to give the combination to a wall safe violates his Fifth Amendment right against self-incrimination, but that forcing a defendant to give a key to a wall safe does not violate that right, because the former requires that the defendant use the contents of his mind and the latter does not). Forcing a defendant to give the combination to a wall safe violates his Fifth Amendment rights against self-incrimination while forcing a defendant to give a key to a wall safe does not. See *Doe*, 487 U.S. at 201 n.9 (same). This is because the former requires that the defendant use the contents of his mind to give the passcode and the latter does not. *Id.*

⁴⁸ See *Stahl*, 206 So. 3d at 131 (explaining the trial court's conclusion that the State could not rely on the foregone conclusion doctrine to compel Stahl to give the State the passcode to his phone because the State could not establish with reasonable particularity the three prongs of the foregone conclusion doctrine, which are location, possession, and authenticity of the evidence sought).

⁴⁹ See *Fisher*, 425 U.S. at 411 (finding that when the state can prove location, possession, and authenticity of the evidence being requested, then the question is not of testimony but of surrendering the evidence).

doctrine by proving that the State already has knowledge of the location, existence, and authenticity of the evidence.⁵⁰

The trial court found that the foregone conclusion doctrine did not apply because the State failed to establish the location element of the foregone conclusion doctrine, since it was unable to prove that the phone in the State's possession was the same phone that the defendant allegedly had in the store.⁵¹ Furthermore, the State failed to establish possession because the phone came from a home where multiple people lived and the State failed to prove that the phone belonged to the defendant.⁵²

B. Florida Second District Court of Appeals Ruling in Stahl

The Second District Court of Appeals of Florida (hereinafter "appeals court") reversed the trial court's decision for two reasons.⁵³ The appeals court found that the passcode was not testimonial and thus, not protected by the Fifth Amendment privilege against self-incrimination.⁵⁴ Additionally, the court found that the foregone conclusion doctrine applied to the defendant's passcode, so even if the compulsion of the passcode was testimonial, it could be compelled.⁵⁵

⁵⁰ *Id.* at 411–12. The act of producing evidence in response to a subpoena can be testimonial whether or not the evidence itself is testimonial. *Id.* This is because compliance with a subpoena tacitly concedes that the evidence being requested is owned by the individual to whom the subpoena was issued and that the documents handed over are those documents described in the subpoena. *Id.* If the state can prove location, possession, and authenticity of the evidence being requested in the subpoena, however, then the question is not of testimony but of surrendering the evidence, since any fact that the production of that evidence conveys about the existence, location, or authenticity of the evidence is already known to the government. *Id.*

⁵¹ *Stahl*, 206 So. 3d at 131; *United States v. Apple MacPro Computer*, 851 F.3d 238 (3d Cir. 2017) (finding in a child pornography case that the government met the location elements of the foregone conclusion doctrine because the government had established that forensic evidence of the images on the defendant's external hard drives were consistent with child pornography).

⁵² *Stahl*, 206 So. 3d at 131. When the trial court denied the State's motion to compel the passcode, the State appealed to the Second District Court of Appeals of Florida and was granted certiorari. *Id.* at 129.

⁵³ *State v. Stahl*, 206 So. 3d 128, 136 (Fla. Dist. Ct. App. 2016) (finding the trial court misinterpreted the meaning of testimonial communications and the three prongs of the foregone conclusion doctrine).

⁵⁴ *Id.* at 133–34 (finding that Stahl being compelled to give law enforcement the passcode to his phone was not a testimonial act because the passcode was sought only for its contents and the passcode itself has no other evidentiary value or significance).

⁵⁵ *Id.* at 135–36; see Kletter, *supra*, note 26, at 10 (stating that evidence is a foregone conclusion when the location, existence, and authenticity of the evidence is already known, so that even if the act of production conveys a fact regarding the existence, location, or authenticity of the evidence, that fact is already a foregone conclusion).

The holding in *Stahl* does not adhere to the precedent set by the Supreme Court in *Doe* and *Fisher*.⁵⁶ Although the appeals court agreed that an act is testimonial if it forces a defendant to use the contents of his or her mind, either explicitly or implicitly, to communicate some fact, the *Stahl* court determined that courts across the United States, and specifically the trial court in this case, have not properly considered the law as stated in *Doe* and *Fisher*.⁵⁷ The appeals court found that the contents of an accused person's mind must be "extensively used" in the defendant's response to a warrant or must directly relate him or her to the offense that he or she is being charged with in order to have testimonial significance warranting Fifth Amendment protections.⁵⁸ If the compelled evidence does not extensively use the contents of the defendant's mind or directly relate the defendant to the offense that he or she has been charged with, then the compelled information does not have testimonial significance regardless of whether it is a product of someone's mind, and is therefore not protected by Fifth Amendment protections.⁵⁹

In reversing the trial court's decision, the appeals court also determined that the foregone conclusion doctrine should have been found to ap-

⁵⁶ See *Doe v. United States*, 487 U.S. 201, 201 n.9 (1988) (determining that the combination to a wall safe is testimonial because forcing a defendant to recall a passcode would be forcing a defendant to reveal a product of his mind); *Fisher v. United States*, 425 U.S. 391, 411 (1976) (determining that the government could compel the defendant to give the government his or her financial statements because the government already knew the location, possession, and authenticity of the statements so that the defendant's compelled testimony would add little to nothing to the government's case); *Stahl*, 206 So. 3d at 135–36 (finding the trial court misinterpreted the meaning of testimonial communications and the three prongs of the foregone conclusion doctrine).

⁵⁷ See *Stahl*, 206 So. 3d at 133–34 (finding that in order for compelled evidence to be testimonial, that evidence must have independent testimonial significance). The appeals court found that the trial court as well as other courts have misread *Doe* and *Fisher* by not taking into account that in order for compelled evidence to be protected by the Fifth Amendment, that evidence must do more than merely force a defendant to use the contents of his or her mind when giving the compelled evidence. *Id.* That evidence must have testimonial significance on its own in order for it to be protected by the Fifth Amendment. *Id.* Relating this to the facts in *Stahl*'s case, the court found that the passcode did not have any intrinsic testimonial significance. *Id.* Because providing a passcode does not equate to the defendant acknowledging that the phone contains evidence of the crime for which he was being accused, the passcode should not be protected by the Fifth Amendment. *Id.*

⁵⁸ See *id.* at 134. The Appeals Court found that the passcode was not testimonial because the passcode was solely being compelled to open up the phone, the actual code itself did not have testimonial significance. *Id.* If the passcode itself does not have testimonial significance, the defendant would not have to extensively use his mind when giving the State the passcode, so the passcode would not be testimonial. *Id.*

⁵⁹ See *id.* (finding that compelling evidence that does not force a defendant to either "extensively use[]" the contents of his mind or relate him directly to the offense he is being charged with does not reach the level of testimonial evidence, and thus does not invoke Fifth Amendment protections).

ply.⁶⁰ The appeals court found that, even if the passcode were testimonial, it did not merit protection under the Fifth Amendment because the State had established the existence, possession, and authenticity of the compelled evidence through independent means.⁶¹ The appeals court found that the State established that the phone could not be searched without entering a passcode, and so a passcode must exist.⁶² The appeals court also determined that the State established, with reasonable particularity, that the phone was his, and therefore that the passcode would be in his possession.⁶³

III. STATE AND FEDERAL APPLICATION OF THE FOREGONE CONCLUSION DOCTRINE

The foregone conclusion doctrine established by the Supreme Court in *Fisher v. United States* has been particularly important in Fifth Amendment self-incrimination cases that deal with the decryption of data.⁶⁴ With courts interpreting the Supreme Court's decision in *Doe v. United States* to mean that passcodes are protected by the Fifth Amendment and with encryption technology becoming increasingly sophisticated, in many situations the on-

⁶⁰ See *id.* at 135–36 (finding that because the phone needed a passcode to be unlocked and that the State established with reasonable particularity through cellphone carrier records that the phone belonged to Stahl, the State had proven the location, authenticity, and existence of the passcode, making it a foregone conclusion).

⁶¹ See *id.* (finding that the passcode was a foregone conclusion because the government knew the location, authenticity, and existence of the evidence being compelled). The appeals court found that the Sarasota Circuit Court incorrectly applied the foregone conclusion doctrine when they determined that it did not apply because the State had failed to prove location and the possession of the evidence on Stahl's phone. *Id.* The appeals court held instead that it was not determinative that the State found Stahl's phone in a house where five other individuals lived, nor was it determinative that the State could not definitively prove the phone they found at Stahl's residence was the phone he had with him at the store. *Id.*

⁶² *Id.* at 136.

⁶³ *Id.* The appeals court found that the phone the police recovered at the defendant's home was in fact the defendant's phone because the phone's number was registered to the defendant. *Id.* This, in conjunction with the fact that the phone required a passcode to be unlocked, was enough for the appeals court to find that it was a foregone conclusion that the defendant knew that passcode to the phone. *Id.*

⁶⁴ See *Doe v. United States*, 487 U.S. 201, 201 n.9 (1988) (noting that courts have interpreted the Supreme Court's determination in *Fisher*—that a combination to a wall safe merits Fifth Amendment protections—to extend to modern passcodes and passwords used in encrypted electronic devices so as to also categorize them as testimonial, because passcodes and passwords are akin to a combination to a wall safe in that they are products of a person's mind); *Fisher v. United States*, 425 U.S. 391, 412–14 (1976) (noting that courts have applied the foregone conclusion doctrine when evaluating motions to compel encrypted electronics); see also *State v. Stahl*, 206 So. 3d 128, 136 (Fla. Dist. Ct. App. 2016) (finding that when a phone has a passcode and is registered to a defendant, the State can compel the password to the phone because it is a foregone conclusion that the defendant knows that password); *Commonwealth v. Baust*, 89 Va. Cir. 267, 271 (Va. Cir. Ct. 2014) (finding that the only way a passcode could be considered a foregone conclusion would be if the government already knew the passcode).

ly way the government can gain access to defendants' electronic devices is by employing the foregone conclusion doctrine.⁶⁵

With the applicability and importance of the foregone conclusion doctrine growing as technology evolves, it has been left to individual courts to interpret this doctrine, which was established before the modern technological era.⁶⁶ This had led to a range of interpretations of the foregone conclusion doctrine, which is due in part to the ambiguous language that the Supreme Court used to set the standard for the foregone conclusion doctrine in *Fisher*.⁶⁷

In order to apply the foregone conclusion doctrine, the government needs to know the location, authenticity, and existence of evidence, with reasonable particularity, so that the compelled evidence adds little to the government's case.⁶⁸ A majority of courts have applied this language in

⁶⁵ See *Fisher*, 425 U.S. at 412–14 (establishing the foregone conclusion doctrine). The Court held that when the compulsion of evidence forces a defendant to make a testimonial communication, that evidence is protected by the Fifth Amendment. See *id.* (finding that testimonial communications force defendants to use the contents of their minds, which are protected by the Fifth Amendment). If that evidence is found to be a foregone conclusion, however, it loses its Fifth Amendment protection and the government may compel the evidence. See *id.* (establishing that when the government knows the location, authenticity, and existence of evidence, that evidence is a foregone conclusion and is no longer protected by the Fifth Amendment); *Stahl*, 206 So. 3d at 135–36 (finding that if defendant Stahl surrendering his passcode was found to be testimonial, the passcode could still be compelled because the State sufficiently satisfied all the requisite elements of the foregone conclusion doctrine).

⁶⁶ See, e.g., *Stahl*, 206 So. 3d at 136 (finding that when a phone that has a passcode and is registered to a defendant, the State can compel the password to the phone because it is a foregone conclusion that the defendant knows that password); *Baust*, 89 Va. Cir. at 271 (finding that the only way that a passcode could be a foregone conclusion would be if the government already knew the passcode).

⁶⁷ See *Fisher*, 425 U.S. at 410–11 (holding that the government must know the location, authenticity, and possession of evidence in order for that evidence to be considered a foregone conclusion). Compare *Stahl*, 206 So. 3d at 136 (finding that when a phone has a passcode and is registered to a defendant, the State can compel the password to the phone because it is a foregone conclusion that the defendant knows that password), with *Baust*, 89 Va. Cir. at 271 (finding that the only way that a passcode could be considered a foregone conclusion would be if the government already knew the passcode itself); see also Ashley Verdon, *International Travel with a "Digital Briefcase": If Customs Officials Can Search a Laptop, Will the Right Against Self-Incrimination Contravene This Authority?*, 37 PEPP. L. REV. 105, 136–37 (2009) (stating that the foregone conclusions standard of proof, requiring that the government be able to independently prove knowledge of the existence, possession, and authenticity of compelled documents, is an ambiguous standard of proof).

⁶⁸ See *United States v. Hubbell*, 530 U.S. 27, 44–45 (2000) (holding that the government must know the location, authenticity, and possession of evidence with reasonable particularity in order for that evidence to be a foregone conclusion); *Fisher*, 425 U.S. at 410–11 (holding that the government must know the location, authenticity, and possession of the evidence in order for that evidence to be considered a foregone conclusion). In *Hubbell*, the Supreme Court applied the foregone conclusion doctrine established in *Fisher* and used the language "reasonable particularity" when describing the extent to which the government must know the location, authenticity, and possession of the evidence being compelled. 530 U.S. at 32–33. After the Court's decision in

Fisher as a way to balance individual privacy interests with the need for law enforcement to gain access to electronic devices that they have established contain evidence with reasonable particularity.⁶⁹

Both federal and state courts have attempted to reasonably apply the foregone conclusion doctrine.⁷⁰ Two examples of federal cases contemplating the application of the foregone conclusion doctrine are *United States v. Doe* and *United States v. Apple MacPro Computer*.⁷¹ In *Doe*, the Eleventh Circuit denied the government's motion to compel a password for the defendant's electronic devices, finding that the foregone conclusion doctrine did not apply to the facts of the case.⁷² The law enforcement officials in

Hubble, that language is what courts look to when conducting a test of whether to apply the foregone conclusion doctrine. *See id.* In *Hubble*, the Court found that the foregone conclusion doctrine did not apply because unlike the facts in *Fisher*, the government did not know with reasonable particularity the existence, possession, and authenticity of the subpoenaed documents. *Id.* at 44–45. In *Fisher*, the Court determined that these elements were met because the Internal Revenue Service knew that the defendant's accountants had prepared the documents and the documents were in the possession of his attorney, allowing the government to independently confirm the documents' existence and location. *Fisher*, 425 U.S. at 411. Here, the government did not show that it had any prior knowledge of the existence or location of the documents produced by the defendant. *Hubbell*, 530 U.S. at 44–45; *United States v. Greenfield*, 831 F.3d 106, 116 (2d Cir. 2016) (finding that the government must show that it knew the location and existence of evidence with reasonable particularity in order for that evidence to be a foregone conclusion); *Slavin v. Artus*, No. 05-CV-0870 (JS), 2010 U.S. Dist. LEXIS 2939, at *9 (E.D.N.Y. Jan. 13, 2010) (finding that it is a settled proposition that an individual may be required to produce incriminating documents, which would otherwise be protected under the Fifth Amendment, if the government knows with reasonable particularity the existence and location of the documents).

⁶⁹ *See United States v. Apple MacPro Computer*, 851 F.3d 238, 248 (3d Cir. 2017) (finding that because the government could show through forensics that there were photographs on the defendant's hard drive that were consistent with child pornography and the hard drive was taken from the defendant's possession, the government met the requisite requirements of the foregone conclusion doctrine and therefore the defendant's passcode could be compelled); *In re Grand Jury Subpoena Duces Tecum* 670 F.3d 1335, 1346–47 (11th Cir. 2012) (finding that the government did not know with reasonable particularity that there was child pornography on the defendant's hard drive and therefore could not compel the defendant to disclose the passcode to the hard drive); *Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 615–16 (Mass. 2014) (finding that the State met the elements necessary to invoke the foregone conclusion doctrine by providing evidence that the defendant had ownership and control of the computers when they were seized, knowledge of the fact that they were encrypted, and knowledge of the kind of decryption key that was necessary to unlock this type of encryption).

⁷⁰ *See supra* note 69.

⁷¹ *See Apple MacPro Computer*, 851 F.3d at 238 (finding that because the government could show through forensics that there were photographs on the defendant's hard drive that were consistent with child pornography and the hard drive was taken from the defendant's possession, the government met the requisite requirements of the foregone conclusion doctrine so the defendant's passcode could be compelled); *Doe*, 670 F.3d at 1346–47 (finding that the government did not know with reasonable particularity that there was child pornography on the defendant's hard drive, so the government could not compel the defendant to give them the passcode to the hard drive).

⁷² *See Doe*, 670 F.3d at 1346–47 (finding that the State had not established possession because the evidence in the defendant's computer was insufficient to prove that there were photographs on the defendant's hard drives).

Doe connected IP addresses to a hotel room, which the defendant was using to share child pornography, and seized all electronic devices found in the room.⁷³ The government seized two laptops and five external hard drives, and gained access to the laptops but not to the hard drives due to encryption.⁷⁴ The government filed a motion to compel the password to the encrypted drives, which was granted by the United States District Court for the Eastern District of Pennsylvania.⁷⁵ On appeal, the Eleventh Circuit reversed the district court's opinion in finding that the government did not know with "reasonable particularity" at the time it sought to compel the act of production, the specific materials on the hard drive, thereby failing to qualify the materials as a foregone conclusion.⁷⁶ The government's argument that the encrypted drives were capable of storing vast amounts of data, some of which may be incriminating, was not enough to persuade the Eleventh Circuit to grant the motion to compel.⁷⁷ In short, although the government physically possessed the media storage devices, it did not have actual knowledge of what, if anything, was stored in those encrypted drives.⁷⁸

In the 2017 case *United States v. Apple MacPro Computer*, the United States Court of Appeals for the Third Circuit upheld a magistrate judge's decision to compel the passcode to an external hard drive based on the government's satisfaction of the foregone conclusion doctrine.⁷⁹ The Third Circuit held that because the government had established that there was forensic evidence of the images on the external hard drives consistent with child pornography, the passcode to those drives could properly be compelled.⁸⁰

⁷³ *Id.* at 1339.

⁷⁴ *Id.*

⁷⁵ *Id.* at 1340.

⁷⁶ *Id.* at 1346–47 (finding that the State had not established the requisite element of possession of the foregone conclusion doctrine because the State's evidence was insufficient to prove that there were photographs on the defendant's hard drives).

⁷⁷ *Id.* The Eleventh Circuit did not find the government's argument persuasive. *Id.* The government argued that since it knew that the external hard drives could store vast amounts of information, that the hard drives were found in a room linked to child pornography, and that the hard drives were encrypted, that collective reasoning should be sufficient to establish that it was a foregone conclusion that evidence of child pornography could have been found on the drives. *Id.*

⁷⁸ *Id.* at 1347 (finding that the government could show that there were a series of random characters in the hard drive, but could not prove that this meant there were files on the hard drive consistent with child pornography).

⁷⁹ See *Apple MacPro Computer*, 851 F.3d at 238 (finding that because the government could show through forensics that there were photographs on the defendant's hard drive that were consistent with child pornography and the hard drive was taken from the defendant's possession, the government met the requisite requirements of the foregone conclusion doctrine, and therefore the defendant's passcode could be compelled).

⁸⁰ *Id.* The court found that this case was dissimilar to *United States v. Doe* because the government was able to prove authenticity, location, and possession of the evidence. *Id.* The government had custody of the hard drives, prior to seizing the drives they were in the defendant's possession, and the images on the electronic devices were consistent with child pornography. *Id.*

The government had established with reasonable particularity that those files existed on the hard drives, and that the defendant possessed, accessed, and owned the devices prior to the government's seizure.⁸¹

State courts have also applied the doctrine in a way that balances individual and state interests.⁸² The 2014 Massachusetts Supreme Judicial Court case *Commonwealth v. Gelfgatt* is one example of a state court applying the foregone conclusion doctrine in a way that balances individual and state rights.⁸³ In *Gelfgatt*, a grand jury indicted the defendant on counts of forgery of a document, uttering a forged instrument, and larceny by false pretenses of the property of another.⁸⁴ These charges arose from evidence that the defendant, through his computers, was diverting money to himself from his clients' accounts.⁸⁵ The Commonwealth seized the defendant's computers, but was unable to access them because of their encryption.⁸⁶ The Commonwealth filed a motion to compel the passcode to the two computers, which the Suffolk County Superior Court denied on Fifth Amendment grounds.⁸⁷ The Massachusetts Supreme Judicial Court reversed the superior

⁸¹ *See id.*

⁸² *See Gelfgatt*, 11 N.E.3d at 615. The Massachusetts Supreme Judicial Court found that the Commonwealth had established possession, location, and authenticity of the evidence located inside the defendant's encrypted computers. *Id.* To establish these elements, thus invoking the foregone conclusion doctrine, the Commonwealth showed that the defendant had ownership and control of the computers when they were seized, knowledge of the fact that they were encrypted, and knowledge of the kind of decryption key that was necessary to unlock this type of encryption. *Id.*; *Vilan v. Ryan*, No. 1 CA-SA 09-0066, 2009 Ariz. App. Unpub. LEXIS 514, at *21–23 (Ariz. Ct. App. May 21, 2009) (holding that the trial court properly held the defendant in contempt when she refused to turn over her house to receivership because although the act of turning over the house could be testimonial because the jury could see it as an admission that the defendant had control of the house, the government already knew that the defendant had possession of the house, the house existed, and the evidence the government had about her owning the house was authentic, so that the act of turning over the house in receivership to the government would add little to nothing to the government's case).

⁸³ *See Gelfgatt*, 11 N.E.3d at 615 (finding that although the compulsion of the defendant's passcode would normally be protected under the Fifth Amendment, the State established that they knew with reasonable particularity the location, authenticity, and possession of the evidence in the defendant's laptops, so the Fifth Amendment protections were void).

⁸⁴ *Id.* at 608.

⁸⁵ *See id.* (noting that the defendant was accused of conducting a sophisticated scheme of diverting his clients' money, which was supposed to be used to pay off large mortgage loans on residential properties, into his own accounts).

⁸⁶ *Id.* at 609–10. On December 17, 2009, state police arrested the defendant. *Id.* The state police also searched the defendant's residence, where they found several computers. *Id.* They seized two desktop computers, one laptop computer, and various other devices from the residence that had the ability to store electronic data. *Id.*

⁸⁷ *Id.* at 611–12. The superior court found that even though the Commonwealth was only asking the defendant for a sequence of numbers that would enable the Commonwealth to access the information on the defendant's computers, this would still violate the Massachusetts state and federal Constitutions. *Id.* The superior court found that compelling the defendant to give the Commonwealth his passcode constituted an "admission of knowledge ownership and control,"

court's decision, reasoning that although the passcode was testimonial and thus would normally be protected under the Fifth Amendment, the Commonwealth knew with reasonable particularity the location, authenticity, and possession of the evidence on the laptops.⁸⁸ As such, the forgone conclusion doctrine should appropriately apply.⁸⁹

IV. WHY *STATE V. STAHL* PRESENTS A POTENTIALLY DANGEROUS INTERPRETATION OF THE FOREGONE CONCLUSION DOCTRINE

The forgone conclusion doctrine, established in *Fisher v. United States* and applied by various federal and state courts since, has been utilized in attempts to balance vital individual privacy rights with the need for law enforcement to gain access to electronic devices that they have established with reasonable particularity contain relevant evidence.⁹⁰ Today, this balance is more important than ever, with an individual's ability to encrypt their personal devices constantly improving, and investigative technology and surveillance more omnipresent and advanced than ever before.⁹¹ Most state and federal courts have been able to balance individual privacy interests and state interests; however, the Florida Second District Court of Ap-

making the passcode testimonial. *Id.* The defendant refusing to give his passcode to law enforcement during his initial interview constituted the defendant invoking his Fifth Amendment right. *Id.*

⁸⁸ *See id.* (finding that because the defendant was linked to the crimes, the hard drives were in his possession, and he admitted knowing that the laptops were encrypted, how to decrypt them, and that the people he was being accused for committed these crimes with used this type of decryption, it was a foregone conclusion that he had ownership and knowledge of the data inside the hard drives and that this data existed in the hard drives).

⁸⁹ *Id.* Christine Licalzi, *Computer Crimes*, 54 AM. CRIM. L. REV. 1025, 1069 (stating that the Massachusetts Supreme Judicial Court in *Gelfgatt*, as well as other state courts, have found that the foregone conclusion applies to forced decryption).

⁹⁰ *See Fisher v. United States*, 425 U.S. 391, 411 (1976) (determining that when the government already knows the location, authenticity, and possession of evidence, compelling a defendant to hand over that evidence is no longer considered a testimonial act by the defendant, but an act of surrender that does not invoke Fifth Amendment protections); *supra* notes 64–89 and accompanying text; *see also State v. Stahl*, 206 So. 3d 124, 136 (2014) (finding that when a phone has a passcode and is registered to a defendant, the State can compel the password to the phone because it is a foregone conclusion that the defendant knows that password); *Commonwealth v. Baust*, 89 Va. Cir. at 267 (Va. Cir. Ct. 2014) (finding that the only way that a passcode could be deemed a foregone conclusion would be if the government already knew the passcode).

⁹¹ *See Apple Announces iOS 8 Available September 17*, *supra* note 5, at 1; Smith, *supra* note 3, at 1; Craig Timberg, *New Surveillance Technology Can Track Everyone in an Area for Several Hours at a Time*, WASH. POST (Feb. 5, 2014), https://www.washingtonpost.com/business/technology/new-surveillance-technology-can-track-everyone-in-an-area-for-several-hours-at-a-time/2014/02/05/82f1556e-876f-11e3-a5bd-844629433ba3_story.html?utm_term=.d40c1424acf6 [<https://perma.cc/7Q5H-8P9D>] (stating that law enforcement with new surveillance technology can compile second by second images over an area the size of a small city for several hours at a time, an ability that law enforcement did not have a few years ago).

peals broke this trend in *State v. Stahl*.⁹² The appeals court's extreme interpretation of the doctrine, if adopted by other courts, could effectively end the Fifth Amendment protections associated with passcodes and passwords.⁹³

In *Stahl v. Stahl*, the appeals court found that the State did not need to establish possession, authenticity, and location of evidence of voyeurism on the defendant's phone in order to compel him to give the state his passcode.⁹⁴ Instead, the State needed only prove that the cellphone could be associated to the defendant for the doctrine to apply.⁹⁵ If the foregone conclusion doctrine were applied according to traditional Supreme Court precedent, the State's motion to compel the defendant's passcode based on the doctrine would have likely been denied, due to the State's inability to show

⁹² See *Stahl*, 206 So. 3d at 124 (finding that the requisite elements of the foregone conclusion doctrine are met if the government can prove that a phone belongs to a defendant and that that phone cannot be opened without a passcode); *supra* notes 64–90 and accompanying text.

⁹³ See *Stahl*, 206 So. 3d at 124 (finding that the only thing necessary for a passcode to be a foregone conclusion is evidence that the phone belongs to the defendant and evidence that the phone requires a passcode to open); *Baust*, 89 Va. Cir. at 271 (finding that the foregone conclusion doctrine nearly never applies, since the doctrine does not apply unless the government already knows the passcode to an encrypted device before compelling the defendant to give them the passcode). On the other end of the ideological spectrum, the Circuit Court of the City of Virginia Beach, in *Commonwealth v. Baust*, found that the only way that evidence could be considered a foregone conclusion would be if the government already had that evidence. See *Baust*, 89 Va. Cir. at 271. In *Baust*, the defendant was charged with assaulting a woman in his bedroom. *Id.* at 267. The victim stated that the defendant maintained a recording device in his home that continuously recorded in the room where the assault took place, and that this recording device transmitted footage directly to his smartphone. *Id.* When the officers at the scene asked the defendant and the victim if the recording device could have recorded the alleged assault, both affirmed that it is possible that the it could have recorded it. *Id.* at 267–68. With this testimony, the government argued that the actual compulsion of the passcode would add little to the government's information about the case, because both the victim and the defendant already affirmed that there was a recording device that transmitted footage to the defendant's smartphone. *Id.* at 268. The government knew with reasonable particularity that the recording of the assault was likely on the defendant's phone, so the passcode was a foregone conclusion. See *id.* The court, however, denied the government's motion to compel the defendant's passcode because it found that the only way that the passcode could be a foregone conclusion would be if the Commonwealth already knew the passcode. *Id.* at 271. This interpretation of the foregone conclusion doctrine, if followed by other courts, would constructively eliminate the ability of law enforcement to use the foregone conclusion doctrine in data encryption and passcode cases. See *id.*

⁹⁴ See *Stahl*, 206 So. 3d at 131 (explaining the trial court's finding that the State was unable to prove possession or authenticity of the phone because the State was unable to prove that the phone found at the defendant's residence, a residence that he shares with roommates, was the phone he had when he allegedly committed voyeurism); Kletter, *supra* note 26, at 10 (stating that Fifth Amendment protections apply to testimonial evidence unless the location, existence, and authenticity of the evidence is already known).

⁹⁵ See *Stahl*, 206 So. 3d at 131 (finding that the foregone conclusion requirements would be met if the government could prove that the phone belonged to the defendant and required a passcode to open).

knowledge of possession and location of the phone.⁹⁶ The State was unable to prove the location element of the foregone conclusion doctrine for the phone since it could not show that the actual phone that the police found at the defendant's house was the same one he used at the crime scene.⁹⁷ Additionally, the government could not prove the possession element of the foregone conclusion doctrine because it could not show that the phone belonged to the defendant, since it was found in a house where five other individuals lived.⁹⁸ Without being able to prove the location and possession elements of the foregone conclusion doctrine, the court, in accordance with *Fisher* and its progeny, should have denied the motion to compel the defendant's passcode.⁹⁹

Instead, the court in *Stahl* reasoned that any electronic device with a passcode encryption must have a password associated with the encryption, and if the government can provide evidence that the defendant owns that electronic device or that the electronic device is registered under the defendant's name, then it is a foregone conclusion that the government knows the phone's passcode.¹⁰⁰

This reasoning uses the foregone conclusion doctrine to completely invalidate the key combination distinction made in *United States v. Doe*.¹⁰¹ A

⁹⁶ See *id.* at 131, 136 (finding that the government was not required to prove that the evidence existed on the phone, but only that the phone belonged to the defendant and required a passcode); see also Robert Mosteller, *Simplifying Subpoena Law: Taking the Fifth Amendment Seriously*, 73 VA. L. REV. 1, 35–36 (1987) (stating that there are two ways in which courts have applied the foregone conclusion doctrine: one that imposes a more rigorous exacting standard that seems to follow the Supreme Court precedent in *Fisher* and *Hubble*, and one that applies a more lenient standard).

⁹⁷ See *Stahl*, 206 So. 3d at 131, 136 (finding that the government did not have to prove that the phone they found at the defendant's residence was the phone the defendant had at the store, but only that the phone belonged to the defendant).

⁹⁸ See *id.* (finding that it was enough that there were phone carrier records that connected the defendant to the phone); Mosteller, *supra* note 96, at 25 (explaining that possession through an act of production implicates the Fifth Amendment when production tends to establish possession of the evidence being compelled at an earlier time when a crime was committed, and that in order for the government to void this Fifth Amendment protection it must show that it independently can prove this link of possession).

⁹⁹ See *Stahl*, 206 So. 3d at 131, 136 (broadening the scope of the foregone conclusion doctrine by only requiring that there was some evidence that connected the defendant to the phone and that the phone belonged to the defendant); see also *Fisher*, 425 U.S. at 412–14 (determining that the government needs to prove the location, authenticity, and possession of evidence in order for that evidence to fall within the foregone conclusion exception).

¹⁰⁰ See *Stahl*, 206 So. 3d at 136; Mosteller, *supra* note 96, at 8, 25 (stating that when possession through an act of production implicates the Fifth Amendment, the foregone conclusion should only apply when the government has independent evidence of the possession of the evidence, so that the production of that evidence adds little to nothing to the government's case).

¹⁰¹ See *Doe v. United States*, 487 U.S. 201, 201 n.1 (1988) (determining that a wall safe combination is protected by the Fifth Amendment because it is a product of an individual's mind); Soares, *supra* note 21, at 2005 (stating that the Supreme Court has distinguished between physical

passcode or a combination to a wall safe would no longer have any Fifth Amendment protections, even if it was considered testimonial by the court.¹⁰²

CONCLUSION

The Florida Second District Court of Appeals decision in *State v. Stahl* breaks from Supreme Court precedent in both *Doe v. United States* and *United States v. Fisher*, and could subsequently have devastating results if followed by other courts. The foregone conclusion doctrine, which up to this point was used as a balancing test, could become an unchecked tool of the State to force the compulsion of testimonial evidence that in the past has been protected by the Fifth Amendment. In a world where almost every aspect of a person's life is connected to the technology that he or she uses, the *Stahl* court's interpretation of the foregone conclusion doctrine could lead to the circumvention of prior constitutional privacy rights and allow the State to have access to almost every aspect of a person's life by simply getting a warrant to search their devices.

JESSE COULON

Preferred Cite: Jesse Coulon, Comment, *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 (2018), <http://lawdigitalcommons.bc.edu/bclr/vol59/iss9/225/>.

acts of surrender and acts that force a defendant to divulge the contents of his or her mind, by finding that the former does not invoke Fifth Amendment protections while the latter does).

¹⁰² See *Stahl*, 206 So. 3d at 136; see Kletter, *supra*, note 26, at 10 (stating that evidence is a foregone conclusion when the location, existence, and authenticity of the evidence is already known, so that even if the act of production conveys a fact regarding the existence, location, or authenticity of the evidence, that fact is already a foregone conclusion).