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, 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.

REPLY BRIEF 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

ORAL ARGUMENT REQUESTED

E-FILED
12/27/2022 3:14 PM
CYNTHIA A. GRANT
SUPREME COURT CLERK

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.

In his opening brief, Mr. Sneed argued that the trial court's decision was not appealable by the State because it did not substantively prevent the State from pursuing its search warrant or presenting any evidence at trial. (Opening Br., pp.9-13) Further, any impairment of the State's case was questionable where its argument on the merits relied on the evidence it was seeking, adding little to the overall information in its possession. (Opening Br., pp. 13-14) In response, the State argues that the court's decision did substantively quash the search warrant and suppress evidence, and that there cannot be any challenge to jurisdiction based on its certificate of impairment. (St. Br., pp. 7-14) The State is incorrect, as it misconstrues the relevant facts, and misunderstands the basis for some of Mr. Sneed's argument.

As an initial matter, the State argues that problems with its certificate of impairment cannot be used independently to challenge jurisdiction. (St. Br., pp. 13-14) But the significance of the certificate of impairment here is that the appellate court relied on it in finding that the trial court's denial was like an order suppressing evidence. *People v. Sneed*, 2021 IL App (4th) 210180, ¶¶ 32-34. In doing so, it was relying on a certificate asserting impairment that was contradicted by the State's underlying argument that the evidence it sought was a foregone conclusion and would add little to its case. (C. 31, R. 30-34) This contradiction demonstrates the appellate court's error in relying on the State's assertion of effect. While not an independent ground to disturb jurisdiction, it illustrates the need for a careful assessment of the substantive effects of a trial court's order, as such an assessment reveals that the denial here neither quashed a warrant, nor suppressed evidence.

The State's primary argument is that denial of the motion to compel effectively quashed the search warrant, because it excluded the only means by which the State could execute that warrant. (St. Br., pp. 8-10) The State also asserts that *In re K.E.F.*, 235 Ill. 2d 530, 537 (2009) and *People v. Lee*, 2020 IL App (5th) 180570 are inapposite on this basis, because the State had other means of presenting the evidence that was limited in those cases, but has no such alternate means in this case. (St. Br., pp. 10-12) However, these arguments are premised on the incorrect assertion that the record contains evidence that the State did not have other means to access the phone in this case. It may be true that the Clinton Police, on their own and without any assistance from another arm of the State, would not have the capability of "cracking" a cell phone without a passcode. (R. 8) But Detective Ummel testified that the Illinois State Police (ISP) had been used for such purposes in the past. (R. 8) The caveat to that was his further testimony that they do not usually provide such assistance if the case does not involve narcotics. (R. 8) This does not establish an inability to access the phone without compelling production of the passcode, it establishes an unwillingness on the part of the State to expend the necessary resources on this particular type of case.

The fact that accessing the phone by some other means might be more costly, time consuming, or difficult does not somehow change the substantive effect of the trial court's denial from one that limits the means of executing the warrant, to one that voids the warrant entirely. In *Lee*, where the trial court held video interviews of child witnesses were inadmissible, the Fifth District rejected the State's arguments that the order should be appealable because the videos would be "more impactful" than live testimony, and that there was a possibility of a witness freezing on the stand or becoming unavailable. 2020 IL App (5th) 180570, ¶¶ 13-16. It found that, where live testimony was another means to present evidence from these witnesses, the mere possibility a witness could become unavailable did not change the order

from one "impacting only the means by which the State may present its evidence into an appealable order suppressing evidence." *Id.*, ¶ 16.

The same is true here with regard to the means of executing the warrant, where compelling the passcode's production might be the most convenient means of accessing the phone, but there is evidence that other means could be available. Indeed, Ummel's testimony indicates that the ISP has provided assistance with cracking cell phones in the past, notwithstanding their reluctance to assist in cases that do not involve narcotics. (R. 8) There is no indication Ummel actually sought assistance from ISP in this case, or determined if obtaining assistance would be beyond the means, financially or otherwise, of the Clinton Police Department if they had to go elsewhere. In fact, the State made no independent effort to access the phone before moving to compel production of the passcode. (R. 7-8)

The State further takes issue with *Lee*, and *K.E.F.*, because they did not deal with search warrants. (St. Br., p. 10) However, the only case the State cites that addressed the appeal of an order on the basis it quashed a warrant is the Fourth District's unpublished decision of *People v. Hollingsworth*, 2022 IL App (4th) 190329-U. (St. Br., p. 12) That case is readily distinguishable, because the search warrant in *Hollingsworth* specifically ordered the defendant to provide his passcode in order to unlock the phone at issue. *Hollingsworth*, 2022 IL App (4th) 190329-U, ¶¶ 11, 14. Thus, by denying compulsion, the trial court voided that term of the search warrant, allowing the defendant not to comply with a direct command of the warrant. *Id.*, ¶ 28. The search warrant in this case made no such command. (Supplement, p. 3) It ordered only that police search the phones found in the possession of Mr. Sneed and his wife, and gave no commands directing Mr. Sneed or his wife to provide passcodes or unlock the phones. (Supplement, p. 3)

The State's argument that evidence was suppressed in this case is also not supported by *Hollingsworth*. (St. Br., pp. 12-13) The Fourth District held that the denial in *Hollingsworth* suppressed evidence because it prohibited the State from accessing the phone, and thereby presenting evidence to the jury. *Hollingsworth*, 2022 IL App (4th) 190329-U, ¶ 27. But this again rests on the idea, similar to the warrant argument, that the State had no other means of searching the phone. Significantly, in *Hollingsworth*, the phone at issue was an Apple iPhone, the affidavit supporting the warrant included information from a detective who had previously been certified as a forensic expert in cellular phone technology, and who asserted that, with the tools available to him, and where the phone at issue had been powered down when it was retrieved, the data sought in the search warrant could not be accessed without the passcode. *Id.*, ¶¶ 11-13. While this information did not seem to take into account assistance that might be available outside the local police department, it at least provided some evidentiary basis on which the appellate court might reasonably conclude that the relevant data on the phone would not be accessible without the passcode.

There is no such evidentiary basis in this case, where Ummel's testimony suggests that cell phone cracking assistance is available, but not generally provided to certain classes of case for policy reasons. (R. 8) The State's argument that further efforts to access the phone might risk locking the phone or erasing its data, is also based on examples involving safety features on Apple iPhones. (St. Br., pp. 8-9, n. 2, citing Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 Geo. L. Rev. 989, 1000 (April 2018).) However, the phone at issue here is not an iPhone at all (Supplement, pp. 1, 3), and the State has not presented evidence that it has any additional security measures that might involve such risks. The only evidence available is Ummel's testimony, which established that there are other means for the State to attempt access, even if it chooses to limit the purposes for which those means are utilized. (R. 8)

The State's argument that the court's denial suppressed evidence is also flawed where it requires a logical leap not present in other cases involving the suppression of evidence: that evidence will in fact be found. As an example, in the case of *People v. Smith*, 399 Ill. App. 3d 534, 536-38 (3d Dist. 2010), to which the State cites (St. Br., p. 13), the State was prevented from presenting the prior statements of the defendant police officers by the trial court's order quashing the subpoena for those statements. *Smith*, 399 Ill. App. 3d at 537. In that case the State was aware that the defendants had made statements to the police department as part of the department's internal review of the offenses at issue, and the defendants had signed forms dictating the reasons for those statements (and reserving their Fifth Amendment rights should the statements be used for any purposes other than those internal to the department). *Id.* at 535-36. Thus, the State knew that evidence relevant to the offenses at issue existed, was available, and would be produced by the subpoena.

Here, the State has no such knowledge that any particular items of evidence would be found, as Ummel testified only that he was "hoping" to find evidence on the phone. (R. 13) He could not establish the existence of any specific files or information on the phone at issue. (R. 11, 12-14, 43-44) Indeed, the State does not now contest this finding by the trial court, or dispute Mr. Sneed's position that it has not established the existence of specific documents or information on the phone. (St. Br., pp. 37-43) Thus, the State's argument rests entirely on the assumption, without proof, that it will find some relevant evidence on this specific phone. Because the State has other means to attempt to search the phone, and has not established that it will actually find any evidence when it does, the trial court's order cannot be said to have the substantive effect of suppressing evidence.

Where the trial court's order does not quash a warrant or suppress evidence, this Court should reverse the appellate court's decision finding jurisdiction, and affirm the trial court's order denying the motion to compel production. See *K.E.F.*, 235 Ill. 2d at 540-41.

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.

In his opening brief, Mr. Sneed argued that production of a passcode is protected by the right against self-incrimination and that the foregone conclusion exception should not be applied, but even if that exception is applied, the State had not met its requirements with regard to the evidence within the phone at issue, on which the exception should be focused. (Opening Br., pp. 15-41) In response, the State recognizes that passcode production is testimonial and presumptively falls under the Fifth Amendment (St. Br., pp. 14-27), but argues that the foregone conclusion exception should be applied, and that the State has fulfilled the exception's requirements where it established the existence, possession, and authenticity of the passcode itself. (St. Br., pp. 27-44) The State is incorrect.

As an initial matter, the State contests the idea that this Court can interpret Illinois' constitutional right against self-incrimination as more expansive than the federal right, where there are not substantial grounds to depart from the federal interpretation. (St. Br., pp. 14-16) The State is correct that this Court has generally interpreted them in the same manner, *People ex rel. Hanrahan v. Power*, 54 Ill. 2d 154, 160 (1973), and recognized that our constitution of 1970 reflected an intention that the existing state of the law remain unchanged. *People v. Rolfingsmeyer*, 101 Ill. 2d 137, 142 (1984). However, it is worth considering that the longstanding rule of *Boyd v. United States*, 116 U.S. 616, 630, 633-35 (1886)–that the Fifth Amendment protected an individual from the compelled production of his private books and papers, as well as compelled oral testimony–was the existing state of the law at the time our state constitution was adopted. See *Schmerber v. California*, 384 U.S. 757, 763-64 (1966); *Couch v. United States*, 409 U.S. 322, 330 (1973); *Bellis v. United States*, 417 U.S. 85, 87-88 (1974).

It was not until the holding of *Fisher v. United States*, 425 U.S. 391 (1976), that the U.S. Supreme Court seemed to step away from that understanding, and suggest that the compelled production of such private papers could be permitted if aspects of the production could be nullified by the State's knowledge. See *United States v. Hubbell*, 530 U.S. 27, 56 (2000) (Thomas, J., concurring). To the extent our state constitution recognized the rule of *Boyd* as the existing state of the law, this Court can and should depart from any narrowing of that rule by *Fisher*, as applicable to the State guarantee against self-incrimination. However, regardless of whether this Court rejects *Fisher*, the production of a passcode must still fall under the protection of the State and Federal rights against self-incrimination.

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 State acknowledges in its brief, that the act of entering a passcode is testimonial because it implicitly conveys knowledge about the passcode (St. Br., pp. 17-22), abandoning the Fourth District's opposition to the mental/physical production dichotomy, and its explicit holding that compelling production of a passcode, either by producing the passcode or providing entry to the phone, does not compel testimony at all under the Fifth Amendment. *People v. Sneed*, 2021 IL App (4th) 210180, ¶¶59-60, 63. In conceding that passcode production is testimonial however, the State seeks to limit the scope of testimony that a court can consider to be conveyed by such an act to its most superficially obvious implications.

In particular, the State argues that producing a passcode is testimonial because it conveys only the three pieces of information that the court in *Fisher* identified as being conveyed by the production of the sought-after tax documents in that case: (1) the evidence exists, (2) it is in a person's possession or control, and (3) it is authentic. 425 U.S. at 410; (St. Br., pp. 17-19) Specifically, the State argues that the only facts conveyed by passcode production are that

the passcode exists, the person possesses the passcode, and the passcode is authentic (because it unlocks the phone). (St. Br., pp. 20-21) The central flaw in the State's reasoning is that the testimony involved in an act of production is entirely based on what the act communicates by implication; in other words, it is based on what inferences can reasonably be drawn from the act. See Laurent Sacharoff, *What am I Really Saying When I Open my Smartphone? A Response to Orin S, Kerr*, 97 Tex. L. Rev. Online 63, 66 (2019) While knowledge of a passcode is certainly one fact that may be inferred from the act of producing it, it is by no means the only reasonable implication.

When a digital device is decrypted the implications of that decryption are far more expansive than those involved in the production of the specifically identified tax documents that were at issue in *Fisher*. Producing a passcode implies a person's knowledge not only of the passcode, but of the files and data found on the device, as well as their possession and control over those contents. See *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012). Such knowledge and control is implied, not only for specifically identified items or categories of items such as those that might be listed in a subpoena or search warrant, but for everything that can possibly be found on the phone. See *Eunjoo Seo v. State*, 148 N.E.3d 952, 957, 960 (Ind. 2020). The State even acknowledges that the entry of a passcode gives rise to numerous inferences beyond knowledge of the passcode, including knowledge of the files found on the phone. (St. Br., pp. 22-23) Thus, its argument that the implied testimony is limited to knowledge of the passcode, is a manufactured restriction on the information inferred from unlocking the phone.

This artificial focus is the basis of the State's argument that the Indiana Supreme Court erred in the *Seo* case. It asserts that the *Seo* court conflated producing the unencrypted contents of a phone, with the simple act of unlocking the phone that police had in their possession, and that a phone is merely a container, the unlocking of which says nothing about the contents.

(St. Br., pp. 23-26) But where all of the testimony inherent in an act of production is made by implication, knowledge and control of the contents are very direct implications from the act of entering the code. See *Commonwealth v. Gelfgatt*, 468 Mass. 512, 522 (2014) ("the defendant implicitly would be acknowledging that he has ownership and control of the computers and their contents***a communication of his knowledge about particular facts that would be relevant to the Commonwealth's case."). Even knowledge of a passcode itself is only a reasonable inference that may be drawn from production, particularly where a person does not actually reveal the passcode. See Sacharoff, *supra*, at 71 ("Only if the act succeeds, and the device opens, can we infer, working backwards, that the person must have known the password, again, assuming she did not guess it.").

While the State seeks to sidestep the Fourth District's position on the mental/physical dichotomy, it still argues that the only production at issue here is the physical act of entering a passcode, and that entering a passcode is analogous to surrendering a key, while revealing it is analogous to revealing a combination. (St. Br., p. 22, footnote 5) Accepting that the State now seeks only the entry of the passcode, and not production of the code itself (St. Br., p. 22, footnote 5), this severely undercuts its repeated reliance on the idea that the contents of the phone are not the focus of the production at issue, and that a passcode can be subjected to the foregone conclusion exception on the same basis as any other evidence. (St. Br., pp. 21-22, 24-25, 27, 30-31, 37, 41-42) If a passcode is entered without the State learning it, the passcode is not being produced at all. The only thing being produced in such a situation are the unencrypted contents of the phone being unlocked. See Sacharoff, *supra*, at 68. The testimony implied by that act can only reasonably be focused on what is actually being produced.

The State is also wrong that the act of entering the code is not akin to the combination in Justice Stevens' famous analogy. The key/combination analogy illustrates the difference between testimonial and nontestimonial acts, based on the fact that an act involves revealing

the contents of a person's mind. See *Hubbell*, 530 U.S. at 43; *Doe v. United States*, 487 U.S. 201, 210, footnote 9 (1988) (*hereinafter "Doe II"*). Justice Stevens' specific statement was that, "***I do not believe [a defendant] can be compelled to reveal the combination to his wall safe–by *word or deed*." *Doe II*, 487 U.S. at 219 (Stevens, J., dissenting) (emphasis added). Even the court in *State v. Andrews*, 243 N.J. 447 (2020), which ultimately focused the foregone conclusion exception on knowledge of the passcode, accepted that a passcode was analogous to a combination and not a key, where either communicating it or entering it required facts contained in the holder's mind. *Andrews*, 243 N.J. at 478.

Entering a passcode is as testimonial an act as disclosing a passcode because they both require the use of a person's mind, and both implicitly reveal facts about that person's knowledge of the contents of the device or container being unlocked , as well as the means of unlocking them. See *United States v. Green*, 272 F.3d 748, 752-53 (5th Cir. 2001) (finding that disclosing the locations and opening the combination locks of cases containing firearms were acts that disclosed the defendant's knowledge of the presence of firearms as well the means of opening the cases). The State argues that the Eleventh Circuit distinguished between the testimony implicit in unlocking a device and that implicit in producing its contents, where the State's order specifically sought the "unencrypted contents" of the laptops and hard drives involved. (St. Br., pp. 26-27) But the State ignores the fact that the act at issue was the same, the unlocking of digital devices, and that the court viewed that act as producing the contents of the devices. *In re Grand Jury Subpoena*, 670 F.3d at 1346. Just as in *Seo,* and in this case, the digital devices at issue were already in the government's possession, *id.* at 1339, so the act of unlocking the devices cannot somehow be seen as separate from the act of producing their contents.

Indeed, the Eleventh Circuit specifically stated that "[r]equiring Doe to use a decryption password is most certainly more akin to requiring the production of a combination because both demand the use of the contents of the mind, and the production is accompanied by the

implied factual statements noted above that could prove to be incriminatory." *Id.* at 1346. The implied statements of using a decryption password that the court recognized would be: that Doe had knowledge of the existence and location of potentially incriminating files; he had possession, control, and access to those files; and he had the capability of decrypting them. *Id.* Thus, aside from the code itself, the reasonable implications of unlocking a device are no different than the implications of providing the code in order to unlock it, and in both cases the direct implications involve knowledge and control of the contents of the device.

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

The State argues that phone passcodes are not uniquely privileged under the Fifth Amendment, that the forgone conclusion exception applies to all acts of producing any kind of evidence, and that this is the reason courts have applied the exception in this context. (St. Br., pp. 27-31) However, the issue is not that passcodes are uniquely privileged, it is that the act of production involved in these cases–the unlocking or decryption of digital devices–does not fit the narrow parameters of the exception as it was created. The State cites to *Fisher* and *Hubbell* as illustrating that a compelled act does not violate the Fifth Amendment where the government has independent knowledge of the facts implied by the act. (St. Br., p. 28) But it overlooks the fact that the acts being compelled in both cases were the production of documents already identified by the government. *Fisher*, 425 U.S. at 394; *Hubbell*, 530 U.S. at 31. In fact, the exception did not apply in *Hubbell* where the government subpoenaed numerous broad categories of documents without sufficient independent knowledge of what would be produced, *Hubbell*, 530 U.S. at 45, just as the State lacks knowledge of particular evidence here.

Even the cases the State's cites, *Balt. City Dep't of Soc. Servs. v. Bauknight*, 493 U.S. 549 (1990) and *Unites States v. Patane*, 542 U.S. 630, 644 (2004)–neither of which relied for their holdings on the foregone conclusion exception–identified that the information being conveyed

by production is about the "things" or "items" that are actually produced. *Bauknight*, 493 U.S. at 555; *Patane*, 542 U.S. at 644, n. 7. As the State has established, the passcode on which it focuses its entire analysis is not being produced at all. (St. Br., p. 22, n. 5) It does not fit the mold of the foregone conclusion exception, which was built in the context of documentary production, where the government sought to have specific identifiable documents turned over. *Fisher*, 425 U.S. at 394. In that context, the implications of producing those specifically identified documents could reasonably be limited to knowledge of their existence, possession, and authenticity, because the items being produced were themselves limited by the government's demand. As described above (see *supra*, sub-argument II.A.), the same is not true where the State seeks the compelled decryption of a digital device. The State's arguments that the volume of information produced is irrelevant, and that the warning of *Carpenter v. United States*, 138 S. Ct. 2206, 2222 (2018)–not to uncritically extend precedent where digital technology creates new concerns–is inapplicable (St. Br., pp. 32-33, 34-36), both suffer from the same oversight. It is not simply that there is a lot of information in the "container" as the State asserts the phone is, it is that the amount and diversity of information, not specifically identified for production by the State, greatly increases the scope of the implications that arise from producing it. *Seo*, 148 N.E.3d at 959.

The State takes issue with the case of *Commonwealth v. Davis*, 656 Pa. 213 (2019), and argues that its reasoning was unsound where it found the foregone conclusion exception did not apply to acts that reveal information as the result of using one's mind, and where it did not identify any unique characteristics of business or financial records that would subject them to less protection. (St. Br., pp. 31-32) The State misreads *Davis*. To the extent the State says that any production requires the use of the mind, and so cannot limit the exception, the *Davis* court did not suggest that the mind was not used in the production of the records to which

the exception had been applied. What the *Davis* court recognized was, as discussed above (see *supra*, sub-argument II.A.), that there are greater implications that can come from the production of other kinds of evidence. The court relied in part on a decision of the California Appellate Court which found that compelled production of a firearm was a testimonial act that fell under Fifth Amendment protection, and would not be a foregone conclusion. *Davis*, 646 Pa. at 238-39; *Goldsmith v. Superior Court*, 152 Cal. App. 3d 76, 85-86 (3d Dist. 1984). In so finding, the *Goldsmith* court said the State's argument that independent evidence established the defendant's possession of the gun before and after the crime was curious, and would be like stating that a confession could be coerced as soon as the government could show that it would produce enough independent evidence to get past a motion for directed verdict in a future trial. *Davis*, 646 Pa. at 238-39 (quoting *Goldsmith*, 152 Cal. App. 3d at 87, n. 12). Thus, the foregone conclusion exception, applied broadly to all evidence, carries the significant danger of obviating the right against self-incrimination entirely. See *Davis*, 646 Pa. at 238 ("***to apply the foregone conclusion rationale in these circumstances would allow the exception to swallow the constitutional privilege.")

With regard to the argument that the *Davis* court did not provide a reason for limiting the exception to business and financial records, the State overlooks the *Davis* court's citation to *Shapiro v. United States*, 335 U.S. 1 (1948). *Davis*, 656 Pa. at 237. There, the U.S. Supreme Court drew a distinction between records maintained pursuant to law for public purposes (in that case a sales record kept by a licensee of the federal Emergency Price Control Act), and private papers that were subject to the protections of the privilege. *Shapiro*, 335 U.S. at 33. This distinction itself was heavily contested as too cavalierly taking the disclosure of such records outside the ambit of the Fifth Amendment, and narrowing the right against self-incrimination. See *Shapiro*, 335 U.S. at 36-70 (Frankfurter, J., dissenting), and 70-71 (Jackson,

J. and Murphy, J., dissenting). However, it still illustrates the *Davis* court's point that documents such as business and financial records, which have connections to third parties outside the individual, have long been seen as separate from information or records held purely in a private capacity. See also *Curcio v. United States*, 354 U.S. 118, 122-23 (1957) (differentiating between corporate or union records, and papers and effects held purely in a personal capacity.)

Even to the extent that *Fisher* suggested some repudiation of *Boyd* and the rule that a person's private papers could not be compelled, it did not go so far as to hold that the foregone conclusion would completely obviate the privilege as to documents that were entirely unconnected to third parties. *Fisher*, 425 U.S. at 414. The *Fisher* court specifically stated that it was not answering the question of "[w]hether the Fifth Amendment would shield the taxpayer from producing his own tax records[,]" because the papers demanded in that case were not the taxpayers' private papers where they had been prepared by third parties. *Id.*; see also *id.* at 432 ("Thus, the Court's rationale provides a persuasive basis for distinguishing between the corporate-document cases and those involving the papers of private citizens.") (Marshall, J., concurring). More importantly, the State ignores the *Davis* court's primary rationale, that "the Fifth Amendment privilege is foundational. Any exception thereto must be necessarily limited in scope and nature." *Davis*, 656 Pa. at 237. Thus, the *Davis* court reasonably limited the application of the foregone conclusion exception to the types of documents it was created to address, and the only type of evidence the U.S. Supreme Court has actually applied it to.

The State argues that providing broad access to a phone is a concern of the Fourth Amendment, which protects privacy, and not the Fifth Amendment, which does not. (St. Br., pp. 33-34) The State too willingly abandons the privacy concerns inherent in the Fifth Amendment. Even *Fisher* recognized that the right against-self-incrimination did serve privacy interests within its focus, and that there could be special problems of privacy that might adhere

if the situation involved the production of a personal diary or similar item. See *Fisher*, 425 U.S. at 399 and 401, n. 7. However, the issue is not a protection of private information generally, but of the compelled disclosure of such information. Here, this means the extensive production of the entire unencrypted contents of a phone, where the State seeks the unlocking of the phone broadly, rather than the production of specifically identified documents or items of evidence. (C. 12-19, St. Br., p. 22, n. 5) Where such production involves significant and expansive implications about all of the data being produced, see Sacharoff, *supra*, at 68-70, the disclosure itself is protected under the Fifth Amendment. Because production is not limited by the State's request, as it was under *Fisher*, the foregone conclusion exception should not be applied in the context of unlocking a digital device by entering a passcode.

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 State argues that the government's reason for compelling production does not matter, and cites *Fisher* to support the position that compulsion was permitted even though the government presumably wished to obtain incriminating evidence by obtaining the tax documents in that case. (St. Br., pp37-38) But the State misunderstands Mr. Sneed's argument that the focus of the exception is on what the government seeks to obtain. The problem is not that the State here wants to obtain incriminating evidence, the State is correct that this intention does not matter. What matters is what the State is actually seeking to have produced. In *Fisher*, the government sought specifically identified tax documents through summonses, and had independent evidence wholly separate from the taxpayer's act of producing them. 425 U.S. at 394-95, 411. It was information about those specifically identified documents that the court ultimately found to be a foregone conclusion. *Id.* at 411. Here, particularly now that the State asserts it is not seeking to have the passcode itself disclosed (St. Br., p. 22, footnote 5), what

the State is seeking production for is the unencrypted contents of the phone (see *supra*, sub-argument II.A.). Thus the contents of the phone are of central importance to the information it must establish if the foregone conclusion exception is to be applied.

The State argues that the exception is not unworkable and can reasonably be applied to a passcode where doing so simply requires the straightforward application of the test. (St. Br., pp. 36, 38-39) Apart from relying on the flawed argument that the only information conveyed by production is information about the passcode (see *supra*, sub-argument II.A.), the State errs in asserting that knowledge of the passcode is somehow independent from the act of production. In particular, while asserting that the existence of a passcode will always be a foregone conclusion based merely on the need for it, the State argues that possession and authentication must still be proven (St. Br., pp. 38-39), and that authentication is reasonably established through "self-authentication," where the State can authenticate the password after it is entered into the phone. (St. Br., pp. 40-42)

The problem with these arguments is that such proof is not independent of the act of production at all. Unlocking a device is not equivalent to knowing a passcode. The knowledge of the passcode is itself an inference based on the act of unlocking the device. See Sacharoff, *supra*, at 71. It is always possible that someone may unlock the device in an unexpected way–such as through biometrics where the police may not have attempted such access, or through guessing the code–and it is only if the device unlocks that we can infer knowledge by working backward from the successful decryption. *Id.* Even if the inference is a sound one, ultimately, it still relies on the act of decryption.

With regard to authentication specifically, the State confuses the time at which authentication occurs with the time at which the State must have independent evidence sufficient to authenticate. It argues that *Pollard v. State*, 287 So.3d 649, 656 (Fla. 1st Dist. Ct. App. 2019), misunderstood authentication in holding that the State must have proof of authentication before

production is compelled. (St. Br., p. 40) But that is the test as it was applied in *Fisher*, which determined that the tax documents were a foregone conclusion "***because the Government knew of the existence of the documents, knew that the taxpayers possessed the documents, and could show their authenticity not through the use of the taxpayers' mind, but rather through testimony from others." *In re Grand Jury Subpoena*, 670 F.3d at 1344 (describing *Fisher*). In other words, at the time production was requested, the government had evidence wholly independent of the act of production with which to confirm authenticity, as it had witnesses in the accountants who created the tax documents who could confirm their authenticity regardless of how the government obtained the documents. See *Fisher*, 425 U.S. at 412-13. The same is not true of password "self-authentication."

The concept of self-authentication was created specifically to deal with applying the forgone conclusion test to passcodes. As the court in *State v. Stahl,* 206 So.3d 124 (Fla. 2d Dist. Ct. App. 2016),explained it:

> "***the act of production and foregone conclusion doctrines cannot be seamlessly applied to passcodes and decryption keys. If the doctrines are to continue to be applied to passcodes, decryption keys, and the like, we must recognize that the technology is self-authenticating—no other means of authentication may exist.***If the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic." *Stahl*, 206 So.3d at 136 (citations ommitted)

The *Stahl* court's statement here admits that the foregone conclusion exception cannot be applied to passcodes at all unless it is stretched to accommodate the fact that authentication of a passcode cannot take place without the act of entering it. The State argues that authenticity is established if the government's ability to authenticate will be a foregone conclusion so long as it is independent of the act of production. (St. Br., pp. 40-41) But this does not support its position that the exception should be focused on the passcode because the government's ability to authenticate the code is entirely dependent on the compelled act of entering it.

None of the cases the State cites in support suggest otherwise. (St. Br., pp. 40-41) All involved an analysis of whether there was evidence to authenticate specific documents independent of the act of production, and the only cases to find authenticity a foregone conclusion did so where authentication could be had from an entirely separate source, as in *Fisher*. See *United States v. Greenfield*, 831 F.3d 106, 118-24 (2d Cir. 2016); *In re Grand Jury Subpoena Dated April 18, 2003*, 383 F.3d 905, 912-13 (9th Cir. 2004); *United States v. Stone*, 976 F.2d 909, 911-12 (4th Cir. 1992) (finding authentication of beach house records a foregone conclusion where they could be authenticated by the utility companies and rental agent); *United States v. Clark*, 847 F.2d 1467, 1473 (10th Cir. 1988) (finding authentication of tax documents a foregone conclusion where accountant who prepared them could authenticate them); *United States v. Rue*, 819 F.2d 1488, 1494 (8th Cir. 1987) (finding the authentication of a doctor's patient cards a foregone conclusion where they could be authenticated through comparison to other documents, the patients themselves, and an agent who had examined a blank patient card). *Greenfield* and *Rue* in particular recognized that the appropriate time for the foregone conclusion analysis is the time at which the demand for compulsion (summonses in both of those cases) was issued. *Greenfield*, 831 F.3d at 124; *Rue*, 819 F.2d at 1493.

Thus, what the State must show here is that it has evidence sufficient to fulfill the authentication requirement, and completely unrelated to the act of entering the passcode, at the time it filed its motion to compel. As the *Stahl* court recognized it cannot do this where the focus is on the passcode, *Stahl*, 206 So.3d at 136, and the only way to apply the exception to the passcode is to abandon the need for independent authentication entirely. Where applying the exception to a passcode would require breaking the very foundation of the exception, it can only reasonably be applied to the unencrypted contents of the phone that the government is actually seeking to have produced. See *People v. Spicer*, 2019 IL App (3d) 170814, ¶¶ 20-21; *G.A.Q.L. v. State*, 257 So.3d 1058, 1063-64 (Fla. 4th Dist. Ct. App. 2018).

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.

The State does not argue that it provided evidence sufficient to establish the existence, possession, and authenticity of particular files on the phone at issue sufficient to fulfill the forgone conclusion exception when it is focused on the contents of the phone. (St. Br., pp. 42-44) Therefore it has forfeited any such argument before this Court. See *People v. Bradley*, 2017 IL App (4th) 150527, ¶ 24 (finding that the State forfeited its argument because it failed to cite authority and present a well-reasoned argument); Ill. S. Ct. Rule 341(h)(7) ("Points not argued are forfeited and shall not be raised in the reply brief, in oral argument, or on petition for rehearing.").

The State relies exclusively on its ability to establish the existence, possession, and authenticity of the passcode, arguing that the trial court made a factual finding that the passcode was a foregone conclusion. (St. Br., pp. 42-43) The State is wrong that the trial court made specific findings about the existence, possession, and authenticity of the passcode, as the statements to which the State cites were questioning the legal underpinnings of finding passcode production to be testimonial at all (R. 39-40), a point which the State has already conceded. (St. Br., pp. 20-22) The court made no findings specific to the passcode, as it properly focused the application of the exception on the contents of the phone, even if it did so grudgingly. (R. 41) Moreover, as demonstrated above (see *supra*, sub-argument II.C.), even were the passcode the proper focus, the State cannot establish authenticity independent of the act of entering the code, and so cannot meet the exception's requirements. See *Stahl*, 206 So.3d at 136; *Pollard*, 287 So.3d at 656. As such, the trial court correctly denied the State's motion to compel, and this Court should affirm that decision and reverse the decision of the appellate court holding otherwise. Mr. Sneed further relies on the arguments in his opening brief.

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 reply brief conforms to the requirements of Rules 341(a) and (b). The length of this reply brief, excluding pages or words contained in the Rule 341(d) cover, the Rule 341(h)(1) statement of points and authorities, the Rule 341(c) certificate of compliance, and the certificate of service, is twenty pages.

/s/Joshua Scanlon
JOSHUA SCANLON
Assistant Appellate Defender

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

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

Mr. Keiron K. Sneed, Logan County Jail, 911 Pekin Street, Lincoln, IL 62656

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 December 27, 2022, the Reply Brief 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 Reply Brief to the Clerk of the above Court.

/s/ Amanda Mann
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