2022 IL App (4th) 190329-U

NO. 4-19-0329

FILED
January 18, 2022
Carla Bender
4th District Appellate
Court, IL

IN THE APPELLATE COURT

OF ILLINOIS

FOURTH DISTRICT

THE PEOPLE OF THE STATE OF ILLINOIS,	)	Appeal from
Plaintiff-Appellant,	)	Circuit Court of
v.	)	Piatt County
CHRISTOPHER A. HOLLINGSWORTH,	)	No. 19CF8
Defendant-Appellee.	)	
	)	Honorable
	)	Jeremy J. Richey,
	)	Judge Presiding.

JUSTICE HOLDER WHITE delivered the judgment of the court.
Justice Turner concurred in the judgment.
Justice Cavanagh specially concurred.

ORDER

¶ 1 *Held*: The appellate court reversed, concluding the trial court erred by denying the State's motion to compel defendant to produce the passcode to his cell phone where the foregone conclusion doctrine applies.

¶ 2 In January 2019, the State charged defendant, Christopher A. Hollingsworth, with criminal drug conspiracy (720 ILCS 570/405.1(a) (West 2018)), two counts of unlawful delivery of a controlled substance (720 ILCS 570/401(a)(2)(A) (West 2018)), and unlawful delivery of a controlled substance within 500 feet of school property (720 ILCS 570/407(b)(1) (West 2018)). Following defendant's arrest, the police found an Apple iPhone in his possession. Police obtained a search warrant requiring defendant to unlock the phone by either applying his fingerprint to the screen or revealing the passcode. Defendant refused to unlock the phone. In March 2019, the State filed a motion to compel, asking the court to compel defendant "to

alternatively unlock the phone and provide it to law enforcement in an unlocked state or provide the State with the passcode with which the phone can be unlocked." The trial court denied the motion to compel.

¶ 3 On appeal, the State asks us to determine whether compelling defendant to unlock his phone, the subject of a search warrant, violates his fifth amendment right against self-incrimination. According to the State, the trial court erred by denying its motion to compel defendant to produce the passcode for his cell phone. For the following reasons, we reverse the judgment of the trial court.

¶ 4 I. BACKGROUND

¶ 5 In January 2019, the State charged defendant with criminal drug conspiracy (720 ILCS 570/405.1(a) (West 2018)), two counts of unlawful delivery of a controlled substance (720 ILCS 570/401(a)(2)(A) (West 2018)), and unlawful delivery of a controlled substance within 500 feet of school property (720 ILCS 570/407(b)(1) (West 2018)).

¶ 6 A. Preliminary Hearing

¶ 7 On February 11, 2019, the trial court held a preliminary hearing. John D. Russell, a sergeant with the Piatt County Sheriff's Office, testified that, in the fall of 2018 and January 2019, he was assigned to a task force investigating a person later identified as defendant. The task force began investigating drug trafficking that, according to numerous complaints, was happening in a house across the street from an elementary school. On November 8 and 19, 2018, and on January 10 and 16, 2019, the police conducted four controlled purchases of cocaine in the house.

¶ 8 According to Russell, defendant did not live in the house and he did not deliver cocaine directly to the confidential informants or receive money directly from the confidential

informants. Each controlled buy was conducted through the resident of the house, James Warren, just after defendant arrived at the house. During the fourth controlled buy, an undercover officer went to the residence and provided the man at the house with $1500 in marked currency. The man who lived in the house told the undercover officer he was waiting for his "guy" to bring the cocaine. Defendant arrived at the house and the man at the residence got into defendant's vehicle and drove around the block with him. Defendant returned to the house and the man got out of the vehicle, went inside the house, and gave the undercover officer 28 grams of cocaine.

¶ 9 When defendant left the house after the fourth controlled buy, police officers followed him to a bar and arrested him. Police found, on defendant's person, an Apple iPhone but none of the marked currency. Video footage from the bar's security system showed defendant handing the bartender an item. Initially, the bartender denied involvement. Police officers secured a search warrant for the bartender's residence where they recovered all $1500 of the marked currency used in the fourth controlled buy. The bartender admitted defendant handed her the currency just before officers came into contact with defendant.

¶ 10 B. Search Warrants

¶ 11 On January 22, 2019, the trial court issued a warrant to search the phone found on defendant's person at the time of his arrest. Russell filed an affidavit in support of the request for the January 22, 2019, search warrant. The affidavit identified an Apple iPhone in a blue case with a protective purple shell found on defendant at the time of his arrest. The warrant ordered the owner of the phone found on defendant to provide any and all security codes to unlock the phone and make available any data retrieved.

¶ 12 Russell sought a second search warrant to search the phone and submitted an affidavit in support. Russell stated he took the previous search warrant to the Piatt County jail and presented it to defendant, but defendant refused to provide the access code to unlock the phone. The affidavit explained why, in Russell's view, there was probable cause to believe the passcode-protected phone contained evidence of a crime. Russell averred he had been a police officer for 27 years and, in his experience, cocaine dealers frequently possessed or had access to cell phones, which they used to "discuss their activities, photograph the progress, [and] assist them in their activities." Cell phones used by cocaine dealers often were "repositories of information relating to those [drug-trafficking] activities, including but not limited to, contact lists, e-mail, text messages, and direct messages." Warren was observed communicating with defendant by cell phone, and just before being arrested, defendant received two phone calls.

¶ 13 Russell took the iPhone found on defendant's person to Detective David Dailey with the Decatur Police Department. The affidavit continued as follows:

> "Detective Dailey is certified as a forensic expert concerning cellular telephones and has testified many times in State court proceedings concerning his findings following cell phone analysis. Detective Dailey suggests that, because the Hollingsworth cell phone was powered down at the time of seizure, the forensic tools available to him cannot access all the data in the cell phone. It appears that the Hollingsworth iPhone has a numeric display, which would accept a passcode prior to entering the storage points on the cell phone. Without the passcode, some data can be

> recovered from the cell phone. However, the data requested in the search warrant cannot be accessed without the code."

The affidavit stated defendant's fingerprint, numeric code, or swipe code were necessary for a complete extraction of data from the phone.

¶ 14 On February 13, 2019, the trial court granted Russell's application for a second search warrant. The second search warrant identified the items or objects to be searched and subject to examination and seizure as follows: "A fingerprint of [defendant] applied to Apple iPhone, or the Numeric Code, and/or Swipe Code from [defendant] to open the password-protected iPhone found on his person who is currently located in the Piatt County Jail."

¶ 15 C. State's Motion to Compel

¶ 16 On March 29, 2019, the State filed a document titled "Motion to Compel." In its motion, the State alleged that defendant, in defiance of the search warrants, still refused to reveal the passcode to the Apple iPhone. Dailey, who was trained in the use of extraction software, examined the phone and determined that "attempts to recover the data[,] without *** the passcode[,] would be severely restricted with, in his experience, no access to text messages or chat sessions." The motion asked the trial court to "compel the defendant to alternatively unlock the phone and provide it to law enforcement in an unlocked state or provide the State with the passcode with which phone can be unlocked."

¶ 17 In a memorandum in support of its motion, the State acknowledged that in *People v. Spicer*, 2019 IL App (3d) 170814, ¶ 23, the appellate court held: "[R]equiring [the defendant] to provide his passcode implicates the fifth amendment right against self-incrimination[,] and the trial court did not err in denying the State's motion to compel." Nevertheless, in light of other

case law, including decisions by the United State Supreme Court, the State respectfully suggested that this holding in *Spicer* is mistaken.

¶ 18 In April 2019, the trial court denied the State's motion to compel based on *Spicer*. In a certificate of impairment, the State represented that "the order in the instant case substantially impairs the ability of the People to proceed in the instant case." The State filed a notice of appeal, specifying it was appealing the trial court's order denying the motion to compel defendant to provide the passcode to his phone.

¶ 19 This appeal followed.

¶ 20 II. ANALYSIS

¶ 21 On appeal, the State asks us to determine whether compelling defendant to unlock his phone, the subject of a search warrant, violates his fifth amendment right against self-incrimination. According to the State, the trial court erred by denying its motion to compel defendant to produce the passcode for his cell phone.

¶ 22 A. Subject-Matter Jurisdiction

¶ 23 Initially, defendant argues we lack jurisdiction to hear this matter. We review *de novo* jurisdictional issues. *People v. Abdullah*, 2019 IL 123492, ¶ 18, 160 N.E.3d 833. Defendant asserts the trial court's order denying the State's motion to compel cannot be characterized as any of the types of orders listed in Illinois Supreme Court Rule 604(a) (eff. July 1, 2017). Illinois Supreme Court Rule 604(a)(1) (eff. July 1, 2017), provides as follows: "In criminal cases the State may appeal only from an order or judgment the substantive effect of which results in dismissing a charge for any of the grounds enumerated in section 114-1 of the Code of Criminal Procedure of 1963 [(725 ILCS 5/114-1 (West 2018))]; arresting judgment

because of a defective indictment, information[,] or complaint; quashing an arrest or search warrant; or suppressing evidence."

¶ 24 Defendant argues the trial court's order did not effectively suppress any evidence or effectively dismiss any charges. Specifically, defendant asserts the court's order did not suppress any evidence or preclude the State from admitting evidence at trial because the State does not know what evidence is on the cell phone. According to defendant, there may or may not be evidence on the cell phone, but the order denying the motion to compel defendant to unlock the phone did not suppress any actual evidence. Nor did the court's order prevent the State from presenting any digital information found on the phone, it merely meant defendant did not have to facilitate the State's access to that information. Defendant further asserts the order did not dismiss any charges against the defendant.

¶ 25 In response, the State argues that "[w]hen a warrant has been issued allowing a search of a defendant's phone, an order denying a motion to compel the defendant to decrypt the phone is like an order suppressing evidence." The State further argues Rule 604(a) is written broadly so as to apply not only to direct suppressions but also to indirectly resulting suppressions: "an order or judgment *the substantive effect of which results in* *** suppressing evidence." (Emphasis added.) Ill. S. Ct. R. 604(a)(1) (eff. July 1, 2017). According to the State, the court's denial of the motion to compel substantively resulted in suppressing the contents of the phone.

¶ 26 In *Spicer*, 2019 IL App (3d) 170814, ¶¶ 10-12, the State made essentially the same jurisdictional argument. There, the police obtained a warrant to search the defendant's cell phone, but the phone was passcode-protected. *Id.* ¶ 4. The defendant refused to reveal the passcode, invoking his fifth amendment right against self-incrimination. *Id.* The State moved

for an order compelling the defendant to reveal the passcode, and the trial court denied the motion. *Id.* ¶¶ 1, 7. The State filed a certificate of impairment and appealed. *Id.* On the question of whether the appellate court had subject-matter jurisdiction, the appellate court rejected defendant's claim and allowed the State's appeal pursuant to Rule 604(a)(1).

¶ 27 Here, the trial court's denial of the State's motion to compel was effectively a suppression order. Although the denial of the motion did not directly suppress specific evidence, it is likely the phone contains incriminating evidence, and the denial prohibited the State from accessing that evidence and presenting it to a jury. Thus, we hold we have subject-matter jurisdiction based on the effective or resulting suppression of evidence. See Ill. S. Ct. R. 604(a)(1) (eff. July 1, 2017); see also *Spicer*, 2019 IL App (3d) 170814, ¶ 12.

¶ 28 We also find we have jurisdiction because denying the motion to compel effectively quashed a search warrant. Rule 604(a) provides: "In criminal cases the State may appeal only from an order or judgment the substantive effect of which results in *** quashing an arrest or search warrant." Ill. S. Ct. R. 604(a)(1) (eff. July 1, 2017). To "quash" a search warrant is "[t]o annul or make void; to terminate." Black's Law Dictionary (8th ed. 2004). The denial of the motion to compel had the effect of nullifying or making void the search warrant of February 13, 2019. That search warrant required defendant to unlock the phone, and defendant refused. The State filed a motion to compel him to obey the search warrant by either unlocking the phone himself or revealing the passcode. The trial court denied the motion, thereby signifying that defendant did not have to comply with the February 13, 2019, search warrant. In substance, the ruling quashed or retracted the search warrant. Thus, we also find we have subject-matter jurisdiction on that basis. We now turn to the question at hand.

¶ 29 B. The Fifth Amendment and Compelled Decryption

¶ 30 Pursuant to the fifth amendment, a person cannot be compelled to testify against himself in a criminal case. U.S. Const., amend. V. Compelling a defendant to make a testimonial communication that incriminates him implicates the fifth amendment. *Spicer*, 2019 IL App (3d) 170814, ¶ 14 (citing *Fisher v. United States*, 425 U.S. 391, 408 (1976)). A communication violates the fifth amendment when the communication is testimonial, incriminating, and compelled. *Id.* An act of production is only testimonial when the government compels the defendant "to make extensive use of 'the contents of his own mind.' " *United States v. Hubbell*, 530 U.S. 27, 43 (2000) (quoting *Curcio v. United States*, 354 U.S. 118, 128 (1957)).

¶ 31 The State argues the compelled production of defendant's passcode is not testimonial because it does not require the "extensive use" of his mind. The State also argues compelling defendant to unlock the phone with his fingerprint or by entering his passcode and providing the unlocked phone to the police does not implicate the fifth amendment privilege because it is neither a testimonial communication nor incriminating. Finally, the State asserts that, even if the compelled production of the phone's passcode or the physical act of unlocking the phone implicates defendant's fifth amendment rights, the foregone conclusion doctrine applies because the State showed with reasonable particularity the contents of the phone.

¶ 32 Defendant argues the fifth amendment privilege against self-incrimination prevents compelling him to unlock a device where decrypting a device is testimonial in nature and not merely a physical act. Finally, defendant argues the foregone conclusion doctrine does not apply where the State has no knowledge of the digital content stored on the device. Although both parties raise arguments regarding whether the State has knowledge of the digital content stored on the device, in analyzing the applicability of the foregone conclusion doctrine, we focus on the passcode rather than the phone's content.

¶ 33 Under the facts in this case, we find determining whether the foregone conclusion doctrine applies dispositive. Specifically, if the foregone conclusion doctrine applies, the testimonial communication implicit in the act of production does not rise "to the level of testimony within the protection of the Fifth Amendment." *Fisher*, 425 U.S. at 411. Thus, we analyze whether the foregone conclusion doctrine applies to requiring defendant to provide the passcode needed to unlock the cell phone. As explained below, we conclude the foregone conclusion doctrine does apply, meaning the trial court improperly denied the State's motion to compel defendant to provide the passcode for the phone.

¶ 34 Under the foregone conclusion doctrine, "the government must establish its knowledge of (1) the existence of the evidence demanded; (2) the possession or control of that evidence by the defendant; and (3) the authenticity of the evidence." *Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 614 (Mass. 2014). Although the Supreme Court has applied the forgone conclusion doctrine only in the context of producing documents, several courts have considered whether the doctrine applies to compelled decryption or compelled passcode production. See *State v. Andrews*, 234 A.3d 1254, 1269-73 (N.J. 2020) (discussing cases in which the applicability of the foregone conclusion doctrine in the context of compelled decryption or the compelled production of a passcode had divergent results). Some courts have concluded the government must prove with reasonable particularity that the contents of the phone are a foregone conclusion. *Spicer*, 2019 IL App (3d) 170814, ¶ 21. In *Spicer*, the appellate court concluded "what the State actually needed to establish with reasonable particularity was the contents of the phone," and not merely the passcode itself. *Id.*

¶ 35 On the other hand, some courts have concluded that, in determining whether the foregone conclusion doctrine applies, the focus is on the passcode and not the contents of the

phone. See, *e.g.*, *State v. Stahl*, 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016) ("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." (Emphasis in original.)); *State v. Johnson*, 576 S.W.3d 205, 227 (Mo. Ct. App. 2019) ("The focus of the foregone conclusion [doctrine] is the extent of the State's knowledge of the existence of the facts conveyed through the compelled act of production. *** The facts conveyed through [the defendant's] act of producing the passcode were the existence of the passcode, his possession and control of the phone's passcode, and the passcode's authenticity."); *Andrews*, 234 A.3d at 1274.

¶ 36 As noted, the *Spicer* court concluded the focus should be on the contents of the phone and not the passcode itself. We disagree. Initially, we look to what the motion to compel seeks to require defendant to do. Pursuant to the motion to compel, the State seeks to require defendant to produce the passcode—not the information contained on the phone. Absent in the motion to compel is any request related to producing the phone's contents. A judicially vetted and authorized search warrant already entitles the State to certain information it believes the phone contains. Focusing on the phone's contents when considering the foregone conclusion doctrine improperly disregards the fact the State has already made, by obtaining judicial authorization to search the phone, the necessary showing to comport with protections provided by the fourth amendment. When we determine whether the foregone conclusion doctrine applies, we are asking whether it applies in the context of requiring defendant to provide the passcode to unlock the phone. Thus, in reaching our decision, we decline to consider what may be found on the phone once it is opened.

¶ 37 In order to apply the foregone conclusion doctrine, the State must show the passcode's existence, possession, and authentication are foregone conclusions. The State demonstrated that a passcode for the phone existed through Russell's averment that Detective Dailey concluded access to the data on the phone required a passcode. Russell's affidavit in support of the January 22, 2019, and February 13, 2019, search warrants identified an Apple iPhone in a blue case with a protective purple shell found on defendant at the time of his arrest. The affidavit in support of the February 13, 2019, search warrant averred Warren was observed communicating with defendant by cell phone, and just before being arrested, defendant received two phone calls. Therefore, the State has demonstrated with reasonable particularity that a passcode exists and defendant knows the passcode. See *Andrews*, 234 A.3d at 1275 (stating the record established the defendant's knowledge of the passcode where the phones were found in the defendant's possession and he owned and operated the phones).

¶ 38 Finally, we turn to whether the passcode was authentic. In *Spicer*, the appellate court concluded the State could never successfully use the foregone conclusion doctrine because it could not show the passcode was authentic until after it was used to decrypt the phone. This position would prevent the State from availing itself of the foregone conclusion doctrine in every instance unless it had obtained a passcode by some other means—which would obviate the need for a motion to compel a defendant to produce a passcode. Moreover,

> "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.

> [Citation.] If the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic." *Stahl*, 206 So. 3d at 136.

When we consider the traditional meaning of self-authentication as it relates to admitting evidence in judicial proceedings, experience teaches such documents are deemed admissible without offering additional proof of authenticity because the document has already been authenticated by some other means. Absent entry of a valid passcode, the phone will not open, and the evidence on the phone would not become available. Thus, there is no danger an invalid or unauthentic passcode will be able to open the device. By actually opening the device, the password self-authenticates, meaning the fact that the passcode opens the phone validates the passcode's authenticity. Requiring the State to somehow determine the passcode by some other means does nothing to ensure the authenticity of the passcode. Just as important, allowing defendant to withhold the passcode provides defendant protection to which he is not entitled where there is an unchallenged search warrant for certain content reasonably believed to be on the phone. Thus, we conclude the passcode is self-authenticated by providing access to the cell phone's contents. See *Andrews*, 234 A.3d at 1275; *Gelfgatt*, 11 N.E.3d at 615 n.14.

¶ 39 The State's demonstration of the passcode's existence, defendant's previous possession and operation of the phone, and the self-authenticating nature of the passcode render the issue here one of surrender, not testimony. Ultimately, the password's existence is a foregone conclusion. Thus, the foregone conclusion doctrine applies. For the foregoing reasons, we conclude the trial court erred by denying the State's motion to compel defendant to produce the passcode for his cell phone. As a final matter, we note the special concurrence's citation to *People v. Sneed*, 2021 IL App (4th) 210180, ¶ 63. We observe that *Sneed*'s discussion, analysis,

and holding pertaining to the foregone conclusion doctrine are entirely consistent with what we have here expressed in the majority order. Accordingly, we reverse the judgment of the trial court and remand for further proceedings.

¶ 40 III. CONCLUSION

¶ 41 For the reasons stated, we reverse the trial court's judgment and remand for further proceedings.

¶ 42 Reversed and remanded.

¶ 43 JUSTICE CAVANAGH, specially concurring:

¶ 44 I agree that we should reverse the circuit court's judgment, but my reason for reversal would be that the fifth amendment is inapplicable. The fifth amendment is inapplicable because, as the Fourth District recently held in *Sneed*, 2021 IL App (4th) 210180, ¶ 63, requiring a person to unlock a phone without requiring the person to disclose the passcode does not compel any testimonial communication. If the fifth amendment is inapplicable, there is no occasion to apply the foregone conclusion doctrine, which is an exception to the fifth amendment (*id.* ¶ 19).