

2021 IL App (4th) 210180

NO. 4-21-0180

IN THE APPELLATE COURT

OF ILLINOIS

FOURTH DISTRICT

FILED

November 18, 2021

Carla Bender

4th District Appellate

Court, IL

THE PEOPLE OF THE STATE OF ILLINOIS,)	Appeal from the
Plaintiff-Appellant,)	Circuit Court of
v.)	De Witt County
KEIRON K. SNEED,)	No. 21CF13.
Defendant-Appellee.)	
)	Honorable
)	Karle E. Koritz,
)	Judge Presiding.

JUSTICE STEIGMANN delivered the judgment of the court, with opinion.

Justices DeArmond and Turner concurred in the judgment and opinion.

OPINION

¶ 1 In February 2021, the State charged defendant, Keiron K. Sneed, with two counts of forgery (720 ILCS 5/17-3(a)(1) (West 2020)). The police later sought and obtained a search warrant for defendant’s cell phone but were unable to execute the search because the cell phone was passcode-protected and defendant declined to provide the passcode. The State filed a “Motion to Compel Production of Cellular Phone Passcode,” but the trial court denied that motion. The court ruled that the fifth amendment privilege against self-incrimination prevented defendant from being compelled to provide the passcode to his cell phone.

¶ 2 The State appeals, arguing two reasons why the trial court erred by concluding the fifth amendment protected defendant from being compelled to provide access to his lawfully seized cell phone: (1) compelling defendant to provide access to his cell phone is neither testimonial nor incriminating and (2) the foregone conclusion exception to the fifth amendment applies. Because

we agree with both of the State’s arguments, we reverse the judgment of the trial court and remand for further proceedings consistent with this opinion.

¶ 3

I. BACKGROUND

¶ 4

A. The Charges

¶ 5

In February 2021, the State charged defendant by information with two counts of forgery (*id.*). The charging documents alleged defendant made two false paychecks from Dairy Queen with the intent to defraud Dairy Queen and “financial institutions.” Defendant and his wife, Allora Spurling, were both arrested in connection with the false paychecks. When they were arrested, the police seized two cell phones from their persons—one from defendant and one from Spurling.

¶ 6

B. The Search Warrant

¶ 7

In March 2021, Detective Todd Ummel of the Clinton Police Department applied for a search warrant to search the contents of both phones. He described the items to be searched as (1) a “Samsung Galaxy A01” “belonging to [defendant]” and (2) a “Samsung Galaxy J2” “belonging to [Spurling.]”

¶ 8

In his complaint for search warrant, Ummel attested to the following information. In January 2021, Sara Schlesinger, a bookkeeper for Dairy Queen in Clinton, Illinois, reported to the Clinton Police Department that she “came across” a paycheck in the amount of \$274.33, payable to defendant. Defendant had never been an employee of Dairy Queen, but his wife—Spurling—was a current employee. Schlesinger reported that the paycheck had been cashed with Citibank via mobile deposit (*i.e.*, through the use of a cell phone). Schlesinger provided Clinton police officer Alex Lovell with a text message Spurling sent to Schlesinger that stated as follows:

“I didn’t know anything about it. I guess it wasn’t meant to happen for real. It [*sic*]

was being curious and he didn't think it would actually work cuz it wasn't real. He never got the money. *** I'm upset and embarrassed. And pissed. But please know I had no clue about it[.] He doesn't have a card for that bank or anything. Is there a way to call the bank and get the money back cuz he didn't get it[.]”

Schlesinger also provided Ummel with a second paycheck she discovered, payable to defendant in the amount of \$423.22. This check was also deposited by mobile deposit. Schlesinger confirmed the amounts written on the paychecks were taken out of Dairy Queen's bank account.

¶ 9 Ummel also stated in his complaint for search warrant that he sought to search defendant's phone to “confirm whom [*sic*] deposited the forged paycheck and to determine if any additional forged paychecks have been deposited.” He further sought to “confirm that the text messages from [Spurling] came from her phone.”

¶ 10 The trial court issued a search warrant granting Ummel permission to search both phones.

¶ 11 C. The State's Motion To Compel

¶ 12 A few days later, the State filed a “Motion to Compel Production of Cellular Phone Passcode” in defendant's case, which requested an order “to compel the entry of a passcode into a cellular device.” The motion alleged that the police were prevented from executing the search warrant because both phones were passcode-protected. (We note that this appeal pertains only to defendant and access to the cell phone identified as his in the search warrant.)

¶ 13 Later that same month, the trial court conducted an evidentiary hearing on the State's motion, at which Ummel was the sole witness. He testified that the Clinton Police Department was contacted by “[m]anagement” at Dairy Queen “[r]egarding fraudulent checks that were cashed on the account of Dairy Queen.” Defendant had never been employed at Dairy Queen,

but defendant's wife was an employee at the time the checks were cashed. Ummel testified that both checks were cashed via mobile electronic deposit from a cellular phone. Ummel explained that mobile deposit involves taking a photograph of a check and sending it electronically to a financial institution for deposit.

¶ 14 Ummel further testified that he observed pictures of the two cashed checks. (The record does not state where Ummel viewed the photographs, who showed him the photographs, or whether they were physical or electronic photographs.) They were payable to defendant and endorsed with the signature "Keiron Sneed." Ummel also stated that Schlesinger provided him with text messages in which Spurling admitted defendant cashed the checks. Schlesinger also provided Ummel with bank records that showed the funds were missing from the Dairy Queen account.

¶ 15 Ummel also testified that he obtained the search warrant to search defendant's and Spurling's cell phones but discovered the phones were locked by security passcodes. He stated defendant and Spurling would not provide him with the passcodes. The Clinton police did not have the technology to "crack" the phone, and the agency that assisted him in the past—the Illinois State Police—would not assist unless his investigation involved narcotics.

¶ 16 Ummel further testified that, following defendant's arrest, defendant filled out a bond form and provided a phone number that matched the phone that was seized from him. Ummel testified he was "hoping to find *** that a photograph exists on that device from submitting the mobile deposit."

¶ 17 D. The Trial Court's Ruling

¶ 18 The trial court denied the State's motion. The court first noted that the fifth amendment privilege against self-incrimination applies only when an accused is compelled to

make a testimonial communication that is incriminating. But then, relying on *People v. Spicer*, 2019 IL App (3d) 170814, 125 N.E.3d 1286, the court found that the act of producing a cell phone passcode is testimonial.

¶ 19 The trial court then examined whether the foregone conclusion doctrine—an exception to the fifth amendment privilege—applied to the facts of this case. Again relying on *Spicer*, the court found that, for the doctrine to apply, the State must show with reasonable particularity that, when it sought the act of production, it “knew the evidence existed, the evidence was in the [d]efendant’s possession and it was authentic.” The court noted (1) a valid search warrant had issued for the phone’s contents, which defendant did not challenge, and (2) law enforcement has a right to access the contents of the cell phone. The court concluded, however, that it “would be speculation *** to presume at this point that the photograph would still be on the phone,” and it “[could not] find here that it’s more likely to be found on the [d]efendant’s phone any more than it might be on the [co-defendant’s] phone.” Accordingly, the court found that the State did not show the foregone conclusion doctrine applied and denied the State’s motion to compel defendant to provide access to his cell phone.

¶ 20 The State filed a certificate of substantial impairment, and this appeal followed. Ill. S. Ct. R. 604(a)(1) (eff. July 1, 2017).

¶ 21 **II. ANALYSIS**

¶ 22 The State appeals, arguing two reasons why the trial court erred by concluding the fifth amendment protected defendant from being compelled to provide access to his lawfully seized cell phone: (1) compelling defendant to provide access to his cell phone is neither testimonial nor incriminating and (2) the foregone conclusion exception to the fifth amendment applies.

¶ 23 Defendant initially responds that the State’s appeal should be dismissed for lack of

jurisdiction because the trial court's order did not have the substantive effect of quashing the search warrant and suppressing evidence, as required by Rule 604(a)(1). *Id.* Alternatively, defendant argues that (1) the compelled production of a cell phone passcode is an act of production that is protected by the fifth amendment and (2) the foregone conclusion doctrine does not apply to the facts of this case.

¶ 24 Because we agree with both of the State's arguments, we reverse the judgment of the trial court and remand for further proceedings consistent with this opinion.

¶ 25 A. The Standard of Review

¶ 26 We review *de novo* whether the State may take an interlocutory appeal under Rule 604(a). *People v. Drum*, 194 Ill. 2d 485, 488, 743 N.E.2d 44, 46 (2000).

¶ 27 We apply a bifurcated standard of review to the trial court's determination that the fifth amendment privilege protects defendant from being compelled to provide his passcode. First, we "accord great deference to the trial court's factual findings, and *** reverse those findings only if they are against the manifest weight of the evidence." *In re G.O.*, 191 Ill. 2d 37, 50, 727 N.E.2d 1003, 1010 (2000). Next, we review *de novo* the ultimate question of whether the privilege applies. *Id.*; see also *Spicer*, 2019 IL App (3d) 170814, ¶ 14 (citing *People v. McRae*, 2011 IL App (2d) 090798, ¶ 25, 959 N.E.2d 1245); *In re A.W.*, 231 Ill. 2d 92, 106, 896 N.E.2d 316, 324 (2008) ("The standard of review for determining whether an individual's [fifth amendment] rights have been violated is *de novo*." (Internal quotation marks omitted.)).

¶ 28 In this case, Ummel was the sole witness at the hearing on the State's motion to compel, and the trial court appeared to have no difficulty accepting his testimony. Thus, like the trial court, we will accept his testimony and now review *de novo* the trial court's determination that the fifth amendment privilege against self-incrimination protected defendant from being

compelled to provide his passcode.

¶ 29

B. Jurisdiction

¶ 30

Defendant first argues that the State's appeal should be dismissed for lack of jurisdiction under Illinois Supreme Court Rule 604(a)(1) (eff. July 1, 2017) because the trial court's denial of the State's motion to compel did not have the substantive effect of quashing the search warrant and suppressing evidence. Defendant also contends that the impairment of the State's case is questionable. The State responds that the court's order precluded the State from accessing the information on the phone, which is no different than precluding the State from presenting the information on the cell phone at trial. We agree with the State.

¶ 31

Rule 604(a)(1) reads as follows: "*When State May Appeal*. 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; or suppressing evidence." *Id.*

¶ 32

Before the State may obtain review of a suppression order under Rule 604(a), the State must certify to the trial court that the suppression order substantially impairs its ability to prosecute the case. *People v. Turner*, 367 Ill. App. 3d 490, 494, 854 N.E.2d 1139, 1143 (2006). "A good-faith evaluation by the prosecutor of the impact of a suppression order is sufficient to meet the State's burden." *Id.* at 495 (citing *People v. Keith*, 148 Ill. 2d 32, 40, 591 N.E.2d 449, 452 (1992)); see also *People v. Young*, 82 Ill. 2d 234, 247-48, 412 N.E.2d 501, 507 (1980). "[T]he substantive effect of a trial court's pretrial order, not the label of the order or its underlying motion, controls appealability under Rule 604(a)(1)." *Drum*, 194 Ill. 2d at 489. We agree with what the Third District wrote in *Spicer*: "When a warrant has issued allowing a search of a defendant's phone, an order that denies a motion to compel the defendant to decrypt the phone is like an order suppressing evidence." *Spicer*, 2019 IL App (3d) 170814, ¶ 11.

¶ 33 Here, the State filed a certificate of substantial impairment, attesting that the trial court’s order “effectively suppress[e] evidence and prevent[s] the State from acquiring evidence pursuant to a search warrant issued by the Court, thereby effectively quashing the search warrant, substantially impair[ing] [the State’s] ability to prosecute this cause.”

¶ 34 We accept the State’s good faith evaluation of the impact of the trial court’s order on its ability to prosecute its case and agree that the trial court’s order is like an order suppressing evidence. Accordingly, we conclude that we have jurisdiction to hear this appeal.

¶ 35 C. The Fifth Amendment Privilege Against Self-Incrimination

¶ 36 1. *The Applicable Law*

¶ 37 The fifth amendment to the United States Constitution provides that “[n]o person *** shall be compelled in any criminal case to be a witness against himself.” U.S. Const., amend. V. The Illinois Constitution similarly provides, “No person shall be compelled in a criminal case to give evidence against himself ***.” Ill. Const. 1970, art. I, § 10. The state and federal constitutional privileges against self-incrimination “differ in semantics rather than in substance and have received the same general construction.” *People ex rel. Hanrahan v. Power*, 54 Ill. 2d 154, 160, 295 N.E.2d 472, 475 (1973).

¶ 38 The privilege against self-incrimination is intended to protect an accused “from having to reveal, directly or indirectly, his knowledge of facts relating him to the offense or from having to share his thoughts and beliefs with the Government.” *Doe v. United States*, 487 U.S. 201, 213 (1988) (*Doe II*). “[T]he Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a testimonial communication that is incriminating.” (Emphasis omitted.) *Fisher v. United States*, 425 U.S. 391, 408 (1976). “To establish a fifth amendment violation,

appellants must therefore demonstrate the existence of three elements: 1) compulsion, 2) a testimonial communication, and 3) the incriminating nature of that communication.” *In re Grand Jury Subpoena*, 826 F.2d 1166, 1168 (2d Cir. 1987).

¶ 39 a. What Constitutes a Testimonial Communication

¶ 40 “[T]o be testimonial, an accused’s communication must itself, explicitly or implicitly, relate a factual assertion or disclose information.” *Doe II*, 487 U.S. at 210. It is “the attempt to force [a suspect] ‘to disclose the contents of his own mind,’ [citation] that implicates the Self-Incrimination Clause.” *Id.* at 211 (quoting *Curcio v. United States*, 354 U.S. 118, 128 (1957)). This requirement that the compelled communication assert a fact or disclose information explains why certain acts, although incriminating, are not testimonial and do not enjoy fifth amendment protection. See, e.g., *Schmerber v. California*, 384 U.S. 757, 765 (1966) (a suspect may be compelled to furnish a blood sample); *Gilbert v. California*, 388 U.S. 263, 266-67 (1967) (handwriting exemplar); *United States v. Dionisio*, 410 U.S. 1, 7 (1973) (voice exemplar); *United States v. Wade*, 388 U.S. 218, 221-22 (1967) (stand in a lineup). The United States Supreme Court has explained that the fifth amendment’s protections are limited to “testimonial” communications because “there is a significant difference between the use of compulsion to extort communications from a defendant and compelling a person to engage in conduct that may be incriminating.” *United States v. Hubbell*, 530 U.S. 27, 34-35 (2000).

¶ 41 For example, in *Doe II*, 487 U.S. at 215-19, the Supreme Court held that an order compelling the petitioner—who was the target of a grand jury investigation—to sign an authorization that permitted foreign banks to disclose records of his accounts (if any existed) had no testimonial significance because the mere act of signing the form made no statement, implicit or explicit, regarding the existence of any foreign bank account, control over any such account, or

the authenticity of any records produced by any bank. The authorization was carefully drafted in the hypothetical to not refer to any specific bank or account number so that it would not serve as an acknowledgement by the target of the existence of any foreign bank account, his control over any bank account, or the authenticity of any documents produced. *Id.* at 215-16. The Court rejected the petitioner’s “blanket assertion” that a statement is testimonial if its content can be used to obtain evidence. *Id.* at 208 n.6. In doing so, the Court reasoned that this argument “confuses the requirement that the compelled communication be ‘testimonial’ with the separate requirement that the communication be ‘incriminating.’ ” *Id.* “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.* (quoting *In re Grand Jury Subpoena*, 826 F.2d at 1171 n.2 (Newman, J., concurring)).

¶ 42 Certain communicative acts, however, may be testimonial for purposes of the fifth amendment. For example, the act of producing documents in response to a subpoena could have “communicative aspects of its own, wholly aside from the contents of the papers produced.” *Fisher*, 425 U.S. at 410; see also *Hubbell*, 530 U.S. at 36 (“[T]he act of producing documents in response to a subpoena may have a compelled testimonial aspect.”). “Compliance with [a] subpoena tacitly concedes the existence of the papers demanded and their possession or control by the [person subpoenaed].” *Fisher*, 425 U.S. at 410. This is known as the “act of production” doctrine, which “permits an individual to assert his fifth amendment privilege against self-incrimination and refuse to produce subpoenaed documents where the mere act of production, rather than the content of the documents, has testimonial ramifications.” *In re Grand Jury Subpoena Duces Tecum No. 001144*, 164 Ill. App. 3d 344, 347, 517 N.E.2d 1157, 1159 (1987).

¶ 43 b. The Foregone Conclusion Doctrine

¶ 44 A corollary doctrine—also formulated in *Fisher*—that serves as an exception to the act of production doctrine is the “foregone conclusion” doctrine. Under this doctrine, the testimonial value of the act of production is lost where the information conveyed by the act of production is already known by the State. *Fisher*, 425 U.S. at 411. For this exception to apply, the State must establish its knowledge of (1) the existence of the information demanded, (2) the possession or control of that information by the defendant, and (3) the authenticity of the information. *Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 614 (Mass. 2014) (citing *Fisher*, 425 U.S. at 410-13); see also *United States v. Bright*, 596 F.3d 683, 692 (9th Cir. 2010). Where these elements are satisfied, the testimony implied by the defendant’s act of production is a “foregone conclusion” that “adds little or nothing to the sum total of the Government’s information.” *Fisher*, 425 U.S. at 411. In that case, “no constitutional rights are touched. The question is not of testimony but of surrender.” (Internal quotation marks omitted.) *Id.*

¶ 45 Thus, the United States Supreme Court has identified two means by which an act of production is not testimonial and, as such, falls outside the protection of the fifth amendment: (1) where the act of production compels a mere physical act (*Doe II*, 487 U.S. at 215) and (2) where the act of production conveys information that is a “foregone conclusion” (*Fisher*, 425 U.S. at 410-14). For the reasons that follow, we conclude the trial court erred because both means apply to the facts of this case.

¶ 46 *2. This Case*

¶ 47 a. Testimonial vs. Non-testimonial

¶ 48 The State first argues that compelling defendant to provide entry to his passcode-protected phone is not a testimonial act of production because it is a mere physical act, such as providing a thumbprint, blood sample, or voice exemplar. Defendant responds that

compelling him to provide access to his passcode-protected phone is a testimonial act of production because it requires him to utilize the “contents of his mind.” See *Hubbell*, 530 U.S. at 43; *Doe II*, 487 U.S. at 210 n.9. Defendant contends the act of providing entry to his cell phone is more like “telling an inquisitor the combination to a wall safe” than “being forced to surrender the key to a strongbox.” See *Hubbell*, 530 U.S. at 43; see also *Doe II*, 487 U.S. at 210 n.9.

¶ 49 Consistent with defendant’s position, several courts have held the compelled production of a passcode or decryption key to be a testimonial act because it reveals the “contents of the person’s mind.” See, e.g., *In re Search Warrant Application for [Redacted Text]*, 279 F. Supp. 3d 800, 806 (N.D. Ill. 2017); *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012); *United States v. Kirschner*, 823 F. Supp. 2d 665, 668-69 (E.D. Mich. 2010). Under this rationale, the “physical/mental production” dichotomy is “a critical distinction” in determining whether an act is testimonial or non-testimonial. *Commonwealth v. Davis*, 220 A.3d 534, 547-48 (Pa. 2019) (“Consistent with a physical/mental production dichotomy, in conveying the combination to a wall safe, versus surrendering a key to a strongbox, a person must use the ‘contents of [his] own mind.’ ”).

¶ 50 However, an examination of the origin of the “mental/physical production” dichotomy leads us to question whether it is properly applied in the context of compelled access to a passcode-protected phone.

¶ 51 i. *The Origins of the Mental/Physical Production Dichotomy*

¶ 52 The dichotomy originates in *Doe II*, where the United States Supreme Court determined that the petitioner was not protected by the fifth amendment from being compelled to sign an authorization that would allow foreign banks to disclose documents relating to his accounts, if those accounts existed. *Doe II*, 487 U.S. at 203, 215. Justice Stevens dissented and

opined that a defendant cannot “be compelled to use his mind to assist the prosecution in convicting him of a crime.” *Id.* at 219 (Stevens, J., dissenting). He reasoned that a defendant “may in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe—by word or deed.” *Id.* The majority addressed Justice Stevens’s analogy and expressed its agreement that “[t]he expression of the contents of an individual’s mind” is testimonial but disagreed that the execution of the authorization at issue “forced [the] petitioner to express the contents of his mind.” (Internal quotation marks omitted.) *Id.* at 210 n.9 (majority opinion). The majority believed the compelled execution of the authorization was more like surrendering a key than providing a combination. *Id.*

¶ 53 Thereafter, in *Hubbell*, a case involving a subpoena *duces tecum*, the Supreme Court rejected the government’s argument that the respondent’s act of producing documents was merely a physical act. *Hubbell*, 530 U.S. at 41-43. The government’s subpoena sought the production of 11 categories of documents. *Id.* at 31. The respondent “produced 13,120 pages of documents and records and responded to a series of questions that established that those were all of the documents in his custody or control that were responsive to the commands in the subpoena.” *Id.* The Court observed the following:

“The assembly of literally hundreds of pages of material in response to a request for ‘any and all documents reflecting, referring, or relating to any direct or indirect sources of money or other things of value received by or provided to’ an individual or members of [respondent’s] family during a 3-year period *** is the functional equivalent of the preparation of an answer to either a detailed written interrogatory or a series of oral questions at a discovery deposition.” *Id.* at 41-42.

The Court also observed that the respondent “took the mental and physical steps necessary to

provide the prosecutor with an accurate inventory of the many sources of potentially incriminating evidence sought by the subpoena.” *Id.* at 42. The Court explained the government’s possession of the documents was not the fruit of a mere physical act of production. Instead, “it was unquestionably necessary for respondent to make extensive use of ‘the contents of his own mind’ in identifying the hundreds of documents responsive to the requests in the subpoena.” *Id.* at 43. The Court then repeated Justice Stevens’s analogy from *Doe II*, observing, “[t]he assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox.” *Id.*

¶ 54 ii. *Lower Courts’ Interpretations*

¶ 55 Several courts have since held that the compelled production of a passcode (or unlocked/decrypted device) is a testimonial act of production because it requires the use of the “contents of the mind.” See, e.g., *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d at 1346 (“[T]he decryption and production of the hard drives would require the use of the contents of [the defendant’s] mind.”); *G.A.Q.L. v. State*, 257 So. 3d 1058, 1061 (Fla. Dist. Ct. App. 2018) (“[R]evealing one’s password *** probes into the contents of an individual’s mind.”); *Davis*, 220 A.3d at 548 (“[O]ne cannot reveal a passcode without revealing the contents of one’s mind.”). This group includes the only Illinois court to address the issue, *Spicer*, 2019 IL App (3d) 170814, discussed in further detail *infra*, ¶¶ 72-81.

¶ 56 Other courts have questioned whether the strongbox key/wall safe combination analogy is appropriate for the digital world. See *State v. Stahl*, 206 So. 3d 124, 135 (Fla. Dist. Ct. App. 2016) (“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.”);

State v. Andrews, 234 A.3d 1254, 1274 (N.J. 2020) (“[I]n some cases, a biometric device lock can be established only after a passcode is created, calling into question the testimonial/non-testimonial distinction in this context.”). Although the *Andrews* court ultimately held that the production of a passcode is testimonial, it noted that “passcodes are a series of characters without independent evidentiary significance and are therefore of ‘minimal testimonial value’—their value is limited to communicating the knowledge of the passcodes.” *Id.* at 1274 (citing *United States v. Apple MacPro Computer*, 851 F.3d 238, 248 n.7 (3d Cir. 2017)).

¶ 57 The *Andrews* and *Stahl* courts also expressed concern that, under the physical/mental dichotomy, fifth amendment protection may apply to a phone that is protected by a numeric passcode, but not to a phone protected by a thumbprint. See, e.g., *Andrews*, 234 A.3d at 1274 (“We also share the concerns voiced by other courts that holding passcodes exempt from production whereas biometric device locks may be subject to compulsion creates inconsistent approaches based on form rather than substance.”); *Stahl*, 206 So. 3d at 135 (“[W]e 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.”).

¶ 58 iii. *This Court’s Conclusion: Production of a Passcode Is Non-testimonial*

¶ 59 The questions raised in *Stahl* and *Andrews* regarding the continued viability of the key/combination analogy (*i.e.*, mental/physical dichotomy) in the digital age deserve consideration. We, too, observe that a cell phone passcode is string of letters or numbers that an individual habitually enters into his electronic device throughout the day. A passcode may be used so habitually that its retrieval is a function of muscle memory rather than an exercise of conscious thought. A fair question that arises, then, is whether the rote application of a series of numbers

should be treated the same as the *Hubbell* respondent's "exhaustive use of the 'contents of his mind' " to produce hundreds of pages of responsive documents. The two scenarios appear to bear no resemblance to each other.

¶ 60 We share the concerns expressed in *Stahl* and *Andrews* and observe that, given the advancements in technology, a cell phone passcode is more akin to a key to a strongbox than a combination to a safe. Or, at the very least, perhaps in this digital age the distinction between a physical key and a combination to a safe has become blurred, with a cellular phone passcode encompassing both. This blurring of distinctions would diminish the analytical value of the analogy that so many courts have relied on to hold that the act of providing a passcode is testimonial.

¶ 61 Moreover, at least one federal court has hinted that the act of unlocking a phone may not be testimonial if (1) no dispute exists that the suspect owns the phone, (2) the suspect is not asked to reveal the passcode to the police, and (3) the suspect makes the contents of her cell phone accessible to the police by entering it herself without telling the police the passcode. See *United States v. Oloyede*, 933 F.3d 302, 309 (4th Cir. 2019) ("[Defendant] has not shown that her act communicated her cell phone's unique passcode. Unlike a circumstance, for example, in which she gave the passcode to an agent for the agent to enter, here she simply used the unexpressed contents of her mind to type in the passcode herself."). In *Oloyede*, the defendant entered the passcode herself and gave the unlocked phone to the police officer. *Id.* at 308. The officer did not ask for the passcode or observe the defendant enter the passcode, and the defendant did not reveal the passcode to the police. *Id.* Similarly, in the case before us, the State is requesting an order that the defendant "provide entry" to his cell phone. That means that defendant, like the defendant in *Oloyede*, could simply enter his passcode into his phone and thereby make its contents accessible

to the police without ever telling the police the passcode.

¶ 62 Notably, the trial court in this case, when ruling on the State’s motion, expressed its belief that the facts here were “no different than compelling a Defendant to disclose a key to a storage unit or a lockbox or something of that nature.” The court then observed, “Here, disclosing the passcode would not seem to make extensive use of the contents of the Defendant’s mind” and expressed its opinion that “an objective, reasonable judge could reach the conclusion that the production of the pass code is not testimonial.” However, the court correctly acknowledged that it was obligated to follow the Third District’s holding in *Spicer* that the production of a passcode is testimonial because no other Illinois court of review had yet spoken on the issue.

¶ 63 For the reasons stated, we conclude that requiring defendant to provide entry or the passcode to the phone does not compel him to provide testimony within the meaning of the fifth amendment.

¶ 64 b. The Foregone Conclusion Doctrine

¶ 65 The State also argues that even if we conclude that the act of providing entry or the passcode to defendant’s phone is testimonial, the foregone conclusion doctrine applies. The State contends the trial court erred in its application of the foregone conclusion doctrine because it equated the act of providing access to the phone with the act of collecting the evidence from the phone. Defendant responds that the trial court properly found the foregone conclusion doctrine did not apply because the State did not establish that, at the time it requested production, it knew of the existence, possession, and authenticity of the information it sought within the phone.

¶ 66 We agree with the State that the foregone conclusion doctrine applies. This conclusion is a second and separate reason for holding that the trial court erred by denying the State’s motion.

¶ 67 i. *The Proper Focus of the Foregone Conclusion Analysis*

¶ 68 (a) Passcode vs. Contents of the Phone

¶ 69 The parties' initial disagreement centers upon whether a court conducting a foregone conclusion analysis should focus on (1) the compelled communication itself (*i.e.*, the entry of the passcode) or (2) the information to be revealed by the entry of the passcode. One scholar has helpfully described these competing focuses as (1) the act that opens the door and (2) the treasure that lies beyond the door. See Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 Tex. L. Rev. 767, 777 (2019).

¶ 70 Courts are also split on this issue. Several courts have held that the proper focus of the foregone conclusion analysis is on the testimonial value of the act of producing the passcode. See *Andrews*, 234 A.3d at 1273 (“[W]e find that the foregone conclusion test applies to the production of the passcodes themselves, rather than to the phones’ contents.”); *Stahl*, 206 So. 3d at 136 (“[T]he relevant question is whether the State has established that it knows with particularity that the passcode exists, is within the accused’s possession or control, and is authentic.”); *Gelfgatt*, 11 N.E.3d at 615 (“[W]e conclude that the factual statements that would be conveyed by the defendant’s act of entering an encryption key in the computers are ‘foregone conclusions’ and, therefore, the act of decryption is not a testimonial communication that is protected by the Fifth Amendment.”); *State v. Johnson*, 576 S.W.3d 205, 227 (Mo. 2019) (“The focus of the foregone conclusion exception is the extent of the State’s knowledge of the existence of the facts conveyed through the compelled act of production. Here, [defendant] was ordered to produce the passcode to his phone.”); *Commonwealth v. Jones*, 117 N.E.3d 702, 710 (Mass. 2019) (“[F]or the foregone conclusion exception to apply, the Commonwealth must establish that it already knows the testimony that is implicit in the act of the required production. [Citation.] In the context of

compelled decryption, the only fact conveyed by compelling a defendant to enter the password to an encrypted electronic device is that the defendant knows the password, and can therefore access the device.”).

¶ 71 Other courts have placed the focus of the foregone conclusion analysis on the files stored on the device. See *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d at 1346 (“Nothing in the record before us reveals that the Government knows whether any files exist and are located on the hard drives ***.”); *Seo v. State*, 148 N.E.3d 952, 958 (Ind. 2020) (“This leads us to the following inquiry: has the State shown that (1) [defendant] knows the password for her iPhone; (2) the files on the device exist; and (3) she possessed those files?”); *G.A.Q.L.*, 257 So. 3d at 1063 (“It is not the verbal recitation of a passcode, but rather the documents, electronic or otherwise, hidden by an electronic wall that are the focus of this exception.”).

¶ 72 (b) *People v. Spicer*: Focus on the Contents of the Phone

¶ 73 The only Illinois court to consider the application of the foregone conclusion doctrine in the context of a motion to compel production of a cell phone passcode is *Spicer*. In *Spicer*, the defendant was pulled over for a traffic violation. *Spicer*, 2019 IL App (3d) 170814, ¶ 3. A drug dog alerted on the vehicle, and officers found a pill bottle containing cocaine inside a bag in the area where the defendant had been sitting. *Id.* ¶ 5. The police arrested the defendant for possession of a controlled substance, and the State later charged him with possession with intent to deliver. *Id.* ¶ 3. The police obtained a search warrant for a cell phone they seized from the defendant during his arrest. *Id.* ¶ 4. After the defendant declined to provide the passcode to the phone, the State filed a motion to compel its production. *Id.*

¶ 74 The Third District concluded the foregone conclusion exception did not apply

because the State did not establish with reasonable particularity “the contents of the phone.” *Id.* ¶ 21. In framing its analysis, the court noted that “Illinois courts [had] not decided whether compelling a defendant to provide his passcode is testimonial,” and acknowledged the analytical split among foreign jurisdictions on the issue. *Id.* ¶¶ 16-17. For guidance, the Third District looked to a case from the Florida District Court of Appeals, *G.A.Q.L.*, 257 So. 3d at 1062, which examined the compelled production of an iTunes password. *Spicer*, 2019 IL App (3d) 170814, ¶ 19.

¶ 75 In *G.A.Q.L.*, the court first determined that the compelled production of the password was testimonial because it necessitates the use of the mind. *G.A.Q.L.*, 257 So. 3d at 1062. The court next determined that “the object of the foregone conclusion exception is not the password itself, but the data the state seeks behind the passcode wall.” *Id.* at 1063. The court then held that foregone conclusion doctrine did not apply because the State “fail[ed] to identify any specific file locations or even name particular files that it [sought] from the *** passcode-protected phone.” *Id.* at 1064. Instead, it “generally [sought] essentially all communications, data, and images on the locked iPhone” based on “the prosecutor’s statement at the hearing that the surviving passenger [of a DUI-related accident] had been communicating with [the defendant] via Snapchat and text message on the day of the accident and after the accident.” *Id.*

¶ 76 The Third District found *G.A.Q.L.* persuasive and held that the focus of a foregone conclusion analysis should be placed on the contents of the phone instead of the production of the passcode. *Spicer*, 2019 IL App (3d) 170814, ¶ 21.

¶ 77 In applying this analytical framework to the facts before it, the Third District concluded that the State “does not know what information might be on [the defendant’s] phone but surmises that cell phones are often used in unlawful drug distribution and such information would be available on [the defendant’s] phone.” *Id.* ¶ 22. The court noted that the search warrant

permitted the State to access “most of the information” on the defendant’s phone, and the State “[did] not identify any documents or specific information it [sought] with reasonable particularity.”

Id.

¶ 78 We view *Spicer* and *G.A.Q.L.* as factually distinguishable. In contrast to those cases, here, the State has described with reasonable particularity the information it seeks.

¶ 79 Ummel testified he believed he would find on defendant’s phone photographs of the false paychecks and evidence of their electronic deposit. Ummel also testified he observed photographs of the false paychecks, which were payable to defendant and endorsed in defendant’s name for mobile deposit to Citibank and Varo Bank. Ummel also observed Spurling’s text message to Schlesinger, which stated that defendant deposited the checks by mobile deposit. Ummel also explained that mobile deposit involves taking a photograph of a check and sending it electronically to a financial institution.

¶ 80 Dairy Queen’s bank records confirmed that the false paychecks were deposited in this manner and the funds were missing from Dairy Queen’s accounts. In other words, Ummel described the documents and evidence he was looking for and explained why he expected it to be found on defendant’s phone.

¶ 81 In addition to viewing *Spicer* and *G.A.Q.L.* as factually distinguishable, we also do not believe—for reasons we discuss in greater detail *infra*, ¶¶ 82-95—that the Third District was correct to conclude that the focus of the foregone conclusion doctrine is properly placed on the information on the phone. On that issue, we find more persuasive the reasoning of the New Jersey Supreme Court in *Andrews*, 234 A.3d at 1273, which held that “the foregone conclusion test applies to the production of the passcodes themselves, rather than to the phones’ contents.”

¶ 82 (c) *State v. Andrews*: Focus on the Passcode

¶ 83 In *Andrews*, the defendant was a former sheriff's deputy who was charged with official misconduct for revealing the existence of an undercover narcotics investigation to its target. *Id.* at 1261. According to the target, the defendant also advised him to (1) remove a tracking device from his vehicle and (2) discard cell phones. *Id.* at 1259. The communications occurred largely through the iPhone FaceTime application and text messages. *Id.* at 1260. The State seized the defendant's cell phones and obtained a warrant to search them but was unable to access the phones' contents without the passcodes. *Id.* at 1261. The State moved to compel the defendant to disclose the passcodes to his two phones. *Id.*

¶ 84 In considering whether the fifth amendment protected the defendant from disclosing the passcodes to his phones, the court first examined the history of the fifth amendment privilege in the context of compelled communications, including *United States v. Doe*, 465 U.S. 605 (1984) (*Doe I*), *Fisher*, and *Hubbell*. *Andrews*, 234 A.3d at 1266-69. The court noted that these cases all involved the production of documents and gave rise to the inference that the act of production "must be considered in its own right, separate from the documents sought." *Id.* at 1269 (citing *Fisher*, 425 U.S. at 410 ("The act of producing evidence *** has communicative aspects of its own, wholly aside from the contents of the papers produced."), *Doe I*, 465 U.S. at 612 ("Although the contents of a document may not be privileged, the act of producing the document may be."), and *Hubbell*, 530 U.S. at 40 ("The 'compelled testimony' that is relevant in this case is not to be found in the contents of the documents produced in response to the subpoena. It is, rather, the testimony inherent in the act of producing those documents.")).

¶ 85 The *Andrews* court concluded, "To be consistent with the Supreme Court case law that gave rise to the exception, we find that the foregone conclusion test applies to the production of the passcodes themselves, rather than to the phones' contents." *Andrews*, 234 A.3d at 1273.

¶ 86 (d) Our Conclusion: The Focus Is on the Passcode

¶ 87 We agree with *Andrews* and find further support for its conclusion in *Doe II*, in which the Supreme Court rejected “[p]etitioner’s blanket assertion that a statement is testimonial for Fifth Amendment purposes if its content can be used to obtain evidence” because it “confuses the requirement that the compelled communication be ‘testimonial’ with the separate requirement that the communication be ‘incriminating.’ ” *Doe II*, 487 U.S. at 208 n.6. As the Supreme Court observed, “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.” (Internal quotation marks omitted.) *Id.* at 208 n.6.

¶ 88 Additionally, the *Hubbell* court noted, “Whether the constitutional privilege *** protects the act of production itself, is a question that is distinct from the question whether the unprotected contents of the documents themselves are incriminating.” *Hubbell*, 530 U.S. at 37.

¶ 89 Placing the focus of the foregone conclusion doctrine on the passcode rather than the documents or evidence contained on the phone appears to strike the most appropriate balance between fifth amendment concerns and fourth amendment concerns. In this case, the State’s motion seeks the compelled production of the *passcode*. The production of the passcode will lead to the contents of the phone, for which the State has obtained a valid search warrant that defendant does not challenge.

¶ 90 In ruling on the State’s motion to compel, the trial court addressed whether “the evidence sought for purposes of the foregone conclusion doctrine consist[s] of the pass code or the contents of the phone.” The court observed, “perhaps the better-reasoned argument is that *** the foregone conclusion exception should only apply to the pass code,” but again acknowledged its obligation, in the absence of any binding authority to the contrary, to follow the Third District’s

holding in *Spicer*.

¶ 91 In applying the Third District’s analytical framework (placing the focus on the contents of the phone rather than the passcode), the trial court observed that, to obtain a search warrant, the State “must articulate with particularity the person and place to be searched and the person and things to be seized. But for the foregone conclusion exception to apply, the State must know—it requires knowledge, but that knowledge is qualified with reasonable particularity.” This observation illustrates how the *Spicer* approach conflates the act of production with the contents of the phone. That is to say, it allows the fifth amendment to swallow the fourth amendment, thereby permitting a suspect to “hide” behind a passcode evidence to which the State is lawfully entitled pursuant to the issuance of the search warrant.

¶ 92 The contents of the phone are protected by the fourth amendment, and in this case, the State followed proper procedures to obtain a valid search warrant to seize that information. The testimonial value of the act of producing the passcode—a series of letters or numbers which “opens the door” to permit the State to execute that valid warrant—must be analyzed separately from the State’s authority to seize the evidence on the phone. And it bears repeating that defendant does not challenge the probable cause supporting the search warrant that authorizes seizure of the contents of his phone. Instead, he seeks to utilize the fifth amendment to prevent the operation of the fourth amendment, which authorizes (as here) the issuance of a search warrant based upon a verified complaint showing probable cause for the presence of evidence of a crime in the premises (here, the cell phone) to be searched.

¶ 93 By focusing (1) the fifth amendment analysis on the production of the passcode and (2) the fourth amendment analysis on the evidence contained on the phone, one constitutional provision does not become either superior or subservient to the other. Further, doing so ensures

that the protection against compelled self-incrimination and the interests of law enforcement in executing a valid search warrant are both respected.

¶ 94 These considerations provide further support for our conclusion that the Third District in *Spicer* erroneously relied on the faulty reasoning of the *G.A.Q.L.* court to hold that the proper focus of a foregone conclusion analysis is on the contents of the phone instead of the production of the passcode. *Spicer*, 2019 IL App (3d) 170814, ¶ 21. The *G.A.Q.L.* court reasoned that the phone’s contents is where the proper focus should lie because that is what the government truly seeks, not the passcode itself. *G.A.Q.L.*, 257 So. 3d at 1062. However, as illustrated above, this reasoning conflates fourth amendment concerns with fifth amendment concerns.

¶ 95 As the *Fisher* court explained,

“We cannot cut the Fifth Amendment completely loose from the moorings of its language, and make it serve as a general protector of privacy[,] a word not mentioned in its text and a concept directly addressed in the Fourth Amendment. We adhere to the view that the Fifth Amendment protects against ‘compelled self-incrimination, not (the disclosure of) private information.’ ” *Fisher*, 425 U.S. at 401 (quoting *United States v. Nobles*, 422 U.S. 225, 233 n.7 (1975)).

¶ 96 We acknowledge the Illinois Supreme Court’s recent decision in *People v. McCavitt*, 2021 IL 125550, ¶ 4, which addressed “a person’s reasonable expectation of privacy in data on an electronic storage device that is subject to search” and “the fourth amendment’s particularity requirement as applied to electronic storage devices.” However, in the case before us, defendant has not challenged the validity of the search warrant, which authorizes the State to seize the contents of his phone. *McCavitt* does not address the application of the fifth amendment where a phone that is the subject of a lawful search warrant is passcode-protected and the owner of the

phone declines to provide the passcode.

¶ 97 *ii. Application of the Foregone Conclusion Doctrine to This Case*

¶ 98 Applying these principles to the case before us, for the forgone conclusion doctrine to apply, the State must establish with reasonable particularity (1) it knows the passcode exists, (2) the passcode is within the defendant's possession or control, and (3) the passcode is authentic. See *Andrews*, 234 A.3d at 1274-75; *Stahl*, 206 So. 3d at 136.

¶ 99 Ummel testified that (1) the phone is locked by a security passcode, (2) defendant has not provided him with the passcode, and (3) Ummel does not have the technology to "crack" the passcode. This evidence establishes with reasonable particularity that a passcode for the phone exists.

¶ 100 Ummel further testified that one phone was retrieved from defendant and another was retrieved from Spurling. Defendant provided his phone number on a jail form when bonding out. When Ummel dialed that phone number, the phone Ummel identified as belonging to defendant in the complaint for search warrant would ring. This evidence establishes with reasonable particularity that defendant has had possession or control of the phone and, accordingly, has possession or control of the passcode required to access and utilize the phone.

¶ 101 Last, the courts in *Andrews* and *Stahl* addressed the authenticity element in the context of a cell phone passcode, noting that a passcode is self-authenticating. *Stahl*, 206 So. 3d at 136; *Andrews*, 234 A.3d at 1275. That is, if the passcode provides entry to the phone, the passcode is authentic. *Stahl*, 206 So. 3d at 136; *Andrews*, 234 A.3d at 1275. Therefore, the authenticity element will be determined when the passcode is entered into the phone.

¶ 102 Accordingly, the State has shown with reasonable particularity that the passcode exists and is within defendant's possession or control. The passcode will self-authenticate if it

unlocks the phone. As such, the foregone conclusion doctrine is satisfied, rendering the act of producing the passcode non-testimonial and outside the protection of the fifth amendment privilege against self-incrimination.

¶ 103 Even applying *Spicer*'s analytical framework to the facts of this case, the foregone conclusion doctrine applies because, as discussed *supra*, ¶¶ 78-80, the State has also established with reasonable particularity the "contents of the phone."

¶ 104 c. Evidence of the Act of Production at Trial

¶ 105 At the hearing on the motion to compel, and in its brief before this court, the State represented that it would not use at trial evidence of defendant's act of production of the passcode. The State explained that it "doesn't need an intricate pass code to prove ownership of the phone or its contents." That is precisely the point of the foregone conclusion doctrine; the testimony implied by the act of producing the passcode—*i.e.*, the defendant has knowledge of the passcode—"adds little or nothing to the sum total of the Government's information." *Fisher*, 425 U.S. at 411.

¶ 106 We agree with the State that the defendant's knowledge of the phone's passcode and his knowledge of the phone's contents are two different things. Because of the commitment the State has made to the trial court—namely, that it will not use evidence of defendant's act of production at trial—the State will be required to prove defendant's knowledge of the phone's contents through other means. And on remand, the State's commitment is enforceable by the trial court.

¶ 107 III. CONCLUSION

¶ 108 For the reasons stated, we reverse the judgment of the trial court and remand for further proceedings consistent with this opinion.

¶ 109 Reversed and remanded.

No. 4-21-0180

Cite as: *People v. Sneed*, 2021 IL App (4th) 210180

Decision Under Review: Appeal from the Circuit Court of De Witt County, No. 21-CF-13; the Hon. Karle E. Koritz, Judge, presiding.

**Attorneys
for
Appellant:** Daniel Markwell, State’s Attorney, of Clinton (Patrick Delfino, David J. Robinson, David E. Mannchen, and James C. Majors, of State’s Attorneys Appellate Prosecutor’s Office, of counsel), for the People.

**Attorneys
for
Appellee:** James E. Chadd, Catherine K. Hart, and Joshua Scanlon, of State Appellate Defender’s Office, of Springfield, for appellee.
