NOT FINAL UNTIL TIME EXPIRES TO FILE REHEARING
MOTION AND, IF FILED, DETERMINED

IN THE DISTRICT COURT OF APPEAL

OF FLORIDA

SECOND DISTRICT

STATE OF FLORIDA, Petitioner, v. AARON STAHL, Respondent.	)	Case No. 2D14-4283

Opinion filed December 7, 2016.

Petition for Writ of Certiorari to the Circuit Court for Sarasota County; Frederick P. Mercurio, Judge.

Pamela Jo Bondi, Attorney General, Tallahassee, and Bilal A. Faruqui, Assistant Attorney General, Tampa, for Petitioner.

Howard L. Dimmig, II, Public Defender, and Tosha Cohen, Assistant Public Defender, Bartow, for Respondent.

BLACK, Judge.

The State seeks a writ of certiorari quashing the trial court's order denying the State's motion to compel the production of the passcode to unlock Aaron Stahl's cellphone. We grant the petition and quash the order.

I. Background

Stahl was charged with video voyeurism in violation of section 810.145(2)(c), Florida Statutes (2014), a third-degree felony. The probable cause affidavit for Stahl's arrest stated that the victim was shopping in a store when she observed a man crouching down with what she believed was a cellphone in his hand. She saw that the screen of the cellphone was illuminated. She then observed the man with his arm extended, holding the cellphone under her skirt. The victim confronted him, and the man told her that he had dropped his cellphone. While yelling for assistance, the victim attempted to detain the man, but he was able to free himself and flee the store before assistance arrived.

Store surveillance video confirmed that the man crouched down with an illuminated device in his hand, moving it toward the victim's skirt. It also showed the man exit the store and get into a vehicle in the parking lot. Using the vehicle's license plate number, law enforcement identified Stahl as the registered owner of the vehicle and obtained his driver's license photo. Law enforcement positively identified Stahl as the man in the surveillance video.

Stahl was arrested but a cellphone was not found on his person. During an interview with law enforcement, Stahl admitted to being in the store, denied taking inappropriate images, and verbally consented to a search of his cellphone, which he

identified as an Apple iPhone 5 located in his residence. After officers retrieved the cellphone from Stahl's residence, Stahl withdrew his consent to search the phone.

The next day law enforcement sought a search warrant for the contents of Stahl's cellphone. The search warrant affidavit described the phone as an Apple iPhone 5 with a cracked screen and a piece of glass missing from the top right corner. It also listed the phone number associated with the phone and the service provider. The search warrant affidavit provided that the victim believed the device in Stahl's hand to be a cellphone and that when she confronted Stahl, he told the victim he had dropped his cellphone. It further provided that Stahl initially consented to a search of his iPhone 5 and that he confirmed the phone number and provided the location of the phone. A search warrant was issued for the contents of the described Apple iPhone 5.

However, the State was unable to execute the warrant and view the contents of the phone because Stahl's cellphone is passcoded and he refused to give law enforcement the passcode. As a result, the State filed a motion to compel production of the passcode. The State alleged that without compelling Stahl to provide the passcode, law enforcement's only option would be to send the phone to Apple to obtain the passcode.[1] The State also alleged that there is no Fifth Amendment

[1]The State contended that sending the phone to Apple would create chain of custody concerns because it did not "know who would have it at the manufacturer, what they would have to do to get into it" and that timeliness was an issue because the manufacturer indicated that the phone would be logged in to the system, only worked on after receipt of a court order, and then shipped back. At the time the State filed its motion, it was known that devices running certain versions of Apple's operating system would permanently lock and potentially erase all of the device's content after ten failed attempts to enter the passcode, but it was unknown that "[f]or all devices running iOS 8 and later versions, Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess."

implication in compelling Stahl to give officers the passcode in this case.[2] Stahl did not file any response to the motion.

At the hearing on the State's motion to compel, neither side presented testimony or evidence; only argument was presented. In denying the motion, the trial court found that the Fifth Amendment privilege against self-incrimination applied such that Stahl could not be compelled to produce the passcode. The court determined that production of the passcode was testimonial and that the State had not sufficiently established that the foregone conclusion doctrine applied.

The State appealed the order denying its motion, contending the order was reviewable pursuant to Florida Rule of Appellate Procedure 9.140(c)(1)(B), permitting State appeals from orders suppressing evidence obtained by search and seizure.[3] In response to an order to show cause why this case should not be dismissed as from a nonfinal, nonappealable order, the State contended that if not appealable as an order suppressing evidence, the order is reviewable by petition for writ of certiorari.

Privacy, Apple Inc., https://www.apple.com/privacy/government-information-requests/ (last visited Oct. 20, 2016). Unlike In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 149 F. Supp. 3d 341 (E.D. N.Y. 2016), the State is apparently unable to determine what iOS is installed on Stahl's phone.

[2]Nothing in our record establishes whether Stahl invoked his Fifth Amendment privilege against self-incrimination or the State preemptively raised the issue. See amend. V, U.S. Const.

[3]Because a warrant has been issued allowing the State to search Stahl's phone, the order denying the motion to compel is more akin to an order suppressing evidence than to an order denying discovery. Cf. State v. Isaac, 696 So. 2d 813, 813 (Fla. 2d DCA 1997); State v. Foley, 193 So. 3d 24, 26 (Fla. 3d DCA 2016).

This court subsequently issued an order converting the appeal to a petition for writ of certiorari and directing the parties to address the certiorari standard.

II. Standard of Review

> The ability of the district courts of appeal to entertain [S]tate petitions for certiorari to review pretrial orders in criminal cases is important to the fair administration of criminal justice in this state. Otherwise, there will be some circumstances in which the [S]tate is totally deprived of the right of appellate review of orders which effectively negate its ability to prosecute. If a nonfinal order does not involve one of the subjects enumerated in Florida Rule of Appellate Procedure 9.140(c)(1), the [S]tate would not be able to correct an erroneous and highly prejudicial ruling. Under such circumstances, the [S]tate could only proceed to trial with its ability to present the case significantly impaired. Should the defendant be acquitted, the principles of double jeopardy prevent the [S]tate from seeking review; thus, the prejudice resulting from the earlier order would be irreparable.

State v. Pettis, 520 So. 2d 250, 253 (Fla. 1988). Where the State has met the jurisdictional requirements for a writ of certiorari—a ruling that significantly impairs the State's ability to prosecute which could not be remedied via postjudgment appeal—and has established that the trial court violated a clearly established principle of law, issuance of a writ of certiorari is "an apt remedy." Id.; see also State v. Fernandez, 141 So. 3d 1211, 1216 (Fla. 2d DCA 2014) ("[T]he trial court's pretrial order would leave the State without an effective remedy and cause irreparable harm. Accordingly, this is a case where certiorari review is an 'apt remedy.' " (quoting Pettis, 520 So. 2d at 253)); State v. Sandoval, 125 So. 3d 213, 215 (Fla. 4th DCA 2013) ("To obtain certiorari relief from a pretrial evidentiary ruling, the [S]tate must show that the ruling was a violation of a clearly established principle of law resulting in a miscarriage of justice."). Here, the

order is not appealable pursuant to rule 9.140(c)(1) and the State cannot appeal an acquittal. See Pettis, 520 So. 2d at 253.

Stahl was charged with the third-degree felony of video voyeurism by "intentionally us[ing] an imaging device to secretly view, broadcast, or record under or through the clothing being worn by another person, without that person's knowledge and consent, for the purpose of viewing the body of, or the undergarments worn by, that person" for his "amusement, entertainment, sexual arousal, gratification, or profit." § 810.145(2)(c). A necessary element of the crime is the use of an imaging device, defined as "any mechanical, digital, or electronic viewing device; still camera; camcorder; motion picture camera; or any other instrument, equipment, or format capable of recording, storing, or transmitting visual images of another person." § 810.145(1)(b). Absent photographic or video evidence of the crime, the State's case would rest solely on the victim's statements and the video surveillance depicting Stahl moving a device in his hand toward the victim's skirt. It is apparent that the trial court's ruling serves as a serious impediment to the State's case if it does not altogether destroy it. The court's order denies the State the ability to execute an unchallenged search warrant, effectively denying the State access to what is likely to be direct evidence establishing elements of the charged offense. Cf. State v. Crumbley, 143 So. 3d 1059, 1065-66 (Fla. 2d DCA 2014) ("This appeal involves an order that prevents the State from developing its evidence in the criminal case . . . . The order not only suppresses the evidence, it seals the information so that the State can never know what evidence is contained within the sealed documents.").

III. The hearing

At the hearing on the State's motion, the court began by asking various questions. The court inquired "How do I know that there was a picture taken?" and "What evidence are you asking me to rely on that gives me probable cause to believe a picture was taken?" The State responded that a warrant had been issued for the contents of the phone and probable cause was "not the issue at this point" but that based on the circumstances, the State believed there were photographs or video taken, based on the surveillance video and the victim's statements.[4] The State then set forth why the Fifth Amendment privilege against self-incrimination is not implicated, identifying the three requirements necessary for a defendant to successfully invoke the privilege. The State argued that there was no difference between the court finding probable cause to issue the warrant and compelling Stahl to assist the State in "opening up" the phone. The State further argued that law enforcement's forensic expert had advised that he could not gain access to the phone because of the passcode and that if he tried to enter every possible combination the phone could permanently lock and potentially erase all of the contents.[5]

---

[4]The trial court's focus on probable cause was misplaced. The State had a search warrant for the contents of the phone. Stahl has not challenged the validity or execution of that warrant. The only issue before the court was whether it could compel Stahl to provide the passcode.

[5]The State made no mention of whether it had attempted to compel Stahl to unlock the phone using his fingerprint. At least one court has held that compelling a witness to use his fingerprint to unlock or access his cellphone is not testimonial. See Commonwealth v. Baust, 89 Va. Cir. 267 (Va. Cir. Ct. 2014). Nor has the State attempted to compel Stahl to produce the contents of the phone without divulging the passcode. Cf. In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335 (11th Cir. 2012).

The court stated that while probable cause existed for the search warrant, the State did not know "for sure" whether a photo or video was on the phone. The court was incredulous that this was a case of first impression, but the State maintained that a dearth of case law existed. The court asked whether the State knew if there was additional security or encryption on the phone or the portion of the phone that stores photographs. Attempting to focus the issue on whether the giving of the passcode itself is testimonial, the State cited In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012), for the principle that production of the passcode would not be testimonial under the foregone conclusion doctrine—where the location, existence, and authenticity of the requested information are known with reasonable particularity. The State went so far as to agree to give Stahl immunity for the act of providing the passcode. When pressed by the court, the State conceded that "in the most technical sense" the court would be forcing Stahl to "use the contents of his mind" in compelling him to provide the passcode.

Stahl argued that the State did not establish the three prongs of the foregone conclusion doctrine. He contended that the State failed to establish location because it was unable to prove that the phone in the State's possession is the phone Stahl allegedly had at the store. He argued that the phone in the State's possession came from a home in which multiple people lived and that the State presented no evidence to show that the phone was Stahl's or that it was the phone from the store surveillance.

In reply, the State argued that it did not have to meet the foregone conclusion elements until it had been determined that the Fifth Amendment privilege

against self-incrimination was applicable. The State reiterated its position that the privilege is not implicated because providing the passcode is not testimonial.

In its written order denying the State's motion, the court found that production of the passcode would require the use of the contents of Stahl's mind and was therefore testimonial. The court then found that the State had not satisfied the reasonable particularity standard of the foregone conclusion doctrine.

IV. Analysis

A. The privilege

The Fifth Amendment to the United States Constitution provides in pertinent part that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself[.]" Amend. V, U.S. Const. This privilege against self-incrimination "protects a person only against being incriminated by his own compelled testimonial communications." Doe v. United States, 487 U.S. 201, 207 (1988) (quoting Fisher v. United States, 425 U.S. 391, 409 (1976)); see also Kessler v. State, 991 So. 2d 1015, 1021 (Fla. 4th DCA 2008) ("The Fifth Amendment privilege protects an accused from being compelled to testify against himself, or otherwise provide the state with evidence of a testimonial or communicative nature." (citing Schmerber v. California, 384 U.S. 757, 763 (1966))). "The word 'witness' in the constitutional text limits the relevant category of compelled incriminating communications to those that are 'testimonial' in character." United States v. Hubbell, 530 U.S. 27, 34 (2000); see also Heddon v. State, 786 So. 2d 1262, 1263 (Fla. 2d DCA 2001) (stating that the privilege against self-incrimination "only precludes forcing an accused to produce incriminating testimonial communications"). "[I]n order to be testimonial, an accused's

communication must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a 'witness' against himself." Doe, 487 U.S. at 210 (footnote omitted).

In order for Stahl to have properly invoked his Fifth Amendment privilege he needed to establish three things: (1) compulsion, (2) a testimonial communication or act, and (3) incrimination. In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d at 1341 (In re Grand Jury). "Once an individual has invoked his privilege against self-incrimination, it becomes the duty of the trial court to determine whether there is a reasonable basis for the assertion of the privilege and whether the privilege has been invoked in good faith." St. George v. State, 564 So. 2d 152, 155 (Fla. 5th DCA 1990). Because the State does not contend otherwise, for purposes of this opinion, we presume that Stahl invoked the privilege.[6]

Although not expressly stated, it is apparent from the record and from the State's filings with this court that the State concedes that producing the password to the phone would be incriminatory. See Commonwealth v. Gelfgatt, 11 N.E.3d 605, 612 (Mass. 2014) ("[T]he entry of the encryption key or password presumably would be incriminating because 'it would furnish the Government with a link in the chain of

[6]Although the transcript of the proceedings below makes it clear that the court did not require Stahl to establish the three components of the privilege but rather assumed the privilege applied and placed the burden on the State to rebut or overcome the claim, we recognize that the somewhat unusual procedural posture in which the issue arose likely caused this burden shift. Cf. State v. Mitrani, 19 So. 3d 1065, 1068 (Fla. 5th DCA 2009) ("If a witness rightfully invokes the privilege against self-incrimination, the State may overcome the claim of privilege . . . ."); In re Grand Jury, 670 F.3d at 1341 ("An individual must show three things to fall within the ambit of the Fifth Amendment . . . ."). Despite this apparent error, the State does not raise the burden shift as a basis to grant certiorari relief.

evidence leading to [the defendant's] indictment.' " (second alteration in original) (quoting Doe, 487 U.S. at 207 n.5)). It also appears that the State has conceded that producing the password would be compelled within the meaning of the privilege.[7] Thus, the crux of the State's argument below, and its argument as to the trial court's departure from the essential requirements of the law, is whether the State sought protected testimony from Stahl.

B. Act of Production

The Fifth Amendment privilege against self-incrimination has been held to apply not only to verbal and written communications but also to the production of documents, usually in response to a subpoena or summons, because the act of production itself could communicate incriminatory statements. See Fisher, 425 U.S. at 410. The courts that have addressed the Fifth Amendment implications for providing decryption keys and passcodes have largely applied the act-of-production doctrine and the foregone conclusion exception. See, e.g., Sec. & Exch. Comm'n v. Huang, No. 15-269, 2015 WL 5611644, *1 (E.D. Penn. Sept. 23, 2015); United States v. Fricosu, 841

[7]We do not believe it is at all clear that producing the password is compelled within the meaning of the privilege because it is a "settled proposition that a person may be required to produce specific documents even though they contain incriminating assertions of fact or belief because the creation of those documents was not 'compelled' " but was voluntary. Hubbell, 530 U.S. at 35-36 (emphasis added); see Fisher, 425 U.S. at 409-10. That is, Stahl may be required to produce the password even though it may be testimonial and incriminate him because the creation of the password was not compelled. Stahl is not being asked to cull through existing documents and assemble a set of documents which he believes are responsive to the subpoena—something newly created and compelled to be created pursuant to subpoena. See In re Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d 87, 93 (2d Cir. 1993) ("Self-incrimination analysis now focuses on whether the creation of the thing demanded was compelled and, if not, whether the act of producing it would constitute compelled testimonial communication.").

F. Supp. 2d 1232, 1235 (D. Col. 2012); In re Grand Jury Subpoena to Boucher (In re Boucher), 2:06-MJ-91, 2009 WL 424718, *2-3 (D. Vt. Feb. 19, 2009); Gelfgatt, 11 N.E.3d at 612; Commonwealth v. Baust, 89 Va. Cir. 267 (Va. Cir. Ct. 2014). But see United States v. Kirschner, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) (concluding that providing the password was testimony protected by the privilege against self-incrimination).

Invoking the privilege still requires the accused to establish compulsion, a testimonial communication, and incrimination. And as we have said, in this case compulsion and incrimination are not at issue, leaving only the testimonial element. Testimonial elements of production include (1) the existence of the documents, (2) the accused's possession or control of the documents, and (3) the authenticity of the documents. Hubbell, 530 U.S. at 36.[8]

It bears repeating that the information sought by the State, that which it would require Stahl to provide, is the passcode to Stahl's iPhone—the iPhone that the State had a warrant to search based on probable cause that the phone was used in Stahl's commission of the crime of video voyeurism. The State has not asked Stahl to produce the photographs or videos on the phone.[9] But the fact that the State sought

[8]We note that the contents of Stahl's phone are neither at issue nor privileged. See United States v. Doe, 465 U.S. 605, 612 (1984); In re Boucher, 2009 WL 424718 at *2.

[9]Neither the State nor Stahl addresses the State's request as anything but an act of production. This is likely because relevant—but not determinative—case law addresses the privilege in the context of producing decrypted documents or files, clearly acts of production. See, e.g, Fricosu, 841 F. Supp. 2d at 1235 ("[T]he government seeks a writ . . . requiring Ms. Fricosu to produce the unencrypted contents of the computer."); In re Boucher, 2009 WL 424718 at *1 ("[T]he Government stated that it does not in fact seek the password for the encrypted hard drive, but requires Boucher to

production of the passcode itself and not production of the contents of Stahl's phone does not resolve the issue before us because the State does not contend the court departed from the requirement of law by applying the act-of-production doctrine.

"The difficult question whether a compelled communication is testimonial for purposes of applying the Fifth Amendment often depends on the facts and circumstances of the particular case." Doe, 487 U.S. at 214-15. Here, the trial court rested its determination that producing the passcode would be testimonial exclusively on the concept that production would require "the use of the contents" of Stahl's mind. The phrase "the contents of the accused's mind" has often been repeated in cases discussing the privilege. See, e.g., Hubbell, 530 U.S. at 43; Doe, 487 U.S. at 211; In re Grand Jury, 670 F.3d at 1345; Kirschner, 823 F. Supp. 2d at 669. And although the trial court correctly quoted the Eleventh Circuit's statement in In re Grand Jury, that "[t]he touchstone of whether an act of production is testimonial is whether the government compels the individual to use 'the contents of his own mind' to explicitly or implicitly communicate some statement of fact," 670 F.3d at 1345, the trial court did not consider the law as stated in Hubbell and Doe—that the contents of the accused's mind must be "extensive[ly] use[d]" in creating the response, Hubbell, 530 U.S. at 43, or must "relat[e]

---

produce the contents of his encrypted hard drive in an unencrypted format by opening the drive before the grand jury."); Gelfgatt, 11 N.E.3d at 612 ("The Commonwealth . . . is seeking to compel the defendant to decrypt 'all' of the 'digital storage devices that were seized from him.' "). And it is not entirely clear from the record whether the State wants Stahl to testify to the passcode or to enter it into the phone. Cf. Gelfgatt, 11 N.E.3d at 611. If the former, the State's request could be considered under the traditional analysis of the self-incrimination privilege—that of verbal communications.

him to the offense," Doe, 487 U.S. at 2013.[10] That is, "it is not enough that the compelled communication is sought for its content. The content itself must have testimonial significance." Doe, 487 U.S. at 211 n.10 (emphasis added) (first citing Fisher, 425 U.S. at 408; then citing Gilbert v. California, 388 U.S. 263, 267 (1967); and then citing United States v. Wade, 388 U.S. 218, 222 (1967)).

In this case, the communication was sought only for its content and the content has no other value or significance.[11] By providing the passcode, Stahl would not be acknowledging that the phone contains evidence of video voyeurism. See Doe, 487 U.S. at 215. Moreover, although the passcode would allow the State access to the phone, and therefore to a source of potential evidence, the State has a warrant to search the phone—the source of evidence had already been uncovered. See id. Providing the passcode does not "betray any knowledge [Stahl] may have about the circumstances of the offenses" for which he is charged. See id. at 219 (Stevens, J., dissenting). It does not implicitly "relate a factual assertion or disclose information."

---

[10]Although the phrase "the use of the contents of the accused's mind" has been used in act-of-production cases, we note that the case cited by the Eleventh Circuit for its proposition that the use of the contents of the accused's mind is the touchstone of whether an act of production is testimonial does not so hold. Curcio v. United States, 354 U.S. 118 (1957), provides that there "is a great difference" between compelled production of documents and compelled testimony, specifying that testifying as to the location of documents "requires him to disclose the contents of his own mind." Id. at 127-28.

[11]We recognize that the court in Kirschner reached the opposite conclusion, but because Kirschner provides no facts regarding the crimes or evidence linking Kirschner to the computer and the computer to the crimes, we cannot discuss the case except to say that our reading of the cases relied upon in Kirschner leads to the conclusion that the statement must have value beyond its actual content. We believe the facts here set forth one of the "very few instances in which a verbal statement, either oral or written, will not convey information or assert facts," and therefore would not be testimonial. Cf. Doe, 487 U.S. at 213.

Doe, 487 U.S. at 210, 215. Thus, "compelling a suspect to make a nonfactual statement that facilitates the production of evidence" for which the State has otherwise obtained a warrant based upon evidence independent of the accused's statements linking the accused to the crime does not offend the privilege. See id. at 213 n.11. "If a compelled statement is 'not testimonial and for that reason not protected by the privilege, it cannot become so because it will lead to incriminating evidence.' " Id. at 208-09 n.6 (quoting In re Grand Jury Subpoena, 826 F.2d 1166, 1172 n.2 (2d Cir. 1987) (Newman, J., concurring)). The trial court's reliance solely on the passcode being the contents of Stahl's mind was a departure because the standard requires something more.

That an accused may be "forced to surrender a key to a strongbox containing incriminating documents," but he cannot "be compelled to reveal the combination to his wall safe," Doe, 487 U.S. at 219 (Stevens, J., dissenting), is another often repeated quote. See, e.g., Hubbell, 530 U.S. at 43; Doe, 487 U.S. at 210 n.9; In re Grand Jury, 670 F.3d at 1345; Kirschner, 823 F. Supp. 2d at 669. Despite the many cases referencing the quote, we have found none that provide details of "surrender[ing] a key." We question whether identifying the key which will open the strongbox—such that the key is surrendered—is, in fact, distinct from telling an officer the combination. More importantly, we question the continuing viability of any distinction as technology advances. See Fisher, 425 U.S. at 407 ("Several of Boyd[v. United States, 116 U.S. 616 (1886)]'s express or implicit declarations have not stood the test of time."). In that respect, we are not inclined to believe that the Fifth Amendment should provide greater protection to individuals who passcode protect their iPhones with letter and number

combinations than to individuals who use their fingerprint as the passcode. Compelling an individual to place his finger on the iPhone would not be a protected act; it would be an exhibition of a physical characteristic, the forced production of physical evidence, not unlike being compelled to provide a blood sample or provide a handwriting exemplar. See Hubbell, 530 U.S. at 35 (and cases cited therein); see also Baust, 89 Va. Cir. 267 at *4.[12]

C. Foregone Conclusion

However, even the testimonial communication implicit in the act of production does not rise "to the level of testimony within the protection of the Fifth Amendment" where the State has established, through independent means, the existence, possession, and authenticity of the documents. Fisher, 425 U.S. at 411. That is, by implicitly admitting the existence of the evidence requested and that it is in the accused's possession the accused "adds little or nothing to the sum total of the Government's information"; the information provided is a foregone conclusion. Id. "In

[12]These considerations, we believe, allow for the balance spoken of in Doe and Schmerber, among others. See Doe, 487 U.S. at 213 ("Even if some of the policies underlying the privilege might support petitioner's interpretation of the privilege, 'it is clear that the scope of the privilege does not coincide with the complex of values it helps to protect. Despite the impact upon the inviolability of the human personality, and upon our belief in an adversary system of criminal justice in which the Government must produce the evidence against an accused through its own independent labors, the prosecution is allowed to obtain and use . . . evidence which although compelled is generally speaking not "testimonial" . . . .' " (quoting Marchetti v. United States, 390 U.S. 62, 72 (1968) (Brennan J., concurring))); Schmerber, 384 U.S. at 762-63 ("[T]he privilege has never been given the full scope which the values it helps to protect suggest. History and a long line of authorities in lower courts have consistently limited its protection to situations in which the State seeks to submerge those values by obtaining the evidence against an accused through 'the cruel, simple expedient of compelling it from his own mouth.' ").

essence, under the 'foregone conclusion' exception to the Fifth Amendment privilege, the act of production does not compel a defendant to be a witness against himself." Gelfgatt, 11 N.E.3d at 615.

In order for the foregone conclusion doctrine to apply, the State must show with reasonable particularity that, at the time it sought the act of production, it already knew the evidence sought existed, the evidence was in the possession of the accused, and the evidence was authentic. In re Grand Jury, 670 F.3d at 1344.[13] Although the State need not have "perfect knowledge" of the requested evidence, it "must know, and not merely infer," that the evidence exists, is under the control of defendant, and is authentic. United States v. Greenfield, No. 15-543, 2016 WL 4073250, *6-7 (2d Cir. Aug. 1, 2016). Where the foregone conclusion exception applies, "[t]he question is not of testimony but of surrender." Fisher, 425 U.S. at 411 (quoting In re Harris, 221 U.S. 274, 279 (1911)).

To know whether providing the passcode implies testimony that is a foregone conclusion, the relevant question is whether the State has established that it knows with reasonable particularity that the passcode exists, is within the accused's possession or control, and is authentic. See In re Boucher, 2009 WL 424718 at *3 ("The Government thus knows of the existence and location of the Z drive and its files." (emphasis added)). But see Baust, 89 Va. Cir. 267 ("Contrary to the Commonwealth's assertion, the password is not a foregone conclusion because it is not known outside of

[13]As noted by the Eleventh Circuit, at the time it adopted the "reasonable particularity" standard, the Ninth and D.C. Circuits had also adopted the standard. In re Grand Jury, 670 F.3d at 1344 n.20. The Second Circuit has also adopted the standard. United States v. Greenfield, No. 15-543, 2016 WL 4073250, *6 (2d Cir. Aug. 1, 2016).

Defendant's mind." (emphasis added)). The question is not the State's knowledge of the contents of the phone; the State has not requested the contents of the phone or the photos or videos on Stahl's phone. Cf. In re Grand Jury, 670 F.3d at 1346-47 (concluding that "[n]othing in the record before us reveals that the Government knows whether any files exist and are located on the hard drives" where the Government requested production of the contents of the hard drives).[14] But see Huang, 2015 WL 5611644 at *3 (stating that, where the SEC sought passcodes and not the contents of the smartphones, "the SEC proffers no evidence rising to a 'reasonable particularity' any of the documents it alleges reside in the passcode protected phones." (emphasis added)). The State established that the phone could not be searched without entry of a passcode. A passcode therefore must exist. It also established, with reasonable particularity based upon cellphone carrier records and Stahl's identification of the phone and the corresponding phone number, that the phone was Stahl's and therefore the passcode would be in Stahl's possession. That leaves only authenticity. And as has been seen, the act of production and foregone conclusion doctrines cannot be seamlessly applied to passcodes and decryption keys. If the doctrines are to continue to be applied to passcodes, decryption keys, and the like, we must recognize that the technology is self-authenticating—no other means of authentication may exist. Cf. Greenfield, 2016 WL 4073250 at *8 (recognizing "[i]mplicit authentication" of documents

[14]The Eleventh Circuit explained that the subpoena at issue directed Doe to appear before a grand jury "and produce the unencrypted contents" of hard drives and "any and all containers or folders thereon." In re Grand Jury, 670 F.3d at 1339. The hard drives were seized pursuant to a warrant, which presumably also allowed the Government to search the drives. The focus of the Government's request was the contents of the drives, not the decryption key.

(alteration in original) (quoting United States v. Fox, 721 F.2d 32, 38 (2d Cir. 1983))). If the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic.

V. Conclusion

The trial court departed from the requirements of the law by considering only part of the standard used to determine whether a communication is testimonial and by burdening the State with proving the existence of incriminating content on Stahl's phone when that was not at issue. It further departed by requiring the State to establish existence beyond the reasonable particularity standard. Unquestionably, the State established, with reasonable particularity, its knowledge of the existence of the passcode, Stahl's control or possession of the passcode, and the self-authenticating nature of the passcode.[15] See In re Boucher, 2009 WL 424718 at *3. This is a case of surrender and not testimony.

Petition granted; order quashed.

SALARIO, J., Concurs.
KELLY, J., Concurs in result only.

[15]Given the State's evidence and the fact that it met the standard necessary to obtain a search warrant for Stahl's iPhone, we would be inclined to find that the State had met the reasonable particularity standard for even the contents of Stahl's phone. The State knew Stahl was the individual in the store surveillance video holding an imaging device, which the victim identified as a phone; it knew that the evidence would be a photo or video file; and it knew the evidence would be authentic based upon the store surveillance video. However, nothing about our conclusion prevents Stahl from filing a motion to suppress any evidence found on the phone based on the validity of the warrant. See, e.g., Baust, 89 Va. Cir. 267 ("[T]he contents of the phone, obtained pursuant to a validly executed warrant are only subject to objections raised under the Fourth Amendment, not the Fifth Amendment." (emphasis omitted)).