RECORD IMPOUNDED

NOT FOR PUBLICATION WITHOUT THE
APPROVAL OF THE APPELLATE DIVISION

SUPERIOR COURT OF NEW JERSEY
APPELLATE DIVISION
DOCKET NO. A-0291-17T4

STATE OF NEW JERSEY,

Plaintiff-Respondent,

v.

ROBERT ANDREWS,

Defendant-Appellant.

APPROVED FOR PUBLICATION

November 15, 2018

APPELLATE DIVISION

Argued October 16, 2018 – Decided November 15, 2018

Before Judges Yannotti, Rothstadt and Natali.

On appeal from an interlocutory order of Superior Court of New Jersey, Law Division, Essex County, Indictment No. 16-06-1781.

Charles J. Sciarra argued the cause for appellant (Sciarra & Catrambone, LLC, attorneys; Charles J. Sciarra, of counsel and on the briefs; Deborah Masker Edwards, on the briefs).

Tiffany M. Russo, Special Deputy Attorney General/Acting Assistant Prosecutor, argued the cause for respondent (Theodore N. Stephens II, Acting Essex County Prosecutor, attorney; Tiffany M. Russo, of counsel and on the brief).

Fox Rothschild, LLP, attorneys for amicus curiae Association of Criminal Defense Lawyers of New

Jersey (Matthew S. Adams, Jordan B. Kaplan, Marissa Koblitz Kingman, and Victoria T. Salami, on the brief).

The opinion of the court was delivered by

YANNOTTI, P.J.A.D.

Defendant appeals, on leave granted, from an order of the Law Division, which required defendant to disclose the personal identification numbers and passwords (the passcodes) for his lawfully-seized iPhones. Defendant argues that the compelled disclosure of this information violates his right against self-incrimination under the Fifth Amendment to the United States Constitution, and the protections against self-incrimination afforded under New Jersey law. We reject defendant's arguments and affirm the trial court's order.

I.

We briefly summarize the pertinent facts and procedural history. In May and June 2015, a task force of the Essex County Prosecutor's Office (ECPO) was investigating a suspected narcotics-trafficking network in Newark. During surveillance, law enforcement officers observed Quincy Lowery (Lowery), the target of the investigation, operating a motorcycle and a Jeep, even though his driver's license was suspended at the time. Both vehicles were registered in defendant's name.

In June 2015, the task force obtained a court order, which authorized a wiretap of Lowery's phone and placement of a global positioning system (GPS) device on the Jeep. On June 30, 2015, Lowery was arrested on suspicion of drug trafficking. On the night of his arrest, Lowery gave a formal statement, alleging that an officer in the Essex County Sheriff's Office (ECSO), whom Lowery knew only as "Bolo," had helped him conceal his drug-trafficking activities. Lowery said he had known "Bolo" for about a year through a motorcycle club in which both men were members. From a photograph, Lowery identified defendant as the person named "Bolo."

Lowery claimed defendant assisted him by registering the Jeep and motorcycle in his own name because defendant knew Lowery's license had been suspended. Lowery said defendant warned him about the wiretap and urged him and his co-conspirators to get rid of their phones. According to Lowery, defendant checked the license plate of a vehicle Lowery had suspected of following him and confirmed it was a county-issued vehicle. Defendant also confirmed Lowery's suspicion that a man Lowery saw at a bar was an undercover officer. In addition, defendant suggested that Lowery put his motor vehicle on a lift to check it for a GPS device, and to discard any such device.

Lowery consented to an electronic search of his phone and showed the police a picture of a license plate he had texted to defendant. The investigators later confirmed the license plate belonged to a vehicle the task force had used in a surveillance operation. The cell phone number associated with the name "Bolo" on Lowery's phone corresponds to the number for one of defendant's iPhones. Lowery suggested to investigators that defendant generally offered this assistance either in person or by using the video app FaceTime, and that the text messages the two exchanged were mostly limited to arranging meetings.

On the night Lowery was arrested, the Internal Affairs Department of the ECSO confronted defendant and asked him to surrender his two phones: an iPhone 5s and an iPhone 6 Plus. Defendant turned in the phones but refused to consent to a search of either phone or give a statement. Defendant later requested that the phones be returned to him. The officers denied the request and held the phones pending an application for a search warrant.

In June 2016, an Essex County grand jury returned a six-count indictment charging defendant with second-degree official misconduct, contrary to N.J.S.A. 2C:30-2 (counts one and two); third-degree hindering the apprehension or prosecution of another person, contrary to N.J.S.A. 2C:29-3(a)(2) (counts three and four); and fourth-degree obstruction of the

administration of the law or government function, contrary to N.J.S.A. 2C:29-1 (counts five and six).

In January 2017, the State filed a motion to compel defendant to disclose the passcodes required to unlock defendant's iPhones. In support of its motion, the State submitted call records it had obtained regarding Lowery's phone, which showed that in the thirty days before Lowery's arrest, 187 phone calls had been exchanged between defendant's iPhones and Lowery's mobile devices. However, these records reflected only the number of calls exchanged, and they provided no information about the duration of the calls.

Lowery's phone and call records also revealed a series of text messages with defendant. However, Lowery told investigators that on defendant's advice, he reset his phone about thirty days before his arrest. Therefore, the State could not access any of that data. Because defendant's iPhones were locked, the State could not determine whether defendant's devices contained any of the missing texts between Lowery and defendant or any information about the duration of their calls. The State asserted that the only way to obtain records as to the duration of the calls was through defendant's iPhones since Apple is a "closed end to end system," and defendant's service providers do not have access to Apple's "system."

Defendant opposed the motion, arguing that compelled disclosure of the passcodes would violate his Fifth Amendment right against self-incrimination. He argued that the State was seeking to compel disclosure of statements that are testimonial and potentially incriminating. He further argued that any compelled disclosure would be inconsistent with the privilege against self-incrimination under New Jersey law.

The trial court heard oral argument on the motion, and on May 22, 2017, filed a written opinion in which it concluded that the State's motion should be granted. The court found that the compelled disclosure of the passcodes was not a violation of defendant's constitutional right against self-incrimination. The court also decided that the privilege against self-incrimination under New Jersey's common law, N.J.S.A. 2A:84A-19(b), and N.J.R.E. 503 did not preclude the court from requiring defendant to disclose the information.

The court memorialized its opinion in an order dated May 22, 2017. The order requires defendant to disclose the passcodes, but limited the State's access "to that which is contained within (1) the 'Phone' icon[s] and application[s] on [defendant's] two iPhones and (2) the 'Messages' icon[s] and/or text messaging applications." The order also requires defendant to disclose the passcodes in camera before any disclosure to the State, and directed the State to perform the actual search "in camera, in the presence of

. . . defense counsel and the [c]ourt."

In June 2017, defendant filed a motion seeking leave to appeal the trial court's May 22, 2017 order. In July 2017, we denied the motion. Defendant then filed a motion in the Supreme Court for leave to appeal. The Supreme Court granted the motion and summarily remanded the appeal to this court for consideration on the merits. We later permitted the Association of Criminal Defense Lawyers of New Jersey (ACDL-NJ) to appear as amicus curiae.

II.

Defendant argues that the trial court's order compelling him to disclose the passcodes for the seized phones violates his right against self-incrimination, as provided in the Fifth Amendment to the United States Constitution. We conclude, however, that under the circumstances presented here, the compelled disclosure of the passcodes is not barred by the Fifth Amendment.

The Fifth Amendment to the United States Constitution, which is made applicable to the states through the Fourteenth Amendment, Malloy v. Hogan, 378 U.S. 1, 6 (1964), provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself[.]" U.S. Const. amend. V. "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).

"[T]o be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information," such as an admission that the revealed evidence "exist[s]," is "in [defendant's] possession or control," and is "authentic." Doe v. United States, 487 U.S. 201, 209-10 (1988) (citing United States v. Doe, 465 U.S. 605, 613 & n.11 (1984); Fisher v. United States, 425 U.S. 391-409-10 (1976)). "Only then is a person compelled to be a 'witness' against himself." Id. at 210.

The Fifth Amendment privilege against self-incrimination applies not only to verbal and written communications but also to the production of documents because "[t]he act of produc[tion]" itself may communicate incriminatory statements. Fisher, 425 U.S. at 410. Nevertheless, the "foregone conclusion" principle is an exception to the "act of production" doctrine. See id. at 411.

For the "foregone conclusion" exception to apply, the State must establish with reasonable particularity: (1) knowledge of the existence of the evidence demanded; (2) defendant's possession and control of that evidence; and (3) the authenticity of the evidence. See Hubbell, 530 U.S. at 30, 40-41; Fisher, 425 U.S. at 410-13. Therefore, when an accused implicitly admits the

existence and possession of evidence, the accused has "add[ed] little or nothing to the sum total" of the information the government has, and the information provided is a "foregone conclusion." Fisher, 425 U.S. at 411.

In Doe, the Court held that an order requiring 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 compel a testimonial act for purposes of the Fifth Amendment. Doe, 487 U.S. at 202, 219. The Court found that the defendant's execution of the disclosure form did not convey anything about the existence of any foreign bank account, the defendant's control over any such account, or the authenticity of any records the banks may produce. Id. at 215-16.

Here, as in Doe, the act of disclosing the passcodes to defendant's phones does not convey any implicit factual assertions about the "existence," or "authenticity" of the data on the device. See ibid. Moreover, in its order, the trial court required defendant to disclose the passcodes in camera before they are communicated to the State. The order thus ensures that any incriminating information would not be disclosed. The order also ensures that by providing the passcodes, defendant will not be compelled "to restate, repeat, or affirm the truth of the contents of the" devices. See Fisher, 425 U.S. at 409.

However, by producing the passcode, defendant is making an implicit statement of fact that the iPhone passcodes are within his "possession or control." See Doe, 487 U.S. at 209 (citing Doe, 465 U.S. at 613 & n.11; Fisher, 425 U.S. at 409-10). Defendant is acknowledging he has accessed the phone before, set up password capabilities, and exercised some measure of control over the phone and its contents.

Nevertheless, these testimonial aspects of the passcodes are a "foregone conclusion" because the State has established and defendant has not disputed that he exercised possession, custody, or control over these devices. See Fisher, 425 U.S. at 411. Therefore, the fact that defendant knows the passcodes to these devices "adds little or nothing to the sum total of the Government's information." See ibid.

Furthermore, the State has described with "reasonable particularity" the specific evidence it seeks to compel, which is the passcodes to the phones. Defendant argues the State is unaware of all of the possible contents of defendant's devices. This is immaterial because the order requires defendant to disclose the passcodes, not the contents of the phones unlocked by those passcodes. See Fisher, 425 U.S. at 409.

Our conclusion that the Fifth Amendment privilege does not bar the court from requiring defendant to disclose the passcodes is supported by

United States v. Apple MacPro Computer, 851 F.3d 238 (3d Cir. 2017). In that case, as part of an investigation of the defendant's access to child pornography over the internet, authorities executed a search warrant and seized an Apple iPhone 5s and an Apple Mac Pro computer with two attached external hard drives, which were protected with encryption software. Id. at 242. The police later seized an Apple iPhone 6 Plus, which also was password-protected. Ibid.

The defendant voluntarily provided the authorities the password for the iPhone 5s, but refused to provide passwords that would allow access to the computer or the external hard drives. Ibid. Forensic analysis of the computer revealed that it had been used to visit sites known for child exploitation, and that thousands of files associated with child pornography had been downloaded. Ibid. The downloaded files were not on the computer, but stored on the external hard drives, which were encrypted. Ibid.

The defendant's sister informed the authorities that the defendant had shown her hundreds of images of child pornography on the external hard drives. Id. at 242-43. The defendant provided the password for the iPhone 6 Plus; however, he "did not grant access to an application on the phone which contained additional encrypted information." Id. at 243. The forensic analysis

indicated that the phone's encrypted database contained more than 2000 images and video files. Ibid.

On an application by the federal authorities, the federal district court ordered the defendant to produce his iPhone 6 Plus, Mac Pro computer, and two external hard drives "in a fully unencrypted state." Ibid. The defendant then filed a motion to quash the government's request, arguing that the act of decrypting would violate his Fifth Amendment privilege against self-incrimination. Ibid. A magistrate judge denied the motion. Ibid.

Later, the defendant appeared at the local police department for a forensic examination of the devices. Ibid. He provided the iPhone 6 Plus and the files on the application in a fully unencrypted state. Ibid. He claimed, however, that he could not recall the passwords required to decrypt the hard drives, and he entered several incorrect passwords during the examination. Ibid. Consequently, the federal authorities were unable to view the decrypted contents of the hard drives. Ibid.

On the government's motion, the federal district court held the defendant in contempt, and ordered his incarceration until he complied with the decryption order. Id. at 243-44. Defendant appealed and argued the order violated his right against self-incrimination. Id. at 244. The Third Circuit held that although the Fifth Amendment may be implicated by the compelled

decryption of the devices, "any testimonial aspects of that production were a foregone conclusion." Id. at 248.

The court found that the record supported the conclusion that the production of the decrypted devices "added little or nothing to the information" the government already had obtained. Ibid. The court noted that: the government had custody of the devices; the government knew the defendant owned, possessed, and had accessed the devices before they were seized; and the government had established that the devices had images that met the definition of child pornography. Ibid.

A similar conclusion was reached in Commonwealth v. Gelfgatt, 11 N.E.3d. 605 (Mass. 2014). In that case, the defendant was charged with various offenses, which were allegedly part of a mortgage-fraud scheme. Id. at 608. The trial court denied the government's motion to compel the defendant to enter his password for encryption software he had placed on various digital media storage devices, which the government had seized as part of its investigation, finding that compelled disclosure of the information would violate the defendant's right against self-incrimination. Id. at 611-12. The Supreme Judicial Court of Massachusetts reversed. Id. at 617.

The court stated that although the Fifth Amendment typically applies to oral and written testimonial statements, "the act of producing evidence . . .

may have communicative aspects." Id. at 613 (quoting Fisher, 425 U.S. at 410). Whether an act of producing evidence is testimonial for Fifth Amendment purposes "depend[s] on the fact and circumstances of [each] particular case[]." Ibid. (alterations in original) (quoting Fisher, 425 U.S. at 410).

The court stated that defendant's act of entering the encryption key "would appear, at first blush, to be a testimonial communication that triggers Fifth Amendment protection." Id. at 614. The defendant "would be acknowledging that he ha[d] ownership and control of the computers and their contents." Ibid. The court held, however, that the Fifth Amendment did not bar the government from compelling the defendant to produce the information because the "foregone conclusion" exception applied. Id. at 615.

The court observed that by entering the encryption key, the defendant would be conveying facts as to "his ownership and control of the computers and their contents, knowledge of the fact of encryption, and knowledge of the encryption key." Ibid. Because the government already knew these facts, their disclosure was a "foregone conclusion." Ibid. The court held that the defendant's rights under the Fifth Amendment were not violated "because the defendant is only telling the government what it already knows." Id. at 615-16.

We are convinced that the decisions in Apple MacPro Computer and Gelfgatt provide persuasive authority for the conclusion that defendant's Fifth Amendment right against self-incrimination is not violated by requiring him to disclose the passcodes for his iPhones, which the State lawfully possessed. The act of producing the passcodes has testimonial aspects because defendant is acknowledging ownership, possession, and control of the devices. He is also acknowledging he has the ability to access the contents of the phone. However, by producing the passcodes, defendant is not implicitly conveying any information the State does not already possess. Defendant is not telling the government something it does not already know. Therefore, the implicit facts conveyed by the act of producing the passcodes is a "foregone conclusion" and compelled disclosure of the passcodes does not violate defendant's Fifth Amendment right against self-incrimination.[1]

[1] Other courts have reached similar conclusions and also support our decision. See, e.g., United States v. Fricosu, 841 F. Supp. 2d 1232, 1236-37 (E.D. Mich. 2010) (holding that the Fifth Amendment did not bar the subpoenaed decryption of the defendant's laptop where the defendant admitted to possession of the computer and federal agents were also aware "of the existence and location of the computer's files"); State v. Stahl, 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016) (concluding that defendant's act of providing the password to his iPhone pursuant to a search warrant was not testimonial where the State knew there was a password and that the defendant possessed the password); Commonwealth v. Davis, 176 A.3d 869, 876 (Pa. Super. Ct. 2017) (holding that the defendant's act of providing the password to his computer was not testimonial where the Commonwealth had already established the (continued)

We recognize that the contents of the phone may contain evidence that ties defendant to the offenses for which he has been charged. However, "[i]f 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.'" Doe, 487 U.S. at 208-09 n.6 (quoting In re Grand Jury Subpoena, 826 F.2d 1166, 1172 n.2 (2d Cir. 1987) (Newman, J., concurring)).

In arguing that compelled disclosure of the passcodes violates his Fifth Amendment right against self-incrimination, defendant relies on In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012). In that case, the defendant was ordered to appear before a federal grand jury and produce unencrypted contents of hard drives on his computers, as well as external hard drives. Id. at 1337.

The defendant refused to comply, relying upon his Fifth Amendment right against self-incrimination. Ibid. The government agreed to provide the defendant with immunity for the act of production of the unencrypted drives, but not for the derivative use of their contents. Id. at 1337-38. The defendant refused to decrypt the hard drives, and the federal district court held him in

---

(continued)
computer was password-protected, the defendant was the only user who knew the password, the "technology is self-authenticating," and there was a "high probability" that incriminating material would be discovered on the defendant's device).

contempt. Id. at 1338. The defendant appealed and the Eleventh Circuit reversed. Id. at 1338-39.

The court noted that in Hubbell, a federal grand jury had issued a subpoena, which required the defendant "to produce eleven categories of documents." Id. at 1344 (citing Hubbell, 530 U.S. at 30-31). The court stated that in Hubbell, the Court had determined that the act of production was sufficiently testimonial to trigger the Fifth Amendment protection against self-incrimination, and the facts implicitly conveyed by the act of production were not a "foregone conclusion." Ibid. (citing Hubbell, 530 U.S. at 44-45). The court stated that, "The touchtone 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." Id. at 1345 (quoting Curcio v. United States, 354 U.S. 118, 128 (1957)).

The court determined that "the decryption and production of the hard drives would require the" defendant to use the contents of his mind. Id. at 1346. This "would be tantamount to testimony by [the defendant] of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; and his capability to decrypt the files." Ibid. The court also rejected the contention that the facts conveyed by the production were a "foregone

conclusion." Id. at 1346-47. The court stated the government did not know whether there was data on the decrypted records. Id. at 1347. The drives could contain as many as twenty million files and the government had not shown that these files could be useful. Ibid.

Here, defendant's reliance upon In re Grand Jury Subpoena is misplaced. In that case, the court found that requiring the defendant to provide the decrypted records was testimonial and the government had not shown that the facts conveyed by the act of production were a "foregone conclusion." Id. at 1346-47. In this case, however, defendant has been ordered to produce the passcodes and the testimonial aspects of that act pertain to the ownership, control, use, and ability to access the phones. The State has shown it has prior knowledge of those facts, and their disclosure is a "foregone conclusion."

Defendant also relies upon United States v. Kirschner, 823 F. Supp. 2d 665 (E.D. Mich. 2010). In that case, the defendant was charged with receiving child pornography by computer. Id. at 666. The government issued a subpoena to the defendant, which required that he appear before the grand jury and provide all passwords used or associated with the subject computer and any files. Ibid. The court found that the production of the computer passwords was testimonial because the government was "seeking testimony from the [d]efendant" which required "him to divulge through his mental

processes his password[.]" Id. at 669. The court stated that the matter did not involve the production of specific documents, but rather the production of "specific testimony asserting a fact." Ibid.

However, defendant's reliance upon Kirschner is unavailing. In that case, the court did not address the question of whether the government already was in possession of the facts implicitly conveyed by the act of producing the passwords. As we have explained, in this case, the State has established all of the elements required for application of the "foregone conclusion" principle.[2]

We note that in its brief, amicus curiae argues that electronically-stored information should be subjected to an enhanced degree of scrutiny because such data raises issues of authenticity. The parties to this appeal have not raised this issue. Therefore, we will not address it. See State v. J.R., 227 N.J. 393, 421 (2017) (declining to "consider arguments that have not been asserted by a party, and are raised for the first time by an amicus curiae").

---

[2] Defendant also relies on In re Search Warrant Application, 279 F. Supp. 3d 800, 806 (N.D. Ill. 2017), where the court held that disclosure of a passcode was testimonial; however, the court did not address the "foregone conclusion" principle. In addition, in Commonwealth v. Baust, 89 Va. Cir. 267, 271 (Cir. Ct. 2014), the court held that a "password is not a foregone conclusion because it is not known outside of [the defendant's] mind." The reasoning of the courts in Apple MacPro Computer, Gelfgatt, and the cases discussed previously is more persuasive.

We therefore conclude that the trial court correctly found that compelled disclosure of defendant's passcodes does not violate defendant's Fifth Amendment privilege against self-incrimination.

III.

Defendant also argues that compelled disclosure of the passcodes would violate the privilege against self-incrimination under New Jersey law. He cites the common law, as well as N.J.S.A. 2A:84A-19 and N.J.R.E. 503.

A. Common-law Privilege

The New Jersey Constitution does not contain a privilege against self-incrimination. Even so, New Jersey has long recognized the privilege under the common law. See, e.g., Fries v. Brugler, 12 N.J.L. 79, 81 (Sup. Ct. 1830) (noting that "the general rule is, that a witness cannot be called upon to impute to himself a crime or to bring a reproach upon himself[.]"). Our Supreme Court has held that, in general, the "state-law privilege against self-incrimination offers broader protection than its federal counterpart." State v. Muhammad, 182 N.J. 551, 568 (2005) (citing State v. Strong, 110 N.J. 583, 595 (1988)).

"Central to our state common-law conception of the privilege against self-incrimination is the notion of personal privacy. . . ." In re Grand Jury Proceedings of Guarino, 104 N.J. 218, 230 (1986). In Guarino, the Court

equated the personal privacy doctrine with a "respect for the inviolability of the human personality and of the right of each individual 'to a private enclave where he may lead a private life.'" Id. at 231 (quoting Murphy v. Waterfront Comm'n of N.Y. Harbor, 378 U.S. 52, 55 (1964)).

"To determine whether the evidence sought by the government lies within that sphere of personal privacy a court must look to the 'nature of the evidence.'" Id. at 231-32 (citing Couch v. United States, 409 U.S. 322, 350 (1973) (Marshall, J., dissenting)). The court must decide whether the "contents" of the compelled disclosures "contain the requisite element of privacy or confidentiality" such that they fall within a "special zone of privacy." See id. at 232 (quoting Bellis v. United States, 417 U.S. 85, 92 (1974)).

In this case, defendant argues that cell phones are "known to contain extremely personal information," and can be "used as a personal diary, recorder of personal images and videos, personal address book, and research device." Defendant therefore argues that cell phone passcodes should be deemed to fall within a "special zone of privacy" or confidentiality. We cannot agree.

Applying the privilege against self-incrimination to cell phone passcodes would essentially preclude the State from obtaining the contents of any

passcode-restricted device as part of a criminal investigation. This would be so even when the State has obtained a warrant, issued on a showing of probable cause, for the contents of the device, and the State has established, as it has in this case, the basis for applying the "foregone conclusion" doctrine.

We see no basis for affording, in the particular circumstances presented by this case, greater protections against self-incrimination than those provided by the Fifth Amendment. We therefore hold that where, as here, the State has established the elements for application of the "foregone conclusion" doctrine, New Jersey's common law privilege against self-incrimination does not bar compelled disclosure of passcodes for defendant's phones.

B. Statutory and Evidentiary Privilege

New Jersey also has enacted a statute and evidence rule that, in identical language, provide that "every natural person has a right to refuse to disclose in an action or to a police officer or other official any matter that will incriminate him or expose him to a penalty," unless one of four exceptions applies. N.J.S.A. 2A:84A-19; N.J.R.E. 503. Under one of the exceptions to the privilege:

> (b) [N]o person has the privilege to refuse to obey an order made by a court to produce for use as evidence or otherwise a document, chattel or other thing under his control if some other person or a corporation or other association has a superior right to the possession of the thing ordered to be produced[.]

[N.J.S.A. 2A:84A-19(b); N.J.R.E. 503(b).]

As we have determined, compelled disclosure of defendant's passcodes is not a violation of his right against self-incrimination under the Fifth Amendment or our common law. Because defendant is not conveying any important facts that the State does not already possess, he is not being required to disclose any "matter" that would incriminate him or expose him to a penalty. Furthermore, the State has a "superior right of possession" to defendant's passcodes because the trial court has issued two search warrants for defendant's iPhones, which allow the State to obtain the passcodes that may be necessary to access information on the phones.

Defendant has not argued that the warrants are unlawful. He argues, however, that under New Jersey law, he cannot be required to produce any evidence that may be used against him. In support of this argument, he relies on In re Addonizio, 53 N.J. 107 (1968), and State v. Kelsey, 429 N.J. Super. 449 (App. Div. 2013). Both cases are distinguishable.

In Addonizio, the defendant was appealing the denial of a motion to set aside subpoenas that, similar to those in Hubbell, 530 U.S. at 31, had directed him to produce ten categories of financial documents. See Addonizio, 53 N.J. at 113. Addonizio involved no warrant of any kind, and would have required defendant to make extensive use of the contents of his mind in order to

comply. See Hubbell, 530 U.S. at 43. As we have determined, however, disclosure of cell phone passcodes does not involve the production of testimonial evidence, and the act of producing the passcodes only coveys implicit facts that the government already knows.

Moreover, in Kelsey, the defendant challenged an order compelling him to produce a flashlight that he allegedly used as a weapon in a brawl. Kelsey, 429 N.J. Super. at 450. The police had obtained a warrant to search defendant's vehicle, but when they did not find what they were searching for, they sought an order for defendant to produce the item, which "may or may not" have been in defendant's possession. Id. at 450, 452 (emphasis added).

Here, the State has evidence indicating that defendant used the iPhones before surrendering them. The State knows defendant possesses the passcodes, and has obtained search warrants issued upon a showing of probable cause that the devices contain evidence of criminality. We therefore conclude the search warrants give the State a superior right to possession of the passcodes; therefore, the exception in N.J.S.A. 2A:84A-19(b) and N.J.R.E. 503(b) applies.

Affirmed.