No. 127968

IN THE

SUPREME COURT OF ILLINOIS

PEOPLE OF THE STATE OF ILLINOIS, Respondent-Appellee, -vs- KEIRON K. SNEED, Petitioner-Appellant.	Appeal from the Appellate Court of Illinois, Fourth Judicial District, No. 4-21-0180. There on appeal from the Circuit Court of the Sixth Judicial Circuit, DeWitt County, Illinois, No. 21-CF-13. Honorable Karle E. Koritz, Judge Presiding.

BRIEF AND ARGUMENT FOR PETITIONER-APPELLANT

JAMES E. CHADD
State Appellate Defender

CATHERINE K. HART
Deputy Defender

JOSHUA SCANLON
Assistant Appellate Defender
Office of the State Appellate Defender
Fourth Judicial District
400 West Monroe Street, Suite 303
Springfield, IL 62704
(217) 782-3654
4thdistrict.eserve@osad.state.il.us

COUNSEL FOR PETITIONER-APPELLANT

E-FILED
6/8/2022 2:35 PM
CYNTHIA A. GRANT
SUPREME COURT CLERK

ORAL ARGUMENT REQUESTED

TABLE OF CONTENTS AND POINTS AND AUTHORITIES

NATURE OF THE CASE

Keiron K. Sneed, petitioner-appellant, appeals from the judgment of the Appellate Court, Fourth Judicial District, reversing the trial court's denial of the State's motion to compel production of a cellular phone passcode. (R. 44-45); *People v. Sneed*, 2021 IL App (4th) 210180, ¶ 108. No issue is raised challenging the charging instrument.

ISSUES PRESENTED FOR REVIEW

I.

Whether there was no jurisdiction for the State to appeal under Rule 604(a)(1) where the trial court's denial of the State's motion to compel did not have the substantive effect of quashing the search warrant or suppressing evidence, and the impairment of the State's case is questionable.

II.

Whether the trial court correctly denied the State's motion to compel production where permitting such compulsion would violate Keiron Sneed's constitutional right against self-incrimination, and the foregone conclusion exception cannot be applied to bypass that constitutional right.

CONSTITUTIONAL PROVISIONS, STATUTES, AND RULES INVOLVED

Constitution of the United States of America, Amendment V

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Constitution of the State of Illinois, Article I. Bill of Rights

Section 10. Self-Incrimination and Double Jeopardy

No person shall be compelled in a criminal case to give evidence against himself nor be twice put in jeopardy for the same offense.

Illinois Supreme Court Rule 604. Appeals from Certain Judgments and Orders

(a) Appeals by the State.

(1) *When State May Appeal***.** 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; arresting judgment because of a defective indictment, information or complaint; quashing an arrest or search warrant; or suppressing evidence.

STATEMENT OF FACTS

Keiron Sneed was arrested and charged with two counts of forgery. (C. 5-6, 8) The State obtained a search warrant for cellular phones taken from Mr. Sneed and his wife Allora, and then moved to compel Mr. Sneed to provide a passcode for one of the phones. (Supplement, C. 12-19) The trial court denied the motion (R. 44-45), but the State appealed (C. 31), and the appellate court reversed. *People v. Sneed*, 2021 IL App (4th) 210180, ¶ 108. Mr. Sneed now appeals the judgment of the appellate court.

Arrest and Search Warrant

According to a search warrant complaint signed by Clinton Police Detective Todd Ummel, Officer Alex Lovell was contacted by Sara Schlesinger, a bookkeeper for Dairy Queen, and told that she found a paycheck for Keiron Sneed, who was not an employee of Dairy Queen, which was cashed by mobile deposit, and the amount of the check was drawn from the Dairy Queen account. (Supplement, p. 1) Schlesinger later provided a second check, similarly deposited. (Supplement, p. 2) Schlesinger informed Lovell that Allora Sneed was an employee, and gave Lovell text messages between herself and Allora. (Supplement, p. 1) The complaint quoted the messages, which said that "he" did not think it would work, did not get the money, did not have a bank card, and Allora did not know about it. (Supplement, p. 1) The complaint further said the "information provided to Schlesinger was turned over to" Ummel, who attempted to interview Allora, but was unsuccessful. (Supplement, pp. 1-2)

Keiron and Allora Sneed were arrested (R. 8-9), and Mr. Sneed was charged with two counts of forgery. (C. 5-6) Both posted bond and, along with other personal information, Mr. Sneed wrote a phone number on the bond sheet. (R. 9, C. 11) Ummel sought and obtained a search warrant for two phones taken from the Sneeds (R. 9-10), stating in the complaint that police wished to confirm who deposited the forged checks, determine if any additional forged checks were deposited, and confirm the messages from Allora came from her phone. (Supplement, p. 2)

The warrant authorized the search of the two phones already in police custody, and the seizure of evidence related to the Dairy Queen transactions and any other forged checks. (Supplement, p. 3) This included photographs and records about the checks, messages about the checks, confirmations of deposits from banks, and other communications (e-mails, messages, notifications) about the deposit of checks. (Supplement, p. 3)

State's Motion to Compel

Four days after receiving the warrant, the State filed a motion to compel production of a passcode for one of the seized phones, stating that the phones were password protected. (Supplement, p. 3, C. 12-13) The State asserted that there was a split in authority over whether a passcode was testimonial for purposes of the privilege against self-incrimination. (C. 15) But it argued that it had satisfied the "foregone conclusion" exception to the privilege, by establishing either that the phone it sought to unlock had been in Mr. Sneed's possession, or, under the reasoning of *People v. Spicer*, 2019 IL App (3d) 170814, it had identified the phone's contents with reasonable particularity. (C. 17, 19) The State also argued that production was not incriminating where it had established the phone's ownership. (C. 17)

Defense counsel filed a response, arguing that the State merely speculated as to what might be found on the phone. (C. 25) Counsel argued the only Illinois precedent was *Spicer*, which found that to compel the production of a passcode the State had to meet the foregone conclusion exception by showing that it knew what information could be found on the phone. (C. 26) Because the State only speculated on what might be found, compelled production would violate Mr. Sneed's Fifth Amendment protection against self-incrimination. (C. 27)

Testimony of Detective Ummel

At the hearing on the motion to compel, in addition to asking that the trial court take judicial notice of the search warrant (R. 14-15), the State presented testimony from Detective Ummel. (R. 4). Ummel testified to the information from the search warrant complaint, stating

that Officer Lovell received information from Schlesinger about the cashed checks, and that he was provided information about text messages from Allora. (R. 4-6) Ummel said it was his understanding that a check could be photographed and sent to a financial institution electronically, and that the messages from Allora admitted that Mr. Sneed cashed the checks, though he did not think they would be deposited and it was a joke. (R. 5, 6) Ummel reviewed pictures of the cashed checks (R. 6), and saw that the signature endorsing the checks read as "Keiron Sneed." (R. 7) He did not witness Mr. Sneed sign the checks, or compare the signatures to other checks or Mr. Sneed's driver's license. (R. 10-11)

Ummel said the Sneeds were arrested (R. 8-9), and police took a cellular device from each of them. (R. 9-10) They posted bond, and the phone number Mr. Sneed put on his bond sheet matched the number of the phone that was seized. (R. 9) Ummel had not been able to access the seized phones, as they were locked by security passcodes that Allora and Mr. Sneed would not provide. (R. 7-8) Ummel said he was being cautious, because he thought too many failed attempts could permanently lock the phones. (R. 8) When asked if anyone else could help crack the phones, he said the Illinois State Police (ISP) had been utilized in the past, but without the security codes he thought it was unlikely, and said they did not usually assist if it did not involve narcotics. (R. 8) The Clinton Police Department did not have a cell phone cracking department of its own, so he would have to submit it to an outside agency. (R. 8)

Ummel said he thought it was likely there was evidence on the phone because a mobile deposit was used. (R. 12) He obtained a search warrant for the cellular phones of Allora and Mr. Sneed because he believed there was evidence on those phones "nonetheless indicating a photograph of the checks" and "communication between Mr. Sneed and his wife and Dairy Queen management." (R. 7) He hoped to gain access to the phone to see whether there were files about the deposited checks, but did not know if they existed. (R. 11) He had not subpoenaed the bank or the cellular carrier for records related to the transactions or messages. (R. 11-12)

When the court asked if there was anything in his investigation, like the bank or Dairy Queen records, that showed that the mobile device associated with the transaction was the same as the device subject to the State's motion, Ummel said he hoped to find a photograph from the deposit, but "I guess I don't know at this time." (R. 12-13) He did not believe there was anything tying Mr. Sneed to these transactions other than Allora's statements, but was inferring that the phone was used because of the mobile deposit. (R. 14)

Denial of the Motion to Compel

The next day, the court heard argument on the motion to compel. (R. 22-24) The State argued that disclosure of a passcode was not protected because it was not testimonial (R. 24-26); that *Spicer* was wrong and the foregone conclusion exception should focus on the passcode instead of the contents of the phone (R. 28-30); and even under *Spicer* it had shown that it was seeking particular evidence. (R. 30-34) The State also said it was open to being barred from using the act of producing the passcode against Mr. Sneed. (R. 30-31) Defense counsel argued that under *Spicer* the foregone conclusion exception was focused on the documents the State wanted to obtain, and while Ummel said he thought there might be evidence, he did not know it existed and took no steps to confirm it existed. (R. 34-37) Counsel also suggested it was not shown that pictures for a mobile deposit application would be stored on the phone, but the State asked the court to disregard this because there had not been evidence presented on how mobile deposits work outside Ummel's testimony. (R. 37)

The court held that, under *Spicer*, disclosure was considered testimonial (R. 38-40), and the focus of the foregone conclusion exception was on the information protected by the passcode. (R. 40-41) The court recognized that a search warrant was issued, was not challenged, and entitled police to the contents of the phone. (R. 41-42) But, based on the distinction between the Fourth and Fifth Amendment focuses, the foregone conclusion exception had a higher threshold than probable cause. (R. 42) The court found that Ummel's testimony did not establish

a link between the phone at issue and the electronic transaction, and assuming a relevant photo was on the phone would be speculation . (R. 43-44) While it did not believe this was a "mere fishing expedition," the State had not established particular knowledge of the existence of evidence, Mr. Sneed's possession of it, or that any evidence was more likely to be found on the phone at issue than on the other phone police seized. (R. 44) The court denied the motion to compel because the State had not shown that it knew evidence existed, was possessed by Mr. Sneed, and was authentic (R. 44-45)

The State filed a notice of appeal and a certificate of impairment. (C. 31, 33) It claimed the court's ruling suppressed evidence and quashed the search warrant by preventing it from acquiring evidence, which substantially impaired its ability to prosecute the case. (C. 31)

Appeal

On appeal, the Fourth District determined there was jurisdiction where it found that an order denying a motion to compel the decryption of a phone was like an order suppressing evidence, accepting the State's certificate attesting that the trial court's ruling "effectively" suppressed evidence and quashed the search warrant. *Sneed*, 2021 IL App (4th) 210180, ¶¶ 32-34. The court then found the trial court's denial of the motion to compel was incorrect for two independent reasons: (1) providing entry to a phone is not compelled testimony within the meaning of the Fifth Amendment, *id*., ¶ 63, and (2) the proper focus of the forgone conclusion exception is on the passcode itself, *id*., ¶¶ 85-87, which the State met by showing a passcode existed, that Mr. Sneed had possession of the phone, and the passcode would be authenticated when entered into the phone. *Id*., ¶¶ 98-102. The appellate court reversed the trial court's judgment and ordered remand for further proceedings. *Id*, ¶ 108.

This Court granted leave to appeal on March 30, 2022.

ARGUMENT

I.

There was no jurisdiction for the State to appeal under Rule 604(a)(1) where the trial court's denial of the State's motion to compel did not have the substantive effect of quashing the search warrant or suppressing evidence, and the impairment of the State's case is questionable.

The State lacks an appealable order in this case. After the trial court denied the State's motion to compel, the State filed a certificate of impairment stating that the order substantively suppressed evidence and quashed the search warrant. (C. 31) It then filed a notice of appeal stating that it was appealing from the certificate of impairment. (C. 33) However, the trial court's denial neither suppressed evidence nor prohibited the State from further pursuing its search warrant, and so lacked the substantive effect necessary to confer jurisdiction. The State's certificate also conflicts with its argument in the trial and appellate courts that the evidence it seeks is a foregone conclusion. Therefore, this Court should reverse the appellate court's decision finding jurisdiction, and affirm the trial court's order denying the motion to compel.

Standard of Review

The determination of jurisdiction under Illinois Supreme Court Rule 604(a)(1) is a legal question that is reviewed *de novo*. *People v. Lee*, 2020 IL App (5th) 180570, ¶ 8; *People v. Drum*, 194 Ill. 2d 485, 488 (2000).

Authorities and Analysis

In a criminal case, the State is permitted to appeal only a limited class of rulings defined by this Court. Ill. S. Ct. R. 604(a)(1). The authority to proscribe State appeals rests solely with this Court, and whether a particular order is appealable depends on this Court's construction of Rule 604(a)(1). *People v. Young*, 82 Ill. 2d 234, 239 (1980). Therefore, "[t]he threshold question to be considered here is whether the circuit court's ruling is appealable under Rule 604(a)(1)—at all." *In re K.E.F.*, 235 Ill. 2d 530, 537 (2009). Under that rule, the State is only permitted to appeal from a judgment that has the substantive effect of, among other results, "quashing an arrest or search warrant; or suppressing evidence." Ill. S. Ct. R. 604(a)(1).

The State's ability to appeal is further limited to those orders which substantially impair its prosecution. See, e.g., *Young*, 82 Ill. 2d at 247. As such, it is required to file a certificate of impairment, averring that the trial court's order "substantially impairs [its] ability to prosecute the case." *People v. Carlton*, 98 Ill.2d 187, 193 (1983). While a reviewing court may rely on the good faith evaluation of the prosecutor with regard to impairment, *People v. Keith*, 148 Ill. 2d 32, 39-40 (1992), "[b]efore that principle even comes into play***the order must, in fact, be one that suppresses evidence." *People v. Truitt*, 175 Ill. 2d 148, 152 (1997), *abrogated in part on other grounds*, *People v. Miller*, 202 Ill. 2d 328, 333-35 (2002).

Here, the trial court's denial of the State's motion to compel did not have the substantive effect of quashing the search warrant or suppressing evidence. In explaining its ruling, the trial court specifically recognized that a search warrant had been issued, that the defense had not challenged the warrant itself, and that law enforcement was allowed to obtain the contents of the phone. (R. 41-42) Far from invalidating the warrant, this pronouncement acknowledged the continuing effect of the warrant, and the State's authority to search the contents of the phone it had seized. Moreover, the court made no suggestion that the State would be barred from presenting any evidence at trial, including any evidence it might ultimately be able to cull from the seized phone. (R. 38-45) The sole effect of the court's ruling was to refuse the State's request that Mr. Sneed be forced to provide access to the phone. (C. 19, R. 45) Stated another way, it limited only the *means* by which the State could pursue the search warrant.

This Court's decision, *In re K.E.F.*, and the Fifth District's decision in *People v. Lee*, are instructive here. In both cases the State attempted to admit into evidence the prior video taped statements of minors who were also witnesses, and in both cases the trial courts ruled that the videos were not admissible as offered. *In re K.E.F.*, 235 Ill. 2d at 533-35; *Lee*, 2020 IL App (5th) 180570, ¶¶ 3-6. In particular, both trial courts ruled that the State had not met the

statutory burden for admitting that evidence, by refusing to question a witness about the events on which her statements were made in *K.E.F.*, 235 Ill. 2d at 539-40, and by failing to present sufficient evidence of reliability in *Lee*, 2020 IL App (5th) 180570, ¶ 6.

In finding the order from *K.E.F.* was not appealable by the State, this Court explained that evidence is considered suppressed under Rule 604(a)(1) when the trial court prevents it from being presented to the fact finder. *In re K.E.F.*, 235 Ill. 2d at 538. This was not what the trial court's order did, as the trial court would have allowed the State to admit the video had it simply questioned its witness about the substance of the statement as required by statute. *Id*. at 539-40. This Court concluded that "the sole impact of the circuit court's order [was] on the *means* by which the information [was] to be presented. That [was] not suppression of evidence." *Id*. at 540 (emphasis in original), relying on *Truitt*, 175 Ill. 2d at 152.

The court in *Lee* determined that this conclusion was "at the heart of the jurisdictional question" being presented. *Lee*, 2020 IL App (5th) 180570, ¶ 22. Where the trial court's ruling left the State with another option for presenting the information it sought to present (live testimony), there was no meaningful distinction from the *In re K.E.F.* decision. *Id*., ¶ 23. Further, the court rejected the State's argument that the video statements served a separate purpose from live testimony, as even if they might be "more impactful" they were not "the only means available" for presenting the relevant information. *Id*., ¶¶ 13-14. The court also found that the "mere possibility" of a witness freezing on the stand or otherwise becoming unavailable could not change an otherwise unappealable order, which only impacted the means of presenting information, into an appealable one that suppressed evidence. *Id*., ¶ 16.

Similarly in this case, the trial court's ruling only addressed the means by which the State could pursue its prosecution of Mr. Sneed. (R. 45) The court did not issue any order that would prevent the State from pursuing other avenues to obtain the evidence it sought, and actually acknowledged the continued validity of the search warrant. (R. 41-42) The possibility that obtaining any potential evidence may be somewhat more difficult does

not transform this ruling into an appealable order, particularly where the State can pursue the evidence it is hoping to obtain by other means. See *Lee*, 2020 IL App (5th) 180570, ¶ 16. Detective Ummel's testimony suggested that he could have attempted to access the device further himself, and though Clinton Police did not have cell phone cracking capability, he could submit the phone to an outside agency. (R. 7-8) He further testified that he had not even attempted to obtain records about the relevant bank deposits or messages from Citibank or the cell phone carrier. (R. 11-12) Thus, the State had other avenues to seek the evidence it speculated was available, and it was not foreclosed from pursuing it.

Neither did the court's order have the effect of suppressing evidence, as it made no ruling at all on the ultimate presentation of any evidence to the trier of fact. (R. 38-45) Indeed, it would be impossible for the court to make any such ruling, as the State's evidence, consisting entirely of Ummel's testimony, did not establish the actual existence of any particular files or information that it knew could be found on the seized phone. (R. 11, 12-14, 43-44) Without a particular item of evidence to suppress, there is simply no way that the court's ruling could have the effect of suppressing evidence.

However, on appeal, the Fourth District agreed with the jurisdictional decision of the Third District in *People v. Spicer*, 2019 IL App (3d) 170814, accepting at face value the State's bare assertion in its certificate of impairment that the order denying compulsion had the effect of suppressing evidence. *People v. Sneed*, 2021 IL App (4th) 210180, ¶¶ 32-34 (citing *Spicer*, 2019 IL App (3d) 170814, ¶ 11). While *Spicer* is factually similar (as applicable to Argument II, *infra*), its jurisdictional decision primarily relied on the Third District's previous decision in *People v. Krause*, 273 Ill. App. 3d 59, 61 (3d Dist. 1995). But *Krause* misinterpreted this Court's decision in *People v. Keith*.

In *Keith*, this Court determined that a trial court's ruling on a motion *in limine*, which prevented breath tests from being admitted into evidence, had the substantive effect of suppressing evidence. *Keith*, 148 Ill. 2d at 39. This Court did not defer to the State's certificate of impairment

in making this determination, but did find that it could rely on the State's certificate with regard to the impairment of its case, where the defendant argued that lack of the breath tests did not substantially impair the prosecution. *Id*. at 39-40. In *Krause* and *Spicer*, the Third District misinterpreted this as requiring reliance on the State's certificate as to the determination of the substantive effect of the lower court order. *Krause*, 273 Ill. App. 3d at 61; *Spicer*, 2019 IL App (3d) 170814, ¶¶ 11-12. However, *Krause* was decided in 1995, without the benefit of the guidance provided by this Court's more recent decision in *K.E.F.*

K.E.F. was decided in 2009, and is the more recent authority on this issue. *In re K.E.F.*, 235 Ill. 2d 530 (2009); *Keith*, 148 Ill. 2d 32 (1992). In *K.E.F.*, this Court clarified that whether an order or judgment is appealable is dependant on the substantive effect of the order rather than its form, and "[i]n making that determination, we do not defer to the parties or the circuit court." *In re K.E.F.*, 235 Ill. 2d at 538. The *Spicer* court relied on *Krause* without addressing the contrary holding in *K.E.F.*, *Spicer*, 2019 IL App (3d) 170814, ¶¶ 11-12, and the Fourth District did the same in this case by relying on *Spicer*. *Sneed*, 2021 IL App (4th) 210180, ¶¶ 32-34. But under *K.E.F.*, the appellate court should not have relied on the simple assertions in the State's certificate to determine the substantive effect of the trial court's order under Rule 604(a)(1). *In re K.E.F.*, 235 Ill. 2d at 538. Neither of the appellate courts' decisions, here or in *Spicer*, addressed this Court's decision in *K.E.F.*, and their uncritical reliance on the State's bare certificate is directly contrary to *K.E.F.*

It is also notable that any impairment to the State's case is questionable at best. While a reviewing court is certainly permitted to rely somewhat on the State's certificate as to the issue of impairment, *Keith*, 148 Ill. 2d at 39-40, it does not seem necessary for a court to abandon logic in doing so. Here, the State's assertion of impairment is inconsistent with its position, and the Fourth District's determination, that the evidence it is seeking (whether the passcode itself or some hoped for file within the phone) is a foregone conclusion (*Sneed*, 2021 IL App (4th) 210180, ¶¶ 65-66; see also sub-arguments II.C. and D., *infra*). If evidence is considered

a foregone conclusion, by definition, "it 'adds little or nothing to the sum total of the Government's information,' [and] the fifth amendment does not protect" the act of producing it. *Spicer*, 2019 IL App (3d) 170814, ¶ 15 (quoting *Fisher v. United States*, 425 U.S. 391, 411 (1976)). If the information the State is after would add little or nothing to its case, denying its production cannot possibly constitute a substantial impairment.

Regardless of any impairment to the State's case, the appellate court erred in relying on the certificate of impairment to determine the substantive effect of the order. *Sneed*, 2021 IL App (4th) 210180, ¶¶ 32-34. Because the trial court's ruling did not have the substantive effect of either quashing the search warrant or suppressing any evidence, this Court should reverse the decision of the appellate court finding jurisdiction, and affirm the trial court's order denying the motion to compel. See *In re K.E.F.*, 235 Ill. 2d at 540-41; *Lee*, 2020 IL App (5th) 180570, ¶¶ 23-24.

II.

The trial court correctly denied the State's motion to compel production where permitting such compulsion would violate Keiron Sneed's constitutional right against self-incrimination, and the foregone conclusion exception cannot be applied to bypass that constitutional right.

The trial court did not err when it denied the State's motion to compel Mr. Sneed to provide the passcode to a cell phone the police had seized. This ruling was correct because the act of producing a passcode is protected by the Federal and State constitutional rights against self-incrimination where it would involve delving into the contents of Mr. Sneed's mind. The State cannot overcome those rights using the foregone conclusion exception, which should not be applied to passcode production. Moreover, it failed to present sufficient evidence to establish, with reasonable particularity, that it actually knew of the existence, possession, and authenticity of the evidence it was seeking, such that the evidence could be considered a foregone conclusion, if that exception were applicable. As such, permitting compulsion would violate Mr. Sneed's constitutional rights, and the trial court properly denied the State's motion. Therefore, Mr. Sneed requests that this Court reverse the appellate court's decision, and affirm the trial court's denial of the motion to compel.

Standard of Review

Whether the constitutional right against self-incrimination is applicable is a question of law generally reviewed *de novo*. *People v. Spicer*, 2019 IL App (3d) 170814, ¶ 14. This Court should not utilize the foregone conclusion exception at all (see sub-argument II.B., *infra*). But if this Court determines that the foregone conclusion exception can be applied in cases involving the production of cellular phone passcodes, the standard of review should be bifurcated. "Whether the existence of documents is a foregone conclusion is a question of fact[.]" *United States v. Norwood*, 420 F.3d 888, 895 (8th Cir. 2005); *United States v. Doe*, 465 U.S. 605, 613-14 (1984) (*hereinafter "Doe I"*) The trial court here, in concluding that the State did not have the requisite knowledge to make the evidence it sought a foregone conclusion, made

findings of fact. (R. 42-45) The trial court's ruling should be construed similarly to an order affecting discovery, and its factual findings reviewed for an abuse of discretion, while the ultimate legal question of whether the privilege against self-incrimination applies is reviewed *de novo*. See *Mueller Industries, Inc., v. Berkman*, 399 Ill. App. 3d 456, 463 (2d Dist. 2010), *abrogated on other grounds by*, *People v. Radojcic*, 2013 IL 114197. Under this bifurcated standard, the trial court's factual findings are given great deference, and should only be reversed if they are against the manifest weight of the evidence. See *In re G.O.*, 191 Ill. 2d 37, 50 (2000).

Authorities and Analysis

The U.S. and Illinois constitutions provide that no person "shall be compelled in any criminal case to be a witness against himself" or to "give evidence against himself[.]" U.S. Const., amend. V; Ill. Const. 1970, art. I, § 10. The Illinois privilege has received the same general construction as the federal Fifth Amendment. *People ex rel. Hanrahan v. Power*, 54 Ill. 2d 154, 160 (1973). But this Court has also found that the rights protected by the privilege can be more broad under the State constitution in some cases. See, e.g., *People v. McCauley*, 163 Ill. 2d 414, 423-25, 439-40 (1994) (finding police were not permitted to deceive custodial suspects about counsel's presence or prevent counsel from assisting clients under the State guarantee against self-incrimination). Thus, in construing State guarantees, federal authorities are not precedential, and "merely guide the interpretation of State law." *McCauley*, 163 Ill. 2d at 436.

Other jurisdictions, and legal scholars, have disagreed on the extent to which passcode production falls under the protection of the privilege, and under what conditions the foregone conclusion exception applies. See *People v. Spicer*, 2019 IL App (3d) 170814, ¶¶ 16-17 (collecting cases), and *In the Matter of a Search Warrant Application for the Cellular Telephone in United States v. Barrera*, 415 F. Supp. 3d 832, 838 (N.D. Ill. 2019) (collecting cases); see also Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 Tex. L. Rev. 767 (2019) (arguing that the act of entering a passcode is testimonial but not

protected where the government can independently show the person knows the passcode), and Laurent Sacharoff, *What am I Really Saying When I Open my Smartphone? A Response to Orin S, Kerr*, 97 Tex. L. Rev. Online 63 (2019) (arguing that production is testimonial and the government must show it knows the person has the files it is seeking to obtain from the locked device).

The Third District determined in *Spicer* that the production of a passcode is protected by the privilege, the foregone conclusion exception is focused on the evidence sought behind the passcode wall, and the State had not met the exception without a sufficient particularized description of the information it wanted. *Spicer*, 2019 IL App (3d) 170814, ¶¶ 19-22. In contrast, the Fourth District here held that passcode production was not sufficiently testimonial to be protected, the focus of the exception was on the passcode itself, and the State met its burden by showing knowledge of: the passcode's existence, that it would be self-authenticating, and possession of the phone. *People v. Sneed*, 2021 IL App (4th) 210180, ¶¶ 63, 85-87, 98-102.

The Fourth District's determination, that the production of a passcode to decrypt a phone is not testimonial, is wrong. Such production requires the use of a person's mind and the divulging of facts and information not already known. *Spicer*, 2019 IL App (3d) 170814, ¶¶ 19-21. The foregone conclusion exception should also not be extended to remove the protection of the constitutional privilege in this case. See *Commonwealth v. Davis*, 220 A.3d 534, 550-52 (Pa. 2019). However, even if the exception can be applied to passcode production, the proper focus is on the evidence the State seeks beyond the passcode wall, *Spicer*, 2019 IL App (3d) 170814, ¶¶ 21-22, and the trial court's determination that the State had not demonstrated sufficiently particularized knowledge of such evidence was not against the manifest weight of the evidence. (R. 43-45)

A. Providing a passcode to decrypt a device such as a cell-phone is an act of production subject to the constitutional right against self-incrimination, unless the foregone conclusion exception applies.

The Fifth Amendment privilege against self-incrimination protects a person from being incriminated by compelled testimony or communications. *Doe v. United States*, 487 U.S. 201, 207 (1988) (*hereinafter "Doe II"*). This protection "encompasses compelled statements that lead to the discovery of incriminating evidence even though the statements themselves are not incriminating and are not introduced into evidence." *United States v. Hubbell*, 530 U.S. 27, 37-38 (2000). Under this rubric, information derived from the compelled communication is protected alongside information that is directly obtained from the communication. See *Hubbell*, 530 U.S. at 41 (finding the relevant question was not whether the prosecution would use the actual response to a subpoena at trial, which would surely be prohibited, but whether it made "derivative use" of the disclosure to obtain indictment and prepare its case).

In addition to being compelled and incriminating, the U.S. Supreme Court has held that a communication must be testimonial to receive protection under the Fifth Amendment. *Doe II*, 487 U.S. at 207. This will almost always encompass verbal statements. *Id*. at 213-14. But an act of producing evidence has communicative aspects of its own, and as such can also fall under the protection of the privilege. *Fisher v. United States*, 425 U.S. 391, 409-10 (1976); *Doe II*, 487 U.S. at 209. The testimonial component was not always a recognized requirement of the Fifth Amendment. Indeed, in his concurring opinion in *United States v. Hubbell*, Justice Thomas argued that limiting the protection to testimonial evidence was reading the Fifth Amendment itself too narrowly, as there was evidence that the term "witness" historically meant a person who gives or furnishes evidence. *Hubbell*, 530 U.S. at 50-52 (Thomas, J., concurring). He argued that this broader understanding would be consistent with other provisions of the constitution, and that the court failed to consider this when limiting it to testimonial evidence in *Fisher*. *Id*. at 53-56.

The Illinois Constitution does not use the word "witness" at all, but prohibits compelling a person "to give evidence against himself[.]" Ill. Const. 1970, art. I, § 10. This language is broader than the Fifth Amendment, and this Court can interpret the State privilege as applying more expansively. See, e.g., *McCauley*, 163 Ill. 2d 414. However, the ultimate "touchstone" for whether an act of production falls under the protections of the privilege should be the same: whether the person is compelled to use "the contents of his own mind" to communicate facts, either explicitly or implicitly. *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1345 (11th Cir. 2012) (quoting *Curcio v. United States*, 354 U.S. 118, 128 (1957)); see also *Hubbell*, 530 U.S. at 43; *Doe II*, 487 U.S. at 210, footnote 9.

It is this touchstone which shows that the production of a passcode is protected by the right against self-incrimination. There is no manner in which Mr. Sneed could produce the passcode requested in this case (C. 19), without making use of the contents of his own mind and revealing facts not otherwise known. This is more akin to "telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox." *Hubbell*, 530 U.S. at 43; see also *Doe II*, 487 U.S. at 210, footnote 9. Based on this analysis, the Fourth District of the Florida Court of Appeals determined that production of a passcode was testimonial and protected by the privilege, *G.A.Q.L. v. State*, 257 So. 3d 1058, 1061-62 (Fla. 4th Dist. Ct. App. 2018), and the Third District of our Appellate Court, in *Spicer*, adopted this conclusion. 2019 IL App (3d) 170814, ¶¶ 19-20.

In the present case, however, the Fourth District incorrectly determined that passcode production is not protected where it does not require testimony within the meaning of the Fifth Amendment. *Sneed*, 2021 IL App (4th) 210180, ¶ 63. In particular, the court questioned the validity of what it called the "mental/physical" production dichotomy, in determining whether an act of production is protected by the privilege against self-incrimination. *Id.*, ¶ 50. It found this dichotomy originated with the key/combination analogy first stated in *Doe II*, 487 U.S. at 210, footnote 9, and 219 (Stevens, J., dissenting). *Sneed*, 2021 IL App (4th) 210180, ¶ 52-53.

It then went on to state its belief that, given the advancement of technology, a passcode is more like a key than a combination, or that the value of the key/combination analogy was diminished because a passcode blurred the lines between the two. *Id.*, ¶¶ 59-60.

The appellate court's decision incorrectly suggests that the mental/physical dichotomy, on which the protection of the privilege is based, came from the key/combination analogy and that the two are essentially synonymous. *Id.*, ¶¶ 52-53, 59. But the distinction between purely physical evidence production, and the production of evidence that communicates information from a person's mind, has much older roots than Justice Steven's analogy in *Doe II*. It was 1910 when the U.S. Supreme Court held that evidence a blouse fit a defendant was not protected, because the privilege against self-incrimination was protection against "compulsion to extort communications from [a person], not an exclusion of his body as evidence when it may be material."*Holt v. United States*, 218 U.S. 245, 252-53 (1910). Later, in 1957, the court held that a custodian of union records, while not protected from producing the association records, was protected from orally testifying about them, where doing so "requires him to disclose the contents of his own mind." *Curcio*, 354 U.S. at 128.

Schmerber v. California, 384 U.S. 757 (1966), later clarified this distinction. In holding that drawing blood was not protected, the U.S. Supreme Court explained that "[i]t is clear that the protection of the privilege reaches an accused's communications, whatever form they might take, and the compulsion of responses which are also communications[.]" *Schmerber*, 384 U.S. at 763-64. The relevant difference then, was between compelled communications or testimony and compulsion that makes the accused a "source of real or physical evidence[.]" *Id.*(internal quotation marks omitted) In drawing that distinction though, the court warned that it would not always be clear, and presented the example of lie detector tests, as ostensibly physical evidence that is in fact directed at obtaining an essentially testimonial response. *Id.*

This was the distinction recognized in *Fisher* in 1976, and the history which formed the basis for the court's determination that an act of producing evidence had communicative aspects of its own that could entitle it to the protections of the privilege. *Fisher*, 425 U.S. at 408-10. Ultimately, the core consideration that makes an act sufficiently testimonial is the use of the contents of a person's mind. See *In re Grand Jury Subpoena*, 670 F.3d at 1345. The key/combination analogy is simply an illustration of that principle, which encapsulates the protected nature of an act where it expresses what can only otherwise be found inside a person's head. See *Hubbell*, 530 U.S. at 43; see also *Doe II*, 487 U.S. at 210, footnote 9.

In questioning this core principle, the Fourth District cited with approval *State v. Andrews*, 243 N.J. 447 (2020) and *State v. Stahl*, 206 So. 3d 124 (Fla. 2d Dist. Ct. App. 2016), as cases that questioned the validity of the dichotomy between physical and mental acts of production where a cellular phone passcode is at issue. *Sneed*, 2021 IL App (4th) 210180, ¶¶ 56-60. In particular, the Fourth District asserted that a passcode was a string of letters or numbers entered more from muscle memory instead of conscious thought, and as such was more like producing a key, or could be considered to encompass both a key and a combination. *Id.*, ¶¶ 59-60.

However, neither *Andrews* nor *Stahl* ultimately held that production of a passcode was not testimonial. Indeed, the New Jersey Supreme Court held that it was testimonial where "[c]ommunicating or entering a passcode requires facts contained within the holder's mind***." *Andrews*, 243 N.J. at 478. Though the court stated that the testimonial value of a passcode was "minimal" where it did not have "independent evidentiary significance," the court still concluded that the act of producing one was testimonial and presumptively protected by the Fifth Amendment. *Id.* at 480.

In *Stahl*, the Second District of the Florida Court of Appeals suggested that producing a passcode alone would not be sufficiently testimonial because use of a person's mind was

not enough, instead the contents of the mind would need to be "extensive[ly] use[d]" to qualify as testimonial. *Stahl*, 206 So. 3d at 133-35 (citing *Hubbell*, 530 U.S. at 43; *Doe II*, 487 U.S. at 213) However, the *Stahl* court did not rest its decision on its musings about whether production was independently testimonial, but concluded that production of a passcode was not protected where the State had sufficiently established its knowledge of the *passcode's* existence, possession, and authenticity. *Id*. at 136-37. This conclusion itself is incorrect (see sub-argument II.C., *infra*), and at least three other districts of the Florida Appellate Court have rejected much of the *Stahl* court's analysis. See *G.A.Q.L.*, 257 So. 3d at 1063-64; *Pollard v. State*, 287 So. 3d 649, 656 (Fla. 1st Dist. Ct. App. 2019); *Garcia v. State*, 302 So. 3d 1051, 1055 (Fla. 5th Dist. Ct. App. 2020) *review granted by State v. Garcia*, Case. No. SC20-1419, 2020 WL 7230441. But with regard to the testimonial nature of producing the passcode, the *Stahl* court, and the Fourth District here, misinterpret the statement in *Doe II* that the content of a compelled communication must have testimonial significance. *Doe II*, 487 U.S. at 211, footnote 10.

In *Doe II*, the U.S. Supreme Court determined that a suspect's signing a consent directive, to allow a grand jury to obtain records from foreign banks, did not have testimonial significance. 487 U.S. at 203-6, 215-19. In so holding, the court said this was because signing the directive did not communicate any implicit or explicit factual assertions. *Id*. at 215. This determination was based heavily on the very narrow phrasing of the directive involved. The directive did not convey any statement about the existence of bank accounts, Doe's control over any such accounts, or the authenticity of any records produced; the banks would be the ones producing the records, and the directive did not exhibit actual consent because it would be compelled by court order. *Id*. at 215-16. The court concluded that signing the document was nontestimonial in the same fashion as a handwriting sample or voice exemplar, as it did not disclose "any knowledge he might have." *Id*. at 217 (quoting *U.S. v. Wade*, 388 U.S. 218, 222 (1967)).

This holding ultimately relied on whether Doe was making a disclosure that revealed the contents of his mind. In fact, responding to Justice Steven's key/combination analogy, the court agreed that "[t]he expression of the contents of an individual's mind is testimonial communication for purposes of the Fifth Amendment." *Doe II*, 487 U.S. at 210, footnote 9 (internal quotations marks omitted). Unlike the directive at issue in *Doe II*, or the compelling of a purely physical act, the production of a passcode inherently involves conveying facts through the use of a person's mind.

The Fourth District also suggested that production of the passcode would not be testimonial where it could be entered into the phone without being provided to police, relying on *United States v. Oloyede*, 933 F.3d 302, 308-9 (4th Cir. 2019). *Sneed*, 2021 IL App (4th) 210180, ¶ 61. In *Oloyede*, an FBI agent asked a suspect, Mojisola Tinuola Popoola, to unlock her phone, which she did without revealing the passcode. *Oloyede*, 933 F.3d at 308. On appeal, Popoola argued the district court had erred in denying her motion to suppress the contents of her phone where she was not advised of her *Miranda* rights. *Id.* In affirming the denial, the Fourth Circuit of the U.S. Court of Appeals stated that Popoola "had not shown that her act communicated her cell phone's unique passcode[,]" and that she used the "unexpressed contents of her mind" to enter the code herself. *Id.* at 309. However, the court did not affirm based on this consideration, but on its finding that Popoola's action in unlocking the phone was voluntary and uncoerced. *Id.* Ultimately, the court did not hold that the act of unlocking the phone was not testimonial, nor did it consider whether information beyond the passcode itself was communicated by that action. *Id.*

In contrast, the Eleventh Circuit Court of Appeals has considered this question, and concluded that the act of decrypting and producing a device could not be fairly characterized as a nontestimonial physical act. *In re Grand Jury Subpoena*, 670 F.3d at 1346. There, the

defendant, John Doe, was ordered to "produce the 'unencrypted contents' " of several hard drives that had been seized pursuant to a search warrant, but the full content of which investigators could not access due to encryption. *Id.* at 1339-40. Recognizing that the "touchstone" for the testimonial nature of an act was whether a person was compelled to use the contents of his own mind, *id.* at 1345, the Eleventh Circuit concluded that decryption and production would amount to testimony of Doe's: knowledge of the existence and location of potentially incriminating files; his possession, control, and access to the encrypted portions of the hard drives; and his capability to decrypt the files. *Id.* at 1346. As such, decryption and production of the contents of the hard drives was testimonial in nature. *Id.*

Other courts have similarly determined that the act of producing an unlocked smartphone is entitled to Fifth Amendment protection. In *Eunjoo Seo v. State*, 148 N.E.3d 952 (Ind. 2020) the Indiana Supreme Court reversed a trial court's contempt order issued after Seo refused to unlock her phone pursuant to the trial court's order, and held that compelling her to unlock her phone violated her right against self-incrimination. *Seo*, 148 N.E.3d at 953, 955. The court determined that, at a minimum, such production conveys that (1) the person knows the passcode, (2) the files on the device exist, and (3) the person has possession and control over those files. *Id.* at 955, 957. Thus, the suspect's compelled action still communicates to the State information it did not previously know and would fall under the protection of the privilege against self-incrimination, unless the State could show it already knew this information under the forgone conclusion exception (see sub-arguments II.B through D., *infra*). *Id.* at 957-58.

In sum, the compelled production of a cellular phone passcode is protected by the privilege against self-incrimination where it involves using the contents of a person's mind and conveys facts about that person's knowledge, possession, and control of the phone and its contents. *Spicer*, 2019 IL App (3d) 170814, ¶¶ 19-20; *G.A.Q.L.*, 257 So. 3d at 1061-63. Therefore, the

compelled production of a passcode from Mr. Sneed falls under the protection of the privilege against self-incrimination, and this Court should reverse the Fourth District's determination that this act is not sufficiently testimonial to merit protection.

Under *Fisher*, where an act of production has testimonial components, the protection of the privilege against self-incrimination is only removed where the evidence the State is seeking to obtain can be considered a "foregone conclusion." See *Fisher*, 425 U.S. at 411.

B. The foregone conclusion exception is a narrow exception that should not be applied to the production of a cellular phone passcode.

The court in *Spicer* addressed the foregone conclusion exception in determining whether or not the production of a passcode was protected. *Spicer*, 2019 IL App (3d) 170814, ¶¶ 15, 20-23. Under that exception, an act of production is not protected by the privilege against self-incrimination where the State can show "with 'reasonable particularity' that when it sought the act of production, the State knew the evidence existed, the evidence was in the defendant's possession and it was authentic." *Id*., ¶ 15 (citing *United States v. Greenfield*, 831 F.3d 106, 116 (2d Cir. 2016)). As mentioned briefly above (see Argument I, *supra*), where the State makes this showing, the evidence is considered a foregone conclusion because it "adds little or nothing to the sum total of the Government's information[.]" *Spicer*, 2019 IL App (3d) 170814, ¶ 15 (quoting *Fisher*, 425 U.S. at 411); see also *United States v. Fricosu*, 841 F.Supp.2d 1232 (D. Colo. 2012) (finding that it was a foregone conclusion that evidence was on a laptop based on a recorded conversation of the defendant and her husband in which defendant admitted the sought-after evidence was on the laptop). Thus, the contents of the defendant's mind are not used against him where "the government is in no way relying on the 'truth-telling' of the [defendant] to prove the existence of or his access to the documents." *Fisher*, 425 U.S. at 411.

Fisher's application of the foregone conclusion exception should not be extended to the circumstances of this case, where the State attempted to force Mr. Sneed to produce a passcode

through a motion to compel. (C. 12-19) The foregone conclusion exception was historically considered in cases where the government subpoenaed tax documents or business records. See *Fisher*, 425 U.S. 391; *Doe I*, 465 U.S. 605; *Hubbell,* 530 U.S. 27. Most courts that have utilized the exception to address circumstances involving the compelled production of a passcode, have done so without critically considering whether the exception should be extended to such situations. See, e.g., *Spicer*, 2019 IL App (3d) 170814, ¶ 15 and *Sneed*, 2021 IL App (4th) 210180, ¶¶ 65-66; see also *Fricosu*, 841 F.Supp.2d at 1236-37; *In re Grand Jury Subpoena*, 670 F.3d at 1346; *Commonwealth v. Gelfgatt*, 468 Mass. 512, 522-23 (2014); *Stahl*, 206 So. 3d at 135; *G.A.Q.L.*, 257 So. 3d at 1063.

One court that has considered the dangers of extending the exception is the Indiana Supreme Court in *Seo*, 148 N.E.3d at 958-62. The *Seo* court outlined three concerns with applying the foregone conclusion exception. First, production of an unlocked phone is significantly different from the production of specified business documents like those at issue in *Fisher* and it progeny, which involved summons or subpoenas seeking specific identified documents. *Id.* at 959. It is unlikely that, when *Fisher* introduced the exception in 1976, the court could possibly have imagined that it would be used to force defendants to unlock cell phones and electronic devices containing the wealth and breadth of information that modern devices are capable of holding. See *id.* at 959-60.

Second, considering the amount of information contained within modern phones to which access could be provided, the forgone conclusion exception is simply unworkable. *Id.* at 960. Though under the exception government should only be provided those files it can establish knowledge of with reasonable particularity, unlocking a phone does not provide those files, but broad access to the phone in its entirety. *Id.* Multiple issues arise from this access, including whether further compulsion would be necessary or appropriate where applications

within the phone are password protected, or where a cloud-storage service is installed which might contain hundreds or thousands of files previously unknown to law enforcement. *Id.* at 960-61. The complexity of this situation reveals that the exception is "a low-tech peg in a cutting-edge hole." *Id.* at 961.

Finally, the limited application of the foregone conclusion exception by the U.S. Supreme Court weighs against further extension. *Id.* As the Supreme Court has recently cautioned, "when confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents." *Carpenter v. United States*, 138 S. Ct. 2206, 2222 (2018) (citing *Riley v. California*, 573 U.S. 373, 386 (2014) ("A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in [prior precedents]")). Indeed, *Fisher* is the only U.S. Supreme Court decision in which the exception has ever been found to apply, and the only two cases to further discuss it (without applying it) did so in the context of grand jury proceedings involving subpoenas for the production of business and financial records. *Seo*, 148 N.E.3d at 961; *Doe I*, 465 U.S. at 606-08; *Hubbell*, 530 U.S. at 30-33. Where the exception was created in a "vastly different context," using it in the situation of modern cellular phones and electronic devices would significantly expand it, and result in a narrowing of the constitutional right. *Seo*, 148 N.E.3d at 962. While the *Seo* court still determined that the exception was further not applicable because the government had not sufficiently showed its knowledge of particular files to be found on the defendant's device, *id.* at 958, the Pennsylvania Supreme Court took these concerns a step farther.

In *Commonwealth v. Davis*, 220 A.3d 534 (Pa. 2019), the Pennsylvania Supreme Court refused to apply the foregone conclusion exception to the situation of the compelled production of computer passwords at all. *Davis*, 220 A.3d at 550-52. In that case, a defendant charged with distributing child pornography had admitted the computer involved was his, and that

only he knew the password. *Id*. at 537-39. In rejecting the applicability of the foregone conclusion exception, the court said that it would be a significant expansion of the rationale supporting the exception to apply it outside the context of business and financial records that had long been subject to compelled production. *Id*. at 549. Despite the added difficulty to the government, "[applying] the foregone conclusion rationale in these circumstances would allow the exception to swallow the constitutional privilege." *Id*. Therefore, the court concluded that compelling the password to a computer was a protected act and did not fit within the exception. *Id*. at 550-52.

Modern phones and computers contain an extraordinary amount of information, and compelling the production of a passcode compels production of all of that information, as opposed to specifically identified documents like those at issue in *Fisher* and its progeny. See *Seo*, 148 N.E.3d at 959. Thus, applying the foregone conclusion exception in this case risks allowing it to "swallow the constitutional privilege" just as surely as applying it to the computer passwords in *Davis* would have. *Davis*, 220 A.3d at 549. In applying the exception here, the Fourth District failed to critically examine its extension to the situation of passcode production, or take into account the manner in which doing so narrows the protections of the constitutional right against self-incrimination. *Sneed*, 2021 IL App (4th) 210180, ¶¶ 65-66. Indeed, its ultimate decision that the exception applies where the State has some partial knowledge about the mere existence of a passcode, *id.*, ¶¶ 98, demonstrates how drastically the right may be narrowed where the exception is utilized, and how cheaply the exception could treat the forced extraction of the contents of a person's mind. As such, this Court should conclude that the foregone conclusion exception does not apply to the compelled production of cellular phone passcodes.

C. If the foregone conclusion exception is applied to the production of a passcode, the appropriate focus of the exception is on the evidence the State is seeking to obtain through production.

The court in *Spicer*, and the Fourth District here, based their decisions, at least in part, on the application of the foregone conclusion exception, without considering whether it should

be expanded to the production of passcodes. *Spicer*, 2019 IL App (3d) 170814, ¶¶ 15, 20-23; *Sneed*, 2021 IL App (4th) 210180, ¶¶ 65-66. If this Court determines the exception should be considered, *Spicer* shows how it should be applied.

In determining whether the State had met the requirements of the exception, the *Spicer* court relied on *G.A.Q.L. v. State*. *Id.*, ¶¶ 19-21. In *G.A.Q.L.*, the Fourth District of the Florida Appellate Court found that the proper focus of the exception was not on the State's ability to show its knowledge of the passcode, but on its ability to show its knowledge of the evidence it was seeking beyond the passcode wall. *G.A.Q.L.*, 257 So. 3d at 1063. If applied to the passcode it would subject all passcode protected phones to compulsion based purely on the fact that they have a passcode, and such a rule "would expand the contours of the foregone conclusion exception so as to swallow the protections of the Fifth Amendment." *Id*. Thus, knowing that a passcode wall exists is not sufficient to meet the foregone conclusion exception; the State must instead "demonstrate with reasonable particularity that what it is looking for is in fact located behind that wall." *Id*. at 1063-64 (citing *In re Grand Jury Subpoena*, 670 F.3d at 1347). The court in *Spicer* adopted this conclusion, reasoning that what the State was seeking by compelling the passcode was not the passcode itself, but the information it would decrypt. *Spicer*, 2019 IL App (3d) 170814, ¶¶ 20-21.

This conclusion was similarly adopted by another district of the Florida Appellate Court in *Pollard v. State*. 287 So. 3d at 657. The courts in both *Pollard* and *G.A.Q.L.* rejected the reasoning of the court in *Stahl* (*G.A.Q.L.*, 257 So. 3d at 1063-64; *Pollard*, 287 So. 3d at 656-57), which is ultimately the same reasoning used by the Appellate Court here, in finding that the State satisfied the foregone conclusion exception by demonstrating its knowledge that there was a passcode. *Sneed*, 2021 IL App (4th) 210180, ¶¶ 98-102. But the court in *Pollard* recognized that the foregone conclusion test was tautological in its application to a passcode, because the fact of the passcode is shown by the need for it. *Pollard*, 287 So. 3d at 656. With regard

to authenticity, the *Stahl* court reasoned that a password was self-authenticating, because its authenticity would be proven as soon as it was entered. *Stahl*, 206 So. 3d at 136. However, the *Pollard* court explained that this logic was circular, and would not in fact show that a State had knowledge of a passcode's authenticity *before* the passcode was compelled, as required by the exception. *Pollard*, 287 So. 3d at 656. Ultimately, the Fourth District's decision in this case relies on the same flawed logic, essentially determining that compelled production is permissible simply because there is some need for it. See *Sneed*, 2021 IL App (4th) 210180, ¶¶ 98-102.

In addition to *Stahl*, the Fourth District here relied on the New Jersey Supreme Court's decision in *Andrews*, as support for its finding that the proper focus of the exception should be on the passcode itself. *Sneed*, 2021 IL App (4th) 210180, ¶¶ 83-87. However, *Andrews* relied on the same type of circular reasoning used in *Stahl* by ignoring the requirement that the State demonstrate the authenticity of the information it is seeking at the time it seeks production, and finding that some showing of possession of the phone at issue will be sufficient to establish a foregone conclusion. See *Andrews*, 243 N.J. at 480-81. This circular approach demonstrates the danger of trying to shoehorn the passcode production situation into the analysis of an exception traditionally applied to subpoenaed documents.

In *Fisher*, the exception was applied with a focus on the actual documents being produced by the taxpayers' otherwise testimonial act of production. *Fisher*, 425 U.S. at 411-13. Because the documents it was seeking were created by accountants, the government was not relying on the taxpayers' act of production to establish their existence or possession, as it had that information from the accountants. *Id*. at 411. The authentication prong of the exception was similarly applicable because the State had independent evidence of the documents' authenticity from the accountants who had actually created them. *Fisher*, 425 U.S. at 412-13. The whole focus was on the information the State had about the actual evidence it wanted to obtain.

If the foregone conclusion exception is to be applied to the production of a cellular phone passcode, it should similarly focus on the evidence the State is seeking to obtain by unlocking the phone. See *Spicer*, 2019 IL App (3d) 170814, ¶ 21.

The Fourth District's position, based on *Andrews*–that the exception applies to the passcode because there is a distinction between the act of production and the incriminating content of the documents or evidence, *Sneed*, 2021 IL App (4th) 210180, ¶¶ 83-89–confuses the content of the phone with the content of the evidence sought. In particular, the Fourth District cited to the statement in *Andrews* that "the act of production must be considered in its own right, separate from the documents sought." 243 N.J. at 471; *Sneed*, 2021 IL App (4th) 210180, ¶ 84. But this conclusion is based on a flawed reading of the U.S. Supreme Court's precedent involving the exception.

In creating the exception, the court in *Fisher* stated that the act of producing evidence has "communicative aspects of its own, wholly aside from the contents of the papers produced." *Fisher*, 425 U.S. at 410. However, it then went on to establish that the testimonial nature of turning over the tax documents involved was negated because the government had demonstrated specific knowledge about the existence and possession of those specific tax documents, because it had that information from the accountants that created them. *id.* at 410-11. Thus, the distinction the court was making was that the government did not need to know about the content of the documents, but it did need to know about the existence and possession of the specific documents that it was seeking.

This was the relevant distinction in the U.S. Supreme Court's decision about the foregone conclusion exception in *Hubbell*. There, the U.S. Supreme Court determined that the foregone conclusion exception did not apply where the government had not shown any prior knowledge of the existence or whereabouts of the 13,120 pages of documents that Hubbell produced in

response to the government's subpoena. *Hubbell*, 530 U.S. at 44-45. The court distinguished this from *Fisher*, where the government had knowledge that a group of tax payers' attorneys had possession of the tax documents at issue, and could independently confirm their existence and authenticity through the accountants that created them. *Id.* Though the court stated that the relevant "testimony" was that which was inherent in the act of producing the documents, not in the contents of the documents, *id.* at 40, its determination about the forgone conclusion exception was dependent on the government's knowledge about the existence and whereabouts of the documents themselves. *id.* at 44-45.

The Eleventh Circuit, in the case of *In re Grand Jury Subpoena* (discussed in sub-argument II.A., *supra*), applied this distinction in the context of passcode production and device decryption. The Eleventh Circuit distinguished the production of decrypted hard drives in that case from the case of *In re Boucher*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009). *In re Grand Jury Subpoena*, 670 F.3d at 1348-49. In *Boucher*, law enforcement had an opportunity to review the encrypted portion of a laptop drive which they could not open again after it was closed (the initial review included identifying a file with a name that suggested it contained child pornography), and they sought production of the unencrypted drive. *Id*. at 1348. In distinguishing that case, the Eleventh Circuit said "[t]he Government correctly notes that *Boucher* did not turn on the fact that the Government knew the contents of the file it sought***Fisher* and *Hubbell*, though, still require that the Government show its knowledge *that the files exist*." *Id*. (emphasis in original) This made it irrelevant that the Government knew what was in the file it identified, but "it was crucial that the Government knew that there existed a file under such a name." *Id*. at 1348-49.

The Eleventh Circuit similarly distinguished *United States v. Fricosu*, 841 F.Supp.2d 1232. There the Government was determined to have the requisite knowledge of the existence of the evidence it sought on a laptop, because it had a recording of a phone conversation in

which Fricosu admitted the content at issue existed and was on the laptop. *In re Grand Jury Subpoena*, 670 F.3d at 1349, footnote 27. In contrast, where the Government did not know whether there were any specific files on the encrypted hard drives at issue, the foregone conclusion exception did not apply. *Id.* So, while the State's knowledge about the content of the evidence it seeks is irrelevant, this is because what it must establish under the foregone conclusion exception is knowledge of the existence, possession, and authenticity of that specific evidence.

This analysis is not altered by the existence of a search warrant, and does not somehow negate or supercede the effect of the Fourth Amendment. Here, the Fourth District asserted that focusing the foregone conclusion exception on the contents of the phone would allow the Fifth Amendment to swallow the Fourth, because the Fourth Amendment protects the contents of the phone, and the Fifth Amendment should not be used to prevent the operation of the Fourth. *Sneed*, 2021 IL App (4th) 210180, ¶¶ 91-95. However, this reasoning flips the purpose of the amendments on their head. Contrary to the court's implication, *id.*, ¶ 91, the Fourth Amendment does not give the State a right to anything, it protects the inherent rights of individuals against unreasonable searches and seizures, a protection the State can only overcome by making the appropriate showing of reasonableness. U.S. Const., amend. IV; see *People v. McCavitt*, 2021 IL 125550, ¶¶ 55-57; *Ohio v. Robinette*, 519 U.S. 33, 39 (1996) ("the touchstone of the Fourth Amendment is reasonableness" (internal quotation marks omitted)).

Here, the trial court's order denying compulsion did not prevent the operation of the Fourth Amendment protection at all. The trial court explicitly acknowledged in its ruling that it had issued a search warrant and that the State could obtain the evidence it was seeking under that warrant. (R. 41-42) The trial court simply concluded that this creature of the Fourth Amendment, did not affect the determination of Mr. Sneed's separate right against self-incrimination pursuant to the Fifth Amendment. (R. 42-43) The correctness of the trial court's decision is demonstrated by the discussion in *Fisher* of the differences between the protections

of the two amendments. There, the U.S. Supreme Court explained that, while privacy was one of the purposes served by the Fifth Amendment, its protections focused on compelled testimonial self-incrimination, and it was not violated by every invasion of privacy otherwise contemplated in the Fourth Amendment. *Fisher*, 425 U.S. at 399. The court said:

> "If the Fifth Amendment protected generally against the obtaining of private information from a man's mouth or pen or house, its protections would presumably not be lifted by probable cause and a warrant***the Fifth Amendment's strictures, unlike the Fourth's, are not removed by showing reasonableness." *Id*. at 400.

In other words, the analysis of the propriety of searches under the Fourth Amendment is separate from the analysis of compelled self-incrimination under the Fifth Amendment. But this does not mean that the protections do not ever overlap. Though the Fifth Amendment does not protect against the disclosure of private information simply because it is private, it does protect against the disclosure of private information where the act of disclosure is obtained through compelled self- incrimination. See *id.* at 401 ("Insofar as private information *not obtained through compelled self-incriminating testimony* is legally protected, its protection stems from other sources ***." (Emphasis added)). Thus, the fact that the State had a warrant here has no bearing on whether the act of producing the passcode is separately entitled to protection under the privilege against self incrimination. In an effort to tidily separate the Fourth and Fifth Amendment rights, the Fourth District's decision here dissolves Mr. Sneed's Fifth Amendment rights completely, making them subservient to the State's Fourth Amendment showing of reasonableness, instead of protecting them as distinct and equal rights.

Focusing the forgone conclusion exception on the existence, possession, and authenticity of the specific evidence the State is seeking through the act of production does not somehow negate the Fourth Amendment's separate protection on the contents of a phone generally.

Rather it appropriately places the focus on the information communicated by the act of unlocking the phone. In *Seo*, the Indiana Supreme Court reasoned that unlocking a phone involves a broad spectrum of communication, at least including knowledge of the password, the existence of the files on the device, and the possession of those files. *Seo*, 148 N.E.3d at 955, 957. It noted that the U.S. Supreme Court cases interpreting acts of production linked the physical acts of handing over documents to the documents ultimately produced. *Id*. at 957. In this way entering the password for a phone is analogous to physically handing over documents, and the files on the phone are analogous to the documents ultimately produced. *Id.* Based on this, the foregone conclusion exception did not apply where the State did not demonstrate that any particular files existed on the device or that Seo possessed them, and providing access to the device would give the State information it did not already know. *Id*. at 958.

Should the foregone conclusion exception be used in this case, *Seo* demonstrates that the proper application in the context of producing a passcode to unlock a phone, is to look at the State's knowledge of the files actually being sought within the phone. *Id*. at 957-58. Contrary to the Fourth District's position that the Fifth Amendment analysis should be focused only on the passcode itself, *Sneed*, 2021 IL App (4th) 210180, ¶ 93, unlocking a phone conveys information not just about the passcode, but about the information contained in the phone. *Seo*, 148 N.E.3d at 955, 957. Moreover, historical use of the exception always considered the link between the act of production and the actual documents ultimately produced by that act. See *id*. at 955-57.

If the foregone conclusion exception is to be applied to cases involving the production of a passcode for an electronic device, this is the approach that must be taken to avoid improperly narrowing the protections of the privilege against self-incrimination. See *G.A.Q.L.*, 257 So. 3d at 1063. The court in *Spicer* took this position, and the focus in this case should similarly be on whether the State demonstrated its knowledge of the specific evidence on the phone that it is seeking to obtain. See *Spicer*, 2019 IL App (3d) 170814, ¶ 21.

D. The foregone conclusion exception is not applicable here where the State had not established that it knew, at the time production was requested, of the existence, possession, and authenticity of the information it sought within the phone.

In order to establish that the foregone conclusion exception applied in this case, the State was required to demonstrate that it knew the evidence it was looking for existed, was in Mr. Sneed's possession, and was authentic. *Spicer*, 2019 IL App (3d) 170814, ¶ 15. It had to demonstrate this with "reasonable particularity" as of the time it sought the act of production. *Id.* As established above (sub-argument II.C., *supra*) the evidence it needed to demonstrate that it had independent knowledge about, is the evidence it was seeking within the phone. *Id.*,¶ 21. *Spicer* is instructive.

In *Spicer*, the State did not meet this requirement where it had not shown that it knew about evidence on Spicer's phone. *Id*., ¶ 22. After recovering a phone from Spicer during an arrest for drug offenses, police obtained a search warrant for the phone seeking information including call logs, messaging records, internet history, and GPS data. *Id*., ¶¶ 5-6. The State moved to compel the production of the passcode after Spicer refused to provide it and police attested in a hearing, and in the affidavit for the search warrant, that they believed the phone had evidentiary value because drug dealers use cell phones to further unlawful conduct. *Id*., ¶¶ 4-6 The trial court took judicial notice of the warrant but ultimately denied the motion. *Id*., ¶ 7. The Appellate Court affirmed, finding that the State did not know what information was on Spicer's phone. *Id*., ¶ 22. Where it had not provided a particularized description of such information, or evidence that any useful information actually existed, the State was engaging in a fishing expedition, and the foregone conclusion exception did not apply. *Id.*

Here, the State similarly did not present any evidence to establish that it clearly knew about the existence of specific documents or information on the seized phone. While Ummel testified that the fraudulent checks were cashed by mobile deposit (R. 5), he did not actually

know what if any records might be found on either of the seized phones, and was hoping to gain access so he could find out whether there were any files related to the mobile deposit. (R. 11) When asked if there was any other documentation tying the deposit to Mr. Sneed's phone, he said he was hoping to find a photo, but he did not know. (R. 12-13) Indeed, Ummel even said he did not believe there was anything tying Mr. Sneed to the transaction beyond his wife's statements to Dairy Queen, and was simply "inferring" that the phone at issue was used because of the mobile deposit. (R. 14) The trial court found that Ummel's statements did not establish the requisite knowledge of evidence on the phone. (R. 43-44)

As to possession, Ummel's most explicit statement about what he was hoping to find–a photograph of the checks and communications between the Sneeds and Dairy Queen management–was about what he thought he might find on *either* of the two seized phones. (R. 7) The trial court noticed this distinction, as it ultimately ruled that even if the State might have demonstrated knowledge that some evidence would be found on one of the phones, it could not find that it was more likely to be on the phone seized from Mr. Sneed, than on the one seized from his wife. (R. 44) As a factual matter, the State did not establish reasonably particularized knowledge of Mr. Sneed's possession of any evidence.

Without establishing knowledge of the existence or possession of particular evidence, the State certainly cannot establish knowledge that any evidence on the phone is authentic, and the trial court found the State had not shown such knowledge. (R. 44-45) Moreover, the State could not establish the element of authenticity even if the proper focus of the foregone conclusion exception was on the passcode itself, as asserted by the Fourth District. *Sneed*, 2021 IL App (4th) 210180, ¶¶ 98-102. The only way to authenticate the passcode would be to use it after it was produced, negating the possibility that the State could establish its knowledge of authenticity at the time it seeks the act of production. See *Pollard,* 287 So. 3d at 656.

Having failed to establish knowledge of any elements of the exception, the trial court was correct to deny the State's motion to compel, where the focus of the exception was on the evidence the State was seeking production for.

The Fourth District viewed this case as factually distinguishable from *Spicer* on the basis that the State had described the information it was seeking with reasonable particularity, where Ummel testified that he believed he would find photographs of the checks or records of the mobile deposits. *Sneed*, 2021 IL App (4th) 210180, ¶¶ 78-80, 103. However, this distinction conflates the standard for a search warrant with the knowledge required to meet the foregone conclusion exception. A search warrant must give a particularized statement of the things police believe that they can seize to ensure that they do not seize the wrong property, see *People v. McCarty*, 223 Ill. 2d 109, 151 (2006), not to establish their knowledge of the items' existence. It is based on probable cause, which involves the reasonable belief of the officer that evidence of a criminal violation is in the location to be searched. See *McCarty*, 223 Ill. 2d at 153. As the trial court in this case recognized (R. 41-43), this is a separate and distinct standard from the requirement of the foregone conclusion exception that the State establish with reasonable particularity, that it actually *knows* that the evidence it is seeking exists, is in a person's possession, and is authentic. *Spicer*, 2019 IL App (3d) 170814, ¶ 15.

G.A.Q.L. v. State, the case *Spicer* relied on, is instructive here. There, a minor crashed while speeding, one of his passengers died, and a blood test showed his blood-alcohol content was .086. *G.A.Q.L.*, 257 So.3d at 1059-60. A surviving passenger told police they had been drinking vodka and she had been communicating with the minor on her phone, and later gave a sworn statement to that effect, further stating that she had communicated with the minor on the day of the crash and the following days through text and Snapchat. *Id*. at 1060. Police sought and obtained a search warrant for the minor's phone seeking data, photographs, assigned

numbers, content, applications, text messages and other information. *Id*. Police then sought orders compelling production of the phone's passcode and an iTunes password (needed to update the phone to make it useable), which the trial court granted. *Id*.

On review, the Florida Appellate Court found that the foregone conclusion exception did not apply, where the State had failed to identify any particular file locations or name specific files that it was looking for on the phone. *Id*. at 1064-65. The one indication that the State might be seeking something more specific was the prosecutor's reference to the sworn statement of the surviving passenger that she communicated with the minor through texts and Snapchat. *Id*. at 1064. But this statement alone was not sufficient to meet the reasonable particularity standard where the State could not show that the text or Snapchat files were on the phone. *Id*. "It is not enough for the state to infer that evidence exists—it must identify what evidence lies beyond the passcode wall with reasonable particularity." *Id*.

Here, Ummel's inference of the possibility that evidence exists on the phones police seized in this case (R. 14), is not sufficient to establish the requisite knowledge to meet the foregone conclusion exception. Indeed, he specifically testified to not knowing what was on the phone at issue in this case. (R. 11) Though he said he believed there was evidentiary material on the "phones" (R. 7), plural, he ultimately testified that he was simply hoping to gain access so he could see whether there were any files related to the mobile deposit. (R. 11) When asked by the court if there was any documentation that he had from Dairy Queen or the banks specifically tying the mobile deposit to Mr. Sneed's phone, he said he was hoping to find a photo, but he did not know. (R. 12-13) He even said he did not believe there was anything tying Mr. Sneed to the transaction other than his wife's (hearsay) statements, and he was simply "inferring" that the phone at issue was used because the checks were deposited by mobile deposit. (R. 14) This testimony establishes that he did not have any independent knowledge that any relevant files or information actually existed on the phone at issue here.

In attempting to distinguish this case on the basis of Ummel's testimony, *Sneed*, 2021 IL App (4th) 210180, ¶¶ 78-80, 103, the Fourth District also failed to give deference to the trial court's ultimate factual determination that the State had not demonstrated knowledge of the existence of evidence, its possession by Mr. Sneed, and its authenticity. (R. 44-45) Though the Fourth District acknowledged the bifurcated standard of review, under which the trial court's factual findings would only be reversed if against the manifest weight of the evidence, *Sneed*, 2021 IL App (4th) 210180, ¶ 27, it failed to establish how the trial court's determination was manifestly erroneous. It was not. Where Ummel testified that he did not know if the files he sought existed (R. 11), did not know if there was anything tying the specific phone at issue to the mobile deposits (R. 12-13), and that he was at best inferring the possibility of evidence based on those mobile deposits (R. 14), the court's finding that the State did not show the requisite knowledge was not against the manifest weight of the evidence. (R. 43-45) As such, this Court should reverse the decision of the appellate court, and affirm the trial court's denial of the motion to compel.

E. Conclusion

The compelled production of a cellular phone passcode falls under the protection of the State and Federal constitutional privileges against self-incrimination because it is an act of production that requires the use of the mind, and conveys information such as knowledge, possession, and control of the phone and its contents. See *Spicer*, 2019 IL App (3d) 170814, ¶¶ 19-20; *G.A.Q.L.*, 257 So. 3d at 1061-63. The foregone conclusion exception should not be applied to remove this protection, as it is a narrow exception tailored toward the circumstances of document production, and expanding that rationale would improperly diminish the constitutional privilege. See *Davis*, 220 A.3d at 549; *Seo*, 148 N.E.3d at 959. Therefore, this Court should reverse the Fourth District's decision, and affirm the trial court's denial of compulsion without applying the exception.

However, if the foregone conclusion exception is applied, it should only allow compelled production where the State can establish its present knowledge that the evidence it is seeking beyond the passcode wall exists, is in Mr. Sneed's possession, and is authentic. See *Spicer*, 2019 IL App (3d) 170814, ¶ 21; *G.A.Q.L.*, 257 So. 3d at 1063; *Seo*, 148 N.E.3d at 957-58. Because the State failed to establish either the existence of evidence or Mr. Sneed's possession of it (R. 42-45), and therefore cannot establish the authenticity of any hoped-for evidence, the foregone conclusion exception cannot be applied to remove the protections of Mr. Sneed's privilege against self-incrimination. See *Spicer*, 2019 IL App (3d) 170814, ¶¶ 22-23. As such, Mr. Sneed requests that this Court reverse the Fourth District's decision, and affirm the trial court's order denying the State's motion to compel.

CONCLUSION

For the foregoing reasons, Keiron K. Sneed, petitioner-appellant, respectfully requests that this Court reverse the decision of the appellate court finding jurisdiction, or in the alternative, reverse the appellate court's decision on the merits and affirm the trial court's order denying the State's motion to compel.

Respectfully submitted,

CATHERINE K. HART
Deputy Defender

JOSHUA SCANLON
Assistant Appellate Defender
Office of the State Appellate Defender
Fourth Judicial District
400 West Monroe Street, Suite 303
Springfield, IL 62704
(217) 782-3654
4thdistrict.eserve@osad.state.il.us

COUNSEL FOR PETITIONER-APPELLANT

CERTIFICATE OF COMPLIANCE

I certify that this brief conforms to the requirements of Rules 341(a) and (b). The length of this brief, excluding the pages or words contained in the Rule 341(d) cover, the Rule 341(h)(1) table of contents and statement of points and authorities, the Rule 341(c) certificate of compliance, the certificate of service, and those matters to be appended to the brief under Rule 342, is forty-two pages.

/s/Joshua Scanlon
JOSHUA SCANLON
Assistant Appellate Defender

APPENDIX TO THE BRIEF

Keiron K. Sneed, No. 127968

APPEAL TO THE APPELLATE COURT OF ILLINOIS
FOURTH JUDICIAL DISTRICT
FROM THE CIRCUIT COURT OF THE SIXTH JUDICIAL CIRCUIT
DEWITT COUNTY, ILLINOIS

PEOPLE	)	
Plaintiff/Petitioner	)	Reviewing Court No: 4-21-0180
	)	Circuit Court No: 2021CF13
	)	Trial Judge: Karle E Koritz
v	)	
	)	
	)	
SNEED, KEIRON K	)	
Defendant/Respondent	)	

COMMON LAW RECORD - TABLE OF CONTENTS

Page 1 of 1

Report of Proceedings

Supplement

In the Circuit Court of the Sixth Judicial Circuit,
DeWitt County, Illinois

FILED
DeWitt County, Illinois
MAR 29 2021
Michelle Van Valey
Clerk of the Circuit Court

THE PEOPLE OF THE STATE OF ILLINOIS,

v. No. 2021-CF-13

KEIRON K. SNEED

Notice of Appeal

An appeal is taken from the order or judgment described below.

(1) Court to which appeal is taken: Fourth District Appellate Court

(2) Name of appellant and address to which notices shall be sent.

Name: The People of The State of Illinois
Address: 201 W. WASHINGTON CLINTON, IL 61727

(3) Name and address of appellant's attorney on appeal.

If appellant is indigent and has no attorney, does he want one appointed?

(4) Date of judgment or order: MARCH 24, 2021.

(5) Offenses of which convicted:

(6) Sentence_____

(7) If appeal is not from a conviction, nature of order appealed from: Certificate of Substantial Impairment

(8) If the appeal is from a judgment of a circuit court holding unconstitutional a statute of the United States or of this state, a copy of the court's findings made in compliance with Rule 18 shall be appended to the notice of appeal.

(Signed): Michelle R. Van Valey
Michelle R. Van Valey,
Clerk of the Circuit Court

C 33

2021 IL App (4th) 210180

NO. 4-21-0180

FILED
November 18, 2021
Carla Bender
4th District Appellate
Court, IL

IN THE APPELLATE COURT

OF ILLINOIS

FOURTH DISTRICT

THE PEOPLE OF THE STATE OF ILLINOIS, Plaintiff-Appellant, v. KEIRON K. SNEED, Defendant-Appellee.	)	Appeal from the Circuit Court of De Witt County No. 21CF13. 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 suppresse[s] 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. 00114A, 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.

No. 127968

IN THE

SUPREME COURT OF ILLINOIS

PEOPLE OF THE STATE OF ILLINOIS, Respondent-Appellee, -vs- KEIRON K. SNEED, Petitioner-Appellant.	)))))))))))	Appeal from the Appellate Court of Illinois, Fourth Judicial District, No. 4-21-0180. There on appeal from the Circuit Court of the Sixth Judicial Circuit, DeWitt County, Illinois, No. 21-CF-13. Honorable Karle E. Koritz, Judge Presiding.

NOTICE AND PROOF OF SERVICE

Mr. Kwame Raoul, Attorney General, 100 W. Randolph St., 12th Floor, Chicago, IL 60601, eserve.criminalappeals@ilag.gov;

Mr. David J. Robinson, Deputy Director, State's Attorney Appellate Prosecutor, 725 South Second Street, Springfield, IL 62704, 4thdistrict@ilsaap.org;

Dan Markwell, DeWitt County State's Attorney, 201 W. Washington St., Clinton, IL 61727, dmarkwell@dewittcountyill.com;

Mr. Keiron K. Sneed, 520 E. Main, Apt. 410, Clinton, IL 61727

Under penalties as provided by law pursuant to Section 1-109 of the Code of Civil Procedure, the undersigned certifies that the statements set forth in this instrument are true and correct. On June 8, 2022, the Brief and Argument was filed with the Clerk of the Supreme Court of Illinois using the court's electronic filing system in the above-entitled cause. Upon acceptance of the filing from this Court, persons named above with identified email addresses will be served using the court's electronic filing system and one copy is being mailed to the petitioner-appellant in an envelope deposited in a U.S. mail box in Springfield, Illinois, with proper postage prepaid. Additionally, upon its acceptance by the court's electronic filing system, the undersigned will send 13 copies of the Brief and Argument to the Clerk of the above Court.

/s/Rachel A. Davis
LEGAL SECRETARY
Office of the State Appellate Defender
400 West Monroe Street, Suite 303
Springfield, IL 62704
(217) 782-3654
Service via email will be accepted at
4thdistrict.eserve@osad.state.il.us