

No. ____

IN THE SUPREME COURT OF THE UNITED STATES

KEIRON K. SNEED,

Petitioner,

v.

PEOPLE OF THE STATE OF ILLINOIS,

Respondent.

On Petition For Writ Of Certiorari
To The Supreme Court Of Illinois

PETITION FOR WRIT OF CERTIORARI

CATHERINE K. HART
Counsel of Record
Deputy Defender
Office of the State Appellate Defender
Fourth Judicial District
400 West Monroe Street, Suite 303
Springfield, IL 62704
(217) 782-3654
4thDistrict@osad.state.il.us

JOSHUA SCANLON
Assistant Appellate Defender
Office of the State Appellate Defender
Fourth Judicial District
400 West Monroe Street, Suite 303
Springfield, IL 62704

COUNSEL FOR PETITIONER

QUESTIONS PRESENTED

Petitioner Keiron Sneed was charged with forgery related to the mobile deposit of two checks from a Dairy Queen at which his wife was employed. Police seized cellular phones from Mr. Sneed and his wife, and obtained a search warrant for the phones. The phones were passcode protected, and the State filed a motion seeking to compel Mr. Sneed to produce the passcode for the phone seized from him by providing it or entering it into the phone. Mr. Sneed argued that such compelled production would violate his right against self-incrimination enshrined in the Fifth Amendment, and the trial court denied the State's motion. On appeal by the State, the Fourth District of the Illinois Appellate Court reversed the trial court's decision. Mr. Sneed then appealed, and the Illinois Supreme Court affirmed the appellate court's reversal. It held that the Fifth Amendment did not prevent Mr. Sneed from being compelled to enter the passcode into the seized phone, where the State met the requirements of the "foregone conclusion doctrine" by demonstrating its knowledge of the passcode.

The questions presented are:

1. Can the forgone conclusion rationale, described in *Fisher v. United States*, 425 U.S. 391 (1976), be used as an exception to the Fifth Amendment right against self-incrimination, and permit the State to compel an individual to truthfully rely on the contents of his mind to enter a passcode into a personally held cellular phone or similar digital device?
2. If so, is the State required to show knowledge of the contents of the device in order to apply the rationale, or is a foregone conclusion analysis satisfied by a showing that the State has knowledge of only the passcode?

PARTIES TO THE PROCEEDING

The caption of this case contains the names of all the parties to the proceeding in the court whose judgment is sought to be reviewed.

RELATED PROCEEDINGS

- *People v. Sneed*, No. 2021-CF-13, Circuit Court of the Sixth Judicial Circuit, Dewitt County, Illinois. Order denying State's motion to compel production of cellular phone passcode entered March 24, 2021.
- *People v. Sneed*, No. 4-21-0180, Appellate Court of Illinois, Fourth District. Opinion and order reversing the judgment of the circuit court entered November 18, 2021.
- *People v. Sneed*, No. 127968, Supreme Court of Illinois. Opinion and order affirming the judgment of the appellate court and reversing the judgment of the circuit court entered June 15, 2023.

TABLE OF CONTENTS

QUESTIONS PRESENTED	i
PARTIES TO THE PROCEEDING.....	ii
RELATED PROCEEDINGS	ii
TABLE OF AUTHORITIES	v
OPINIONS BELOW.....	1
JURISDICTION.....	2
CONSTITUTIONAL PROVISION INVOLVED.....	2
STATEMENT OF THE CASE.....	3
REASONS FOR GRANTING THE PETITION	8
I. There is a growing nationwide conflict among state and federal courts over the application of Fifth Amendment protections to the compelled production and use of passcodes for digital devices, and the scope of the foregone conclusion rationale as an exception.....	8
A. There is a divide among state supreme courts over whether the foregone conclusion rationale is an exception that applies to the compelled production or entry of a passcode.	9
B. There is a divide among federal courts of appeal and state supreme courts over the proper focus of a foregone conclusion analysis.	13
II. The questions at issue present important and recurring concerns for criminal cases throughout the country due to the ubiquity of personal electronic devices, and the governmental desire to access them for criminal investigations.....	16
III. The decision of the Illinois Supreme Court applying the foregone conclusion rationale as an exception to Fifth Amendment protection was incorrect, and this case cleanly presents the questions underlying that application, making it a good vehicle for their resolution.....	20
A. The Illinois Supreme Court erred in applying the foregone conclusion rationale as an exception beyond the production of the kinds of third-party records that it was created to address.	21

TABLE OF CONTENTS
(continued)

B.	The Illinois Supreme Court erred in focusing the foregone conclusion analysis on the State’s knowledge about the existence of a passcode, rather than its knowledge about the unencrypted contents of the phone that would actually be produced.	25
C.	This case presents an opportunity for this Court to provide important clarification of its decision in <i>Fisher</i> and determine whether the Fifth Amendment contemplates a broader protection against the compelled production of incriminating evidence.	29
CONCLUSION.		34
APPENDIX		
Appendix A — Illinois Supreme Court Opinion.		1a
Appendix B — Appellate Court Opinion		59a
Appendix C — Trial Court Order		88a
Appendix D — Search Warrant Complaint and Search Warrant.		98a
Appendix E — State’s Motion to Compel Production of Cellular Phone Passcode		101a
Appendix F — Defendant’s Response to State’s Motion to Compel Production of Cellular Phone Passcode		109a

TABLE OF AUTHORITIES

CASES

<i>Bellis v. United States</i> , 417 U.S. 85 (1974)	22
<i>Boyd v. United States</i> , 116 U.S. 616 (1886)	19, 29
<i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018)	12, 17, 30
<i>Commonwealth v. Davis</i> , 656 Pa. 213 (2019)	9-10, 21, 23, 28, 33
<i>Commonwealth v. Gelfgatt</i> , 468 Mass. 512 (2014)	15
<i>Commonwealth v. Hughes</i> , 380 Mass. 583 (1980).	33
<i>Dreier v. United States</i> , 221 U.S. 394 (1911).	22
<i>Fisher v. United States</i> , 425 U.S. 391 (1976)	5, 8, 10, 19, 21-22, 24, 26-27, 29-32
<i>G.A.Q.L. v. State</i> , 257 So. 3d 1058 (Fla. 4th Dist. Ct. App. 2018)	13, 26
<i>Goldsmith v. Superior Court</i> , 152 Cal. App. 3d 76 (3d Dist. 1984)	33
<i>In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011</i> , 670 F.3d 1335 (11th Cir. 2012)	14, 24
<i>In re Harris</i> , 221 U.S. 274 (1911)	22
<i>Kastigar v. United States</i> , 406 U.S. 441 (1972).	24
<i>People v. Sneed</i> , 2021 IL App (4th) 210180.	3
<i>People v. Sneed</i> , 2023 IL 127968	3
<i>People v. Spicer</i> , 2019 IL App (3d) 170814	4, 26
<i>Pollard v. State</i> , 287 So. 3d 649 (Fla. 1st Dist. Ct. App. 2019)	13
<i>Riley v. California</i> , 573 U.S. 373 (2014)	17
<i>Seo v. State</i> , 146 N.E.3d 952 (Ind. 2020).	11-13, 16-17, 26, 32
<i>Shapiro v. United States</i> , 335 U.S. 1 (1948)	10-11, 23
<i>State v. Andrews</i> , 243 N.J. 447 (2020).	12, 15

State v. Pittman, 367 Or. 498 (2021) 15

State v. Stahl, 206 So.3d 124 (Fla. 2d Dist. Ct. App. 2016) 15, 28

State v. Valdez, 482 P.3d 861 (Utah Ct. App. 2021) 11

United States v. Apple MacPro Computer, 851 F.3d 238 (3rd Cir. 2017) 14-15

United States v. Djibo, 151 F. Supp. 3d 297 (E.D.N.Y. 2015) 32

United States v. Greenfield, 831 F.3d 106 (2d Cir. 2016) 28

United States v. White, 322 U.S. 694 (1944) 22, 31

United States v. Doe, 465 U.S. 605 (1984) 22

United States v. Hubbell, 530 U.S. 27 (2000) 22, 24, 28, 30

Wilson v. United States, 221 U.S. 361 (1911) 22

CONSTITUTIONAL PROVISIONS

U. S. Const. amend. V 2, 32

STATUTES

28 U.S.C. § 1257(a) 2

OTHER AUTHORITIES

Adriana Christianson, Note, *Locked Out or Locked Up: The Need for New Guidelines for Compelled Decryption*, 55 Suffolk U. L. Rev. 237 (2022) 20

Aubrey Zimmerling, *Actions Speak Louder than Words: Compelled Biometric Decryption is a Testimonial Act*, 100 Wash. U. L. Rev. 827 (2023) 20

Brief of *Amici Curiae* States of Utah *et al.* Supporting Petitioner at 1, *Pennsylvania v. Davis*, 141 S. Ct. 237, *denying certiorari* (May 26, 2020) . . 17

Bryan H. Choi, *The Privilege Against Cellphone Incrimination*, 97 Tex. L. Rev. Online 73 (2019). 32

David Rassoul Rangaviz, *Compelled Decryption & State Constitutional Protection Against Self-Incrimination*, 57 Am. Crim. L. Rev. 157 (2020) 18-19

Kirstyn Watson, Comment, *Under Digital Lock and Key: Compelled Decryption and the Fifth Amendment*, 126 Penn. St. L. Rev. 577 (2022) 19

Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*,
87 Fordham L. Rev. 203 (2018). 16, 19-20

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) 16, 19, 23-24, 26, 28

Logan Koepke, et al., *Mass Extraction: The Widespread Power of U.S. Law Enforcement
to Search Mobile Phones*, pp. 32-33 (Oct. 2020), [https://www.upturn.org/static/reports/
2020/mass-extraction/files/Upturn%20-%20Mass%20Extraction.pdf](https://www.upturn.org/static/reports/2020/mass-extraction/files/Upturn%20-%20Mass%20Extraction.pdf). 18

News Release, Cellebrite, *Cellebrite’s 2022 Industry Trends Survey Reveals the Digital
Evidence ‘Tipping Point’ has Been Reached, Creating New Challenges for Law
Enforcement Agencies* (Nov. 14, 2022), <https://investors.cellebrite.com/node/7336/pdf>.
. 17-18

Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97
Tex. L. Rev. 767 (2019) 15, 18-19

Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 Geo. L. J. 989(2018) . 18

Pew Res. Ctr., *Mobile Fact Sheet* (April 7, 2021), [https://www.pewresearch.org/internet/fact-
sheet/mobile/](https://www.pewresearch.org/internet/fact-sheet/mobile/). 17

Richard A. Nagareda, *Compulsion “To Be a Witness” and the Resurrection of Boyd*,
74 N.Y.U. L. Rev. 1575 (1999) 30

No. _____

IN THE SUPREME COURT OF THE UNITED STATES

KEIRON K. SNEED,

Petitioner,

v.

PEOPLE OF THE STATE OF ILLINOIS,

Respondent.

On Petition For Writ Of Certiorari
To The Supreme Court Of Illinois

PETITION FOR WRIT OF CERTIORARI

Petitioner Keiron K. Sneed, respectfully prays that a writ of certiorari issue to review the judgment of the Supreme Court of Illinois, reversing the circuit court's denial of the State's motion to compel production of a cellular phone passcode.

OPINIONS BELOW

The published opinion and order of the Illinois Supreme Court (Pet. App. 1a-58a) is reported at 2023 IL 127968. The published opinion and order of the Appellate Court of Illinois, Fourth District (Pet. App. 59a-87a), is reported at 2021 IL App (4th) 210180, 187 N.E.3d 801. The order of the Circuit Court of the Sixth Judicial Circuit, Dewitt County, Illinois (Pet. App. 88a-97a), is not reported.

JURISDICTION

On June 15, 2023, the Illinois Supreme Court issued an opinion affirming the judgement of the appellate court and reversing the judgment of the circuit court below. No petition for rehearing was filed. By order issued on August 22, 2023, Justice Amy Coney Barrett extended the deadline to file a petition for a writ of certiorari, then due on September 13, 2023, to and including October 13, 2023. Petitioner invokes this Court's jurisdiction under 28 U.S.C. § 1257(a).

CONSTITUTIONAL PROVISION INVOLVED

The Fifth Amendment to the Constitution of the United States provides, in pertinent part, that: "No person . . . shall be compelled in any criminal case to be a witness against himself[.]" U. S. Const. amend. V.

STATEMENT OF THE CASE

In February of 2021, Keiron Sneed was charged with two counts of forgery, based on allegations that Mr. Sneed had created two false paychecks from Dairy Queen with the intent to defraud Dairy Queen and financial institutions. Mr. Sneed and his wife, Allora Spurling Sneed (Spurling), were both arrested and the State seized one cellular phone from each of them at the time of the arrest. Pet. App. 2a-3a, ¶ 5.¹ The State sought a warrant to search both phones alleging that police were contacted by Sara Schlesinger, a bookkeeper for Dairy Queen, who reported discovering a \$274.33 paycheck for Mr. Sneed that was cashed by mobile deposit, and provided text messages between herself and Spurling. Pet. App. 98a.² In those messages, Spurling was quoted as saying “it wasn’t meant to happen for real” and that “he didn’t think it would actually work cuz [sic] it wasn’t real.” Pet. App. 98a.

The State asserted that Schlesinger later provided police a second check payable to Mr. Sneed of \$423.22 that was also deducted from Dairy Queen’s account by mobile deposit. Pet. App. 99a. In its warrant complaint, the State sought evidence related to the forging of these checks and any other forged checks, including: photographs or records of paychecks from Dairy Queen; records of text messages and other messaging applications with messages related to the checks; deposit confirmations from banks; and emails, messages, and notifications related to check deposits. Pet. App. 98a. The trial court issued the requested warrant on March 1, 2021. Pet. App. 100a.

¹ All citations to the opinions of the Illinois Supreme Court, *People v. Sneed*, 2023 IL 127968, and the Illinois Appellate Court, *People v. Sneed*, 2021 IL App (4th) 210180, 187 N.E.3d 801, contained in the appendix, also include citation to the relevant paragraphs marked within those opinions.

² The State’s warrant complaint and the search warrant appear in the appendix (Pet. App. 98a-100a) as reproduced in the official record filed with the appellate court below.

On March 5, 2021, the State filed a motion to compel production of a cellular phone passcode, which stated that both phones were passcode protected, preventing law enforcement from searching them. Pet. App. 101a-102a.³ The State asked that the court issue an order compelling Mr. Sneed to provide or enter the passcode to the phone seized from him (the State made no request concerning Spurling or the phone seized from her). Pet. App. 108a. In support, the State argued that the Fifth Amendment did not protect Mr. Sneed from being compelled to provide the passcode to the phone seized from him, where the ownership of the phone was a foregone conclusion and the State had sufficiently identified the contents of the phone that it was seeking through obtaining the search warrant. Pet. App. 106a-108a.

Trial counsel for Mr. Sneed filed a response to the State's motion arguing that the compelled disclosure of the passcode would violate the Fifth Amendment protection against self-incrimination. Pet. App. 109a-111a. In particular, counsel argued that there was a nationwide split over: (1) whether the "foregone conclusion exception" to Fifth Amendment protection applied to all requests to compel a passcode; and (2) if the "exception" was applicable, whether it was focused on the passcode itself or the files protected by the passcode. Pet. App. 110a. Based on the only binding Illinois precedent at the time, *People v. Spicer*, 2019 IL App (3d) 170814, counsel argued that the State had only speculated about what might be beyond the passcode wall, that the existence of the evidence it was seeking was not a foregone conclusion, and that compelling the passcode would violate the Fifth Amendment. Pet. App. 110a-111a.

³ The State's motion appears in the appendix (Pet. App. 101a-108a) as it was reproduced in the official record filed with the appellate court below, with the final two pages (pp. 7-8), out of order. Pet. App. 107a-108a.

The trial court held a hearing at which the lead detective, Todd Ummel, testified regarding the State's investigation and the information alleged in its warrant request. Pet. App. 4a-5a, ¶¶ 13-16. After argument from the parties, the court identified *Fisher v. United States*, 425 U.S. 391 (1976), as the seminal case under which an act of production can be considered testimonial for purposes of applying Fifth Amendment protection, and opined that a reasonable judge might find that producing the passcode here would not be testimonial. Pet. App. 90a-92a. However, the court recognized that the *Spicer* case held such production was testimonial, and that the evidence applicable to the foregone conclusion rationale would be the contents of the phone. Pet. App. 92a-93a. Applying *Spicer*, the court held that the State had not established particular knowledge of the existence of the evidence it sought, Mr. Sneed's possession of it, or its authenticity, and that it could not find such evidence was more likely to be found on the phone seized from Mr. Sneed than on the one seized from Spurling. The court then denied the State's motion to compel production of a passcode from Mr. Sneed. Pet. App. 95a-97a.

The State appealed the trial court's ruling, and the Fourth District of the Illinois Appellate Court reversed. Pet. App. 59a-60a, ¶ 2. The appellate court, disagreeing with the *Spicer* case, found that the trial court's denial of the motion to compel was incorrect for two independent reasons: (1) providing a passcode or entry to a phone is not compelled testimony within the meaning of the Fifth Amendment (Pet. App. 73a-75a, ¶¶ 58-63), and (2) the proper focus of the foregone conclusion rationale is on the passcode itself (Pet. App. 77a-81a, ¶¶ 72-87). Pet. App. 8a-9a, ¶¶ 27-29. The court held that the State met the requirements of the foregone conclusion doctrine by showing a passcode existed, that the phone at issue was seized from Mr. Sneed, and that the passcode was

“self-authenticating” because its authenticity would be shown once it is entered into the phone. Pet. App. 84a-85a, ¶¶ 97-103. The appellate court held that this placed the production of a passcode outside the Fifth Amendment’s protection against self-incrimination. Pet. App. 75a, 84a-85a, ¶¶ 63, 102. It reversed the trial court’s decision (Pet. App. 85a, ¶ 108), and Mr. Sneed appealed. Pet. App. 9a, ¶ 30.

On June 15, 2023, the Illinois Supreme Court affirmed the judgement of the appellate court on slightly different grounds. Pet. App. 1a, 2a, ¶ 3. In front of the Illinois Supreme Court, the State sought only the entry of the passcode into the phone at issue (rather than disclosure of the passcode to police), and conceded that such an act would be testimonial. Pet. App. 18a, ¶ 69. The court agreed, finding that the compelled entry of a passcode was testimonial because the ability to unlock the phone established that the passcode exists, the person producing the passcode possesses or controls it, and the passcode produced is authentic. Pet. App. 20a, ¶ 78. In so finding, the court compared a passcode to a key for a container, and disagreed with the argument that entry of a passcode was testimonial because it required delving into the contents of a defendant’s mind. However, because it was testimonial based on the facts it implied about a passcode, the court found the Fifth Amendment was implicated, and a foregone conclusion analysis was warranted. Pet. App. 21a-22a, ¶¶ 82-85.

The Illinois Supreme Court found that the foregone conclusion doctrine was applicable to the compelled entry of a passcode, rejecting Mr. Sneed’s argument that it was historically applied to the production of subpoenaed tax documents and business records and should not be extended to passcode production. Pet. App. 23a, 26a, ¶¶ 89, 102. The court then held that the proper focus of a foregone conclusion analysis was on the

passcode and not the contents of the phone where the act being compelled was entry of the code, overruling the *Spicer* case. Pet. App. 26a-27a, ¶ 104. The court found that the State had met its burden under the foregone conclusion doctrine by showing: (1) that a passcode existed because the phone was passcode protected, (2) that Mr. Sneed possessed the passcode because the phone was seized from him and he had identified the phone number as his own, and (3) that the passcode would “self-authenticate” by opening the phone once entered. Pet. App. 27a-28a, ¶¶ 106-12.

The court further rejected Mr. Sneed’s state law claims (Pet. App. 10a-18a, ¶¶ 36-67), including finding there were no grounds to justify interpreting the Illinois constitution’s right against self-incrimination more expansively than the same right under the federal Fifth Amendment. Pet. App. 17a-18a, ¶¶ 64-67. In doing so, the court rejected Mr. Sneed’s argument that it should not apply the *Fisher* case, where the Illinois constitution provided that a person could not be compelled to “give evidence against himself.” Pet. App. 17a, ¶ 65. One justice dissented on this basis, reasoning that the State constitution should be interpreted as forbidding orders compelling individuals to produce self-incriminating documents, and rejecting the foregone conclusion doctrine as applicable to bypass the right against self-incrimination. Pet. App. 30a-58a, ¶¶ 120-214. However, relying on *Fisher*, the majority concluded that the foregone conclusion doctrine applied as an exception to the Fifth Amendment right in this case, affirming the judgment of the appellate court, and reversing the decision of the trial court. Pet. App. 28a-29a, ¶¶ 113-16.

This petition follows.

REASONS FOR GRANTING THE PETITION

This case presents critical questions about the nature and scope of our fundamental right against self-incrimination, enshrined in the Fifth Amendment. In particular, it raises concerns with the application of this Court's decision in *Fisher v. United States*, 425 U.S. 391 (1976), to permit a government to obtain potentially incriminating information from a criminal defendant through the harsh expedient of compelled action, and regarding the amount of effort the government must expend before being permitted to take advantage of such compulsion. The resolution of these issues by this Court is necessary, because they have caused a significant split of authority among the decisions of both state and federal courts of last resort. The questions presented are also important, as the widespread use of personal cellular phones, and the desire by law enforcement to access them, makes it highly likely that these issues will continue to reoccur. Additionally, the decision below was wrong in its interpretation of the Fifth Amendment and the forgone conclusion rationale, and this case provides an excellent vehicle through which this Court can resolve that misinterpretation. Furthermore, the issues involved have developed from a fundamental shift in our understanding of what it means to be a witness against oneself, and this Court's consideration is needed to clarify the boundaries of the right against self-incrimination.

For these reasons, this Court should grant Mr. Sneed's petition for a writ of certiorari.

I. There is a growing nationwide conflict among state and federal courts over the application of Fifth Amendment protections to the compelled production and use of passcodes for digital devices, and the scope of the foregone conclusion rationale as an exception.

The decision of the Illinois Supreme Court below is in direct conflict with decisions in other state supreme courts and the federal circuit courts of appeal. There are two major conflicts that this decision presents. The first is over the question of whether the

production or entry of a passcode for a digital device fits under the act of production doctrine, such that the government can utilize the foregone conclusion rationale to engage in compulsion of that act. By finding that the rationale is an exception to Fifth Amendment protection that can be used in this manner, the Illinois Supreme Court directly disagreed with the Pennsylvania Supreme Court, which found that the compelled production of computer passwords does not fit within such an exception.

The second conflict is about how this “foregone conclusion exception” works if it is applied. In particular, whether a government entity seeking compulsion must establish: (1) only knowledge of the existence of the passcode and the defendant’s possession of the device, or (2) knowledge of the existence, possession, and authenticity of specific evidence within the device the passcode is alleged to unlock. In holding that the State was only required to establish knowledge that a passcode existed and that Mr. Sneed was in possession of the phone at issue, the Illinois Supreme Court’s decision conflicts with both state and federal courts that have held that a government must demonstrate knowledge about the files and information that would be produced from within the device. These conflicts deepen the growing dispute in courts across the nation over whether the foregone conclusion rationale can or should be utilized to bypass the Fifth Amendment right. This Court’s intervention is necessary to resolve that dispute, and prevent the whittling away of our fundamental right against self-incrimination.

A. There is a divide among state supreme courts over whether the foregone conclusion rationale is an exception that applies to the compelled production or entry of a passcode.

In *Commonwealth v. Davis*, 656 Pa. 213, 238-40 (2019), the Pennsylvania Supreme Court determined that what it called the “foregone conclusion exception” did not apply to the compelled production of computer passwords at all. There, a defendant was charged

with disseminating child pornography, and refused to provide the password for a computer that police had obtained from his home pursuant to a search warrant. *Davis*, 656 Pa. at 218-20. When the Commonwealth moved to compel the defendant to divulge the password, the trial court applied the foregone conclusion exception and granted the Commonwealth's motion. *Id.* at 220-21. But on review, the Pennsylvania Supreme Court rejected the application of the exception, finding that it "constitutes an extremely limited exception to the Fifth Amendment privilege against self-incrimination." *Id.* at 236-37.

The court found that disclosing a password was testimonial where there was no physical manifestation of a password, and that "the Commonwealth [was] seeking the electronic equivalent to a combination to a wall safe . . . not as an end, but as a pathway to the files being withheld." *Id.* at 235. The court then described this foregone conclusion "exception," as articulated in *Fisher v. United States*, 425 U.S. 391 (1976), and its progeny, as requiring that the government "establish its knowledge of: (1) the existence of the evidence demanded; (2) the possession or control of the evidence by the defendant; and (3) the authenticity of the evidence." *Davis*, 656 Pa. at 236. In rejecting its application to computer passwords, the court reasoned that the right against self-incrimination is foundational, and that any exception to it must be extremely limited in its scope. *Id.* at 236-37.

In particular, the kinds of business and financial records that the foregone conclusion rationale had been applied to in the past were a unique category of material that had long been subject to compelled production. *Id.* at 237 (citing *Shapiro v. United States*, 335 U.S. 1, 33 (1948)). Prohibiting the rationale's application to the "compulsion of one's mental processes" would be consistent with this Court's precedents, which the *Davis*

court said “uniformly protect information arrived at as a result of using one’s mind.” *Id.* at 238. Despite the potential difficulty to the government, the *Davis* court determined that “to apply the foregone conclusion rationale in these circumstances would allow the exception to swallow the constitutional privilege.” *Id.* Therefore, it concluded that compelling the password to a computer was a protected act and did not fit within the rationale. *Id.* at 239-40; *see also State v. Valdez*, 482 P.3d 861, 873-76 (Utah Ct. App. 2021) (coming to the same conclusion as to the disclosure of a passcode).

The Indiana Supreme Court has also indicated that the foregone conclusion rationale should not be extended to permit the compelled entry of a passcode into a phone. *Seo v. State*, 146 N.E.3d 952, 958-62 (Ind. 2020). In *Seo*, police took possession of the defendant’s locked phone when she was arrested for charges based on claims of stalking and harassment, and police then obtained a search warrant compelling her to unlock the phone. 146 N.E.3d at 953-54. She refused to unlock the phone, and was ultimately held in contempt. *Id.* On appeal, the Indiana Supreme Court held that, even if the foregone conclusion rationale was an applicable exception, the State had failed to make the showing necessary to meet its requirements. *Id.* at 958. In making this decision, the court said the case “underscores several reasons why the narrow exception may be generally unsuitable to the compelled production of any unlocked smartphone[,]” and specifically asserted that “such an expansion (1) fails to account for the unique ubiquity and capacity of smartphones; (2) may prove unworkable; and (3) runs counter to U.S. Supreme Court precedent.” *Id.* at 958-59.

The Indiana Supreme Court highlighted this Court’s caution that (*id.* at 961), “[w]hen 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). It further noted that *Fisher* was the only decision by this Court to ever find that the rationale applied in the over 40 years since it was issued. *Seo*, 146 N.E.3d at 961. Because the rationale was crafted in a “vastly different context,” the Indiana Supreme Court concluded (without ultimately making a pronouncement on its validity) that extending it would not only expand an otherwise limited legal “exception,” but would also narrow a constitutional right. *Id.* at 962.

However, in this case the Illinois Supreme Court squarely rejected the reasoning of both *Seo* and *Davis*, and determined that a foregone conclusion analysis was applicable to determine if the State was permitted to compel the production of a passcode to a cellular phone. Pet. App. 23a-26a, ¶¶ 89-102. It was not the first to do so, and it joined the position of the New Jersey Supreme Court, which had also disagreed with *Davis* in *State v. Andrews*, 243 N.J. 447, 473-75, 478-80 (2020). The *Andrews* court utilized a foregone conclusion analysis to determine that the State there could compel the disclosure of passcodes to two cell phones that had been seized from the defendant. *Andrews*, 243 N.J. at 456, 478-81.

Here, the Illinois Supreme Court followed the same path. It stated that “[t]he foregone conclusion doctrine is an exception to the fifth amendment privilege.” Pet. App. 22a, ¶ 87. It found that the concerns expressed by the Pennsylvania and Indiana Supreme Courts, particularly regarding the distinct nature of cellular phones and electronic devices, were irrelevant to the application of the foregone conclusion rationale. Pet. App. 25a-26a, ¶¶ 98-101. It concluded that nothing in the history of the rationale suggested that it could not be applied to the act of producing a cellular phone passcode. Pet. App. 26a, ¶ 102. As such, it applied the rationale, and ultimately found that it obviated Fifth Amendment protection for Mr. Sneed. Pet. App. 29a, ¶ 115.

The Illinois Supreme Court's decision directly split with the Pennsylvania Supreme Court over whether the foregone conclusion rationale can be applied to orders compelling passcode production. It also split from the reasoning of the Indiana Supreme Court, which strongly aligned with the position of Pennsylvania. Only this Court can resolve the conflict created by these decisions.

B. There is a divide among federal courts of appeal and state supreme courts over the proper focus of a foregone conclusion analysis.

The Illinois Supreme Court's decision in this case also contributes to a split among federal and state courts over how the foregone conclusion rationale should function when it is applied as an exception. In the *Seo* case, the Indiana Supreme Court thought beyond the question of whether this "foregone conclusion exception" should be applied, and considered whether the State could meet its requirements if such an exception was utilized. 146 N.E.3d at 955-58. In doing so, the court observed that entering a password to unlock a phone is analogous to the physical act of handing over documents, and that the files on the phone were analogous to the documents ultimately produced. *Id.* at 957. As such, to meet the requirements of the rationale, the State must show it already knew that: (1) the suspect knows the password, (2) the files on the device at issue exist, and (3) the suspect possessed those files. *Id.* at 957-58. The court concluded that, even if it assumed the defendant knew the password for the phone at issue, the "exception" did not apply because the State had failed to demonstrate that any particular files existed on the device or that the defendant possessed those files. *Id.* at 958; *see also G.A.Q.L. v. State*, 257 So. 3d 1058, 1063-65 (Fla. 4th Dist. Ct. App. 2018) (also concluding that the State must establish knowledge of files within a phone); *Pollard v. State*, 287 So. 3d 649, 653-57 (Fla. 1st Dist. Ct. App. 2019) (same).

This same analysis of the foregone conclusion rationale was used by the Eleventh Circuit Court of Appeals. *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1346-48 (11th Cir. 2012). In that case, law enforcement seized several devices from a John Doe, but could not access portions of multiple hard drives due to encryption. *In re Grand Jury Subpoena*, 670 F. 3d at 1339. A grand jury subpoena was issued requiring Doe to produce the unencrypted contents of the devices. *Id.* The Eleventh Circuit held that compelling Doe to decrypt the hard drives implicated his Fifth Amendment right against self-incrimination, and that the testimony inherent in using a decryption password included Doe’s (1) knowledge of the existence and location of potentially incriminating files; (2) his possession, control, and access to the encrypted portions of the hard drives; and (3) his capability to decrypt the files. *Id.* at 1346. As such, the government had not shown that information to be a foregone conclusion, where it did not show that it knew whether any files existed and were located on the hard drives, that Doe had access to such files, or that he was capable of decrypting them. *Id.* at 1346-47, 1349.

Relying on this decision, the Third Circuit applied the same formulation of the foregone conclusion analysis in *United States v. Apple MacPro Computer*, 851 F.3d 238, 247-48 (3rd Cir. 2017). There, the Third Circuit upheld an order requiring the defendant to produce devices that had been seized from him in “a fully unencrypted state.” *Apple MacPro Computer*, 851 F.3d at 246. In doing so, the court recognized the Eleventh Circuit’s understanding of the foregone conclusion rationale and determined that, unlike in the Eleventh Circuit’s case, the government established a foregone conclusion by providing evidence to show that relevant files existed on the encrypted portions of the devices at

issue, and that the defendant could access them. *Id.* at 248. However, in a footnote, the Third Circuit acknowledged that there was also an argument that the foregone conclusion analysis should focus only on whether the government had knowledge that the defendant knew the password at issue. *Id.* at 248 n.7.

While the Third Circuit did not base its decision on that argument, the Illinois Supreme Court in this case did, splitting from the decisions of Indiana and the federal circuits by determining that knowledge about the passcode itself was all the State needed to demonstrate to establish a foregone conclusion. Pet. App. 26a-27a, ¶ 104. In making this determination, the Illinois Supreme Court joined the position established by previous decisions in the Massachusetts Supreme Judicial Court and the New Jersey Supreme Court, similarly finding that the constitutional protection can be overcome by a government establishing knowledge of a passcode's existence and possession of a phone, rather than knowledge about the files and information sought within the device being unlocked. *See Commonwealth v. Gelfgatt*, 468 Mass. 512, 523-24 (2014); *Andrews*, 243 N.J. at 480-81; *see also State v. Stahl*, 206 So.3d 124, 137-36 (Fla. 2d Dist. Ct. App. 2016); and *State v. Pittman*, 367 Or. 498, 517-18, 523-25 (2021) (making a similar analysis on state law grounds).

These splits over the proper application and function of the foregone conclusion rationale, in the context of decrypting digital devices, have been developing for over a decade now. *See* Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 Tex. L. Rev. 767, 769 (2019). Other courts and legal scholars have recognized the national disagreement and have taken similarly opposing stances. *See, e.g.,* Kerr, *supra*, at 768 n.4 (collecting cases), and at 782-85 (arguing that the foregone conclusion rationale should apply when the government can establish independent

knowledge that the person knows the password); Laurent Sacharoff, *What am I Really Saying When I Open my Smartphone? A Response to Orin S. Kerr*, 97 *Tex. L. Rev. Online* 63, 71-72 (2019), and Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 *Fordham L. Rev.* 203, 235-37 (2018) (arguing that to satisfy a foregone conclusion analysis the government should be required to show knowledge of particular files on the device at issue).

In sum, lower courts are thoroughly divided over both the scope of this foregone conclusion rationale, and the manner of its application, if indeed it is appropriate to employ. The decision of the Illinois Supreme Court considered both of these questions, and conflicted with state supreme courts and federal circuit courts of appeal in its conclusions. Only this Court's intervention can resolve the deep split among these courts.

II. The questions at issue present important and recurring concerns for criminal cases throughout the country due to the ubiquity of personal electronic devices, and the governmental desire to access them for criminal investigations.

The widespread use of cellular phones and similar digital devices makes resolution of the questions presented important not only to Mr. Sneed, but to everyone who uses such devices on a daily basis. The disparate application of the Fifth Amendment protection, caused by the conflicting interpretations of the courts, will continue to create confusion among both those asserting their right against self-incrimination and law enforcement agencies that seek to access digital devices. Without action by this Court, questions about when and how to apply the foregone conclusion rationale to governmental efforts to compel production and entry of passcodes are likely to continue arising for the foreseeable future.

As the Indiana Supreme Court observed, “[s]martphones are everywhere and contain everything.” *Seo v. State*, 146 N.E.3d 952, 959 (Ind. 2020). According to the Pew Research Center, in 2021, 97% of Americans owned a cellular phone of some kind, and 85% owned

a “smartphone,” which was an increase from 35% in 2011. Pew Res. Ctr., *Mobile Fact Sheet* (April 7, 2021), <https://www.pewresearch.org/internet/fact-sheet/mobile/>. In addition, 77% of adults owned a desktop or laptop computer, and 53% owned a tablet computer. *Id.* This Court has recognized the pervasiveness of cell phones and similar devices, and that they can create unique problems for interpreting and applying existing legal rules and constitutional precedents. See *Riley v. California*, 573 U.S. 373, 385-86 (2014); see also *Carpenter v. United States*, 138 S. Ct. 2206, 2222 (2018). The extensive use of digital devices, particularly cell phones, means that questions about access to such devices, and the lawfulness of refusing access, will continue to arise.

Following the Pennsylvania Supreme Court’s decision in *Davis*, the attorneys general of 22 states urged this Court to resolve the growing split over whether a person can be compelled to unlock an electronic device (discussed in Argument I, *supra*), stating that the answer “could affect almost every criminal case.” Brief of *Amici Curiae* States of Utah *et al.* Supporting Petitioner at 1, *Pennsylvania v. Davis*, 141 S. Ct. 237, *denying certiorari* (May 26, 2020) (No. 19-1254). Indeed, the use of digital evidence and concern with obtaining it, is significant. An industry survey by Cellebrite, a prominent company that provides law enforcement agencies with products to obtain access to locked phones, see *Seo*, 146 N.E.3d at 962, recently found that 66 % of such agencies believed that evidence obtained from digital devices was more significant than physical evidence and DNA in successfully prosecuting cases. News Release, Cellebrite, *Cellebrite’s 2022 Industry Trends Survey Reveals the Digital Evidence ‘Tipping Point’ has Been Reached, Creating New Challenges for Law Enforcement Agencies* (Nov. 14, 2022), <https://investors.cellebrite.com/node/7336/pdf>. One Cellebrite official commented that

the common misconception of evidence gathering as “all about plastic bags, fingerprints, and DNA swabs . . . fundamentally ignores the massive, growing role that digital evidence plays.” *Id.*

A report by the non-profit organization Upturn, concerned with the use of forensic tools like those offered by Cellebrite, found that at least 2,000 law enforcement agencies across the country—found in all 50 states and the District of Columbia—have purchased and used such tools to extract data. Logan Koepke, et al., *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones*, pp. 32-33 (Oct. 2020), <https://www.upturn.org/static/reports/2020/mass-extraction/files/Upturn%20-%20Mass%20Extraction.pdf>. According to Upturn, these tools have been used “tens of thousands of times, as an all-purpose investigative tool, for an astonishingly broad array of offenses, often without a warrant. And their use is growing.” *Id.* at 40.

Legal scholars have similarly recognized the importance of questions related to digital device access, and of the debate over compelled passcode use in particular. Indeed, at least one has said that “[c]ompelled decryption is the most important self-incrimination issue of the digital age.” David Rassoul Rangaviz, *Compelled Decryption & State Constitutional Protection Against Self-Incrimination*, 57 *Am. Crim. L. Rev.* 157, 157 (2020). The questions presented by this case have proliferated largely because of the significant increase in the use of cell phones and similar devices, and the growing use of encryption to protect the information within them. *See* Rangaviz, *supra*, at 157; Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 *Tex. L. Rev.* 767, 768 (2019)[hereinafter Kerr, *Compelled Decryption*]; *see also* Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 *Geo. L. J.* 989, 990-91 (2018). Professors Orin Kerr and Laurent Sacharoff, two prominent scholars with opposing views on the application of

the foregone conclusion rationale, have both recognized a shift in the balance of power between the government and the citizen due to the proliferation of phones and encryption. Kerr, *Compelled Decryption*, *supra*, at 770; Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 Fordham L. Rev. 203, 205 (2018)[hereinafter Sacharoff, *Unlocking*].

In Professor Sacharoff's estimation, the trend towards more encryption comes from citizens seeking greater privacy protection for personal papers. Sacharoff, *Unlocking*, *supra*, at 205. This, he believes, fills a gap left in the constitutional protection against self-incrimination by this Court's decision in *Fisher v. United States*, 425 U.S. 391 (1976), from the apparent rejection of the previous rule stated in *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 testimonial communications. *See* Sacharoff, *Unlocking*, *supra*, at 205.

Some scholars have expressed concern that encryption shifts the balance too much in favor of citizens, and argue that interpretation of the Fifth Amendment should protect the public interest in criminal investigation. *See* Kerr, *Compelled Decryption*, *supra*, at 770; *see also* Kirstyn Watson, Comment, *Under Digital Lock and Key: Compelled Decryption and the Fifth Amendment*, 126 Penn. St. L. Rev. 577, 603-07 (2022). Others join Professor Sacharoff in arguing that applying the foregone conclusion rationale to permit compelled decryption will not restore balance, but instead give the government an unprecedented ability to scour personal information that did not previously exist, and result in an impermissible narrowing of the right against self-incrimination. *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, 72 (2019); Rangaviz, *supra*, at 196-206;

see also Adriana Christianson, Note, *Locked Out or Locked Up: The Need for New Guidelines for Compelled Decryption*, 55 Suffolk U. L. Rev. 237, 257-62, 265-66 (2022); Aubrey Zimmerling, *Actions Speak Louder than Words: Compelled Biometric Decryption is a Testimonial Act*, 100 Wash. U. L. Rev. 827, 843-58 (2023).

For as long as government law enforcement agencies wish to make some use of the ever growing amount of information stored in personal digital devices, they will undoubtedly continue to seek access to such devices through the compelled disclosure or entry of passcodes. In short, the questions presented by this case have been “bedeviling courts and scholars[,]” for some time. Sacharoff, *Unlocking*, *supra*, at 207 (omitting footnotes). They will certainly continue to do so until this Court takes action.

III. The decision of the Illinois Supreme Court applying the forgone conclusion rationale as an exception to Fifth Amendment protection was incorrect, and this case cleanly presents the questions underlying that application, making it a good vehicle for their resolution.

Mr. Sneed asserted his right against self-incrimination at the outset of this case, in the trial court, in direct response to the State’s motion to compel him to produce a passcode. Pet. App. 109a-111a. In particular, he identified the nationwide split in authority (*see* Argument I, *supra*) on both the application of the foregone conclusion rationale to requests to compel passcodes, and on the proper focus of the rationale if it is applied. Pet. App. 110a. As such, these questions were fully preserved and properly presented to the lower courts on appeal.

Additionally, the case arises from pre-trial proceedings, and the court below fully addressed both questions, leaving no potential issues of harmless error or any procedural barriers to the decision of this case. Indeed, both issues were squarely addressed by the Illinois Supreme Court and resolved on their merits. Pet. App. 22a-27a, ¶¶ 86-104. Further, in resolving them, the court specifically discussed the extent to which it believed

that the act of entering a passcode was testimonial, as the foundation for why it ultimately determined that the foregone conclusion rationale was applicable as an exception, negating the value of that testimony. Pet. App. 19a-22a, 29a, ¶¶ 71-85, 115. As such, this case cleanly and fully presents the questions of whether the foregone conclusion rationale should apply as an exception that permits the compelled entry of a passcode—and if so, how it should work—for this Court to consider and resolve.

Furthermore, the Illinois Supreme Court’s decision is wrong as to both of the questions presented on the foregone conclusion rationale’s application. This case presents an opportunity for this court to correct those errors, and to clarify its holding in *Fisher v. United States*, 425 U.S. 391 (1976), as well as the scope of its impact on the right against self-incrimination.

A. The Illinois Supreme Court erred in applying the foregone conclusion rationale as an exception beyond the production of the kinds of third-party records that it was created to address.

The court below held that a foregone conclusion analysis was applicable in this case, concluding that “there is nothing in the history of the foregone conclusion doctrine to suggest that it does not apply to acts of producing passcodes to cell phones.” Pet. App. 26a, ¶ 102. In doing so, it rejected *Commonwealth v. Davis*, 656 Pa. 213 (2019), as inapplicable, asserting that the Pennsylvania Supreme Court incorrectly conflated the testimonial nature of a person disclosing the contents of his mind with the inapplicability of the foregone conclusion rationale. Pet. App. 25a, ¶ 98. Instead, the court reasoned that information being disclosed from a person’s mind has no bearing on the rationale’s application, and it is because an act of production is testimonial that a foregone conclusion analysis becomes necessary. Pet. App. 25a, ¶ 98. However, the court misunderstands *Davis*, and ignores the primary reason that the rationale is not applicable as an exception in this case.

The foregone conclusion rationale can only properly function as it was created when applied to documents that involve a third party. Historically, this Court has only considered the rationale in cases where the government sought production of tax documents or business records through a summons or subpoena. *See Fisher*, 425 U.S. at 393-95; *United States v. Doe*, 465 U.S. 605, 606-07 (1984); *United States v. Hubbell*, 530 U.S. 27, 30-31 (2000). Of those cases, only *Fisher* found the rationale’s requirements had been met as to tax documents that had been specifically identified by the government in their summonses, and which had been created by third-party accountants. *Fisher*, 425 U.S. at 394, 410-11; *see also Hubbell*, 530 U.S. at 44-45. The reason the documents were considered a foregone conclusion was because they were prepared by accountants who could independently confirm their existence and authenticity. *Fisher*, 425 U.S. at 411-13; *Hubbell*, 530 U.S. at 44-45. So the government was not relying on the “truth-telling” of the taxpayers to establish the relevant factors (existence, possession, or authenticity). *See Fisher*, 425 U.S. at 411.

In making that determination, this Court also specifically noted that it had repeatedly permitted the compelled production of corporate documents, and those of similar collective entities, by the custodians of such documents—despite any implied admissions about the existence and location of such documents that doing so would entail. *Id.* at 411-13 (*citing In re Harris*, 221 U.S. 274 (1911); *Wilson v. United States*, 221 U.S. 361 (1911); *Dreier v. United States*, 221 U.S. 394 (1911); *United States v. White*, 322 U.S. 694 (1944); and *Bellis v. United States*, 417 U.S. 85 (1974)). The *Davis* court made a similar connection in choosing not to apply the foregone conclusion rationale as an exception, stating that “business and financial records are a unique category of material that has

been subject to compelled production and inspection by the government for over a century.” 656 Pa. at 237 (citing *Shapiro v. United States*, 335 U.S. 1, 33 (1948)). So it is not that passcodes and the digital devices they unlock should enjoy unique protection under the Fifth Amendment, but rather that business and financial documents—which are necessarily within the knowledge and testimonial capabilities of third-parties—fall within the foregone conclusion rationale specifically because they are uniquely *unprotected* by the Fifth Amendment.

Moreover, the implications of producing documents that the government has specifically identified—because it has knowledge of them from a third party—might reasonably be limited to the existence, location, and authenticity of those documents. The same is not true where the government does not have knowledge from a third party of what is being produced, as is the case with the broad production of an unencrypted device. Here, the Illinois Supreme Court took issue with the *Seo* court’s concern that the high data storage capacity of cell phones made the foregone conclusion rationale unworkable, asserting that cell phone capacity was only relevant to a Fourth Amendment analysis of the scope of a search, and not relevant at all to whether the rationale applied. Pet. App. 25a-26a, ¶¶ 99-101. The court based this on its determination that the act of entering a passcode is testimonial only to the extent that it implicitly asserts that: “(1) the passcode exists, (2) the person producing the passcode possesses or controls it, and (3) the passcode produced is authentic.” Pet. App. 20a, ¶ 78.

However, this ignores the fact that all testimony involved in an act of production is made by implication. Such testimony is entirely 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)

[hereinafter Sacharoff, *What Am I Really Saying*]. 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). The Illinois Supreme Court's determination too narrowly limits that testimony to only the most superficial inferences.

The testimony inherent in producing specifically identified documents under a subpoena may be limited to the documents' existence, possession, and authenticity, because the documents have already been specifically identified. *See, e.g., Fisher*, 425 U.S. at 410-11. By contrast, the rationale's strictures are not met where documents are compelled through an overly broad subpoena and the government cannot show that it had prior knowledge of what was being produced through independent sources. *See, e.g., Hubbell*, 530 U.S. at 43-45. Indeed, this Court's discussion of immunity in the *Hubbell* case made the necessity of fully independent sources clear. When an individual gives up the right against self-incrimination under a grant of immunity—coextensive with the scope of the right—the prosecution has an affirmative duty “to prove that the evidence it proposes to use is derived from a legitimate source wholly independent of the compelled testimony[.]” if it wishes to prosecute the individual on matters about which he has produced information. *Hubbell*, 530 U.S. at 38-40 (*quoting Kastigar v. United States*, 406 U.S. 441, 460 (1972)). No less should be required where the right is being forcibly stripped away without a grant of immunity. Without the clear involvement of a third party to give the government prior knowledge of everything that will be produced, independent from the knowledge gleaned through the act of production, it would be a significant expansion of the foregone

conclusion rationale to apply it to the compelled entry of a passcode and the resultant production of the unencrypted contents of a cell phone. The Illinois Supreme Court was incorrect to do so.

Even if this Court ultimately disagrees, and finds that the foregone conclusion rationale can be applied as an exception in such circumstances, the Illinois Supreme Court was also incorrect when it determined that the rationale's focus must be on information about the passcode instead of any files or information within the phone.

B. The Illinois Supreme Court erred in focusing the foregone conclusion analysis on the State's knowledge about the existence of a passcode, rather than its knowledge about the unencrypted contents of the phone that would actually be produced.

Upon finding that a foregone conclusion analysis was applicable, the court below held that the proper focus of the analysis was on the passcode itself. Pet. App. 26a-27a, ¶ 104. The court reasoned that the act at issue was the act of entering the passcode, that the State did not request production of information contained on the phone, and that focusing the analysis on the contents of the phone would disregard the fact that access to the phone passed a probable cause determination when a search warrant was issued. Pet. App. 26a-27a, ¶ 104. Applying this analysis, the court found that the State knew a passcode existed because the phone at issue was passcode protected, that it knew Mr. Sneed possessed the passcode because the phone was seized from him and he used the number for the phone on his bond paperwork, and that the passcode was "self-authenticating" because its authenticity would be determined once entered into the phone if it unlocked. Pet. App. 27a-28a, ¶¶ 107-12. This application of the analysis to knowledge of the passcode is wrong for at least three major reasons.

First, what is produced by compelling the disclosure or entry of a passcode, and what the State is actually seeking, are the unencrypted contents of the phone. Particularly here, where the State now seeks only the entry of a passcode into a phone without disclosing it (Pet. App. 18a, ¶ 69n.5), the passcode itself is not being produced at all. In *People v. Spicer*, the previous Illinois appellate court case that was overruled by the decision below (Pet. App. 26a-27a, ¶ 104), the court recognized that “the State is not seeking the passcode *per se* but the information it will decrypt.” 2019 IL App (3d) 170814, ¶ 21 (*relying on G.A.Q.L v. State*, 257 So. 3d 1058, 1063-65 (Fla. 4th Dist. Ct. App. 2018)).

This is consistent with the focus of the foregone conclusion analysis as it was applied to documents. 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. Therefore, it is information about what is actually provided to the government that the government must show it already has existing knowledge of. Put another way, “entering the password to unlock the device is analogous to the physical act of handing over documents . . . [and] the files on the smartphone are analogous to the documents ultimately produced.” *Seo v. State*, 146 N.E.3d 952, 957 (Ind. 2020) (*citing* Sacharoff, *What Am I Really Saying*, *supra*, at 68). Focusing the foregone conclusion analysis on knowledge of only the passcode itself obviates the purpose of the underlying rationale, which is to negate the information implied by handing over the specific evidence the government is actually receiving.

Second, focusing the analysis on the contents of the phone being produced does not somehow negate the effects of the Fourth Amendment under which a search warrant may be authorized. Indeed, this Court explained in *Fisher* the way in which the Fifth Amendment's protections were separate from those in the Fourth:

“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.” *Fisher*, 425 U.S. 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. Even if 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 it would involve 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 presence of a warrant to search the phone has no bearing on whether the compelled act of entering the passcode is separately entitled to protection under the right against self-incrimination. In an effort to tidily separate the Fourth and Fifth Amendment rights, the Illinois Supreme Court's decision here takes away Mr. Sneed's Fifth Amendment right, making it subservient to the State's Fourth Amendment showing of reasonableness, instead of protecting both as distinct and equal rights.

Finally, focusing the foregone conclusion analysis on the passcode necessitates a complete subversion of its core requirement—that the State obtain its knowledge of the evidence independent of, and prior to, the act being compelled—particularly where

focusing on a passcode requires the passcode to “self-authenticate.” At a basic level, 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, What Am I Really Saying, supra*, at 71. Perhaps most importantly though, authentication is entirely dependent on the act of entering the code. The court below adopted the reasoning of the Second District of the Florida Appellate Court (Pet. App. 28a, ¶ 111), which said:

“[T]he act of production and foregone conclusion doctrines cannot be seamlessly applied to passcodes and decryption keys. If the doctrines are to continue to be applied to passcodes, decryption keys, and the like, we must recognize that the technology is self-authenticating—no other means of authentication may exist. [Citation] If the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic.” *State v. Stahl*, 206 So.3d 124, 136 (Fla. 2d Dist. Ct. App. 2016).

In other words, because it is impossible for the State to independently authenticate a passcode without the act of entering it to see if it works, the requirements of the analysis must be broken in order to permit compulsion. This is simply incorrect.

The Illinois Supreme Court’s decision ignores the necessity that the State must have sufficient knowledge of existence, possession, and authenticity of the evidence it seeks, at the time it requests compulsion; before the act of production, not after. *See United States v. Greenfield*, 831 F.3d 106, 124 (2d Cir. 2016); *see also Hubbell*, 530 U.S. at 45 (“here the Government has not shown that it had any *prior* knowledge of [the documents produced].” (Emphasis added)). To permit a foregone conclusion analysis to focus on the passcode in this way would be to allow the State to fulfill its obligation by saying, in effect, “[t]urn over the facts we want, and we will tell you if it is authentic or not.” *Davis*, 656 Pa. at 240 n.10. This would flip the analysis on its head, and undermine the core

concern of the foregone conclusion rationale—that the Government’s knowledge about what is being produced not be based on the truth-telling of the person compelled. *Fisher*, 425 U.S. at 411.

In short, the Illinois Supreme Court erred by applying the foregone conclusion rationale to the compelled entry of a passcode, and focusing the analysis on the State’s knowledge of the passcode instead of the unencrypted contents of the phone that would be produced. Only this Court can correct these errors, and resolve the questions presented.

C. This case presents an opportunity for this Court to provide important clarification of its decision in *Fisher* and determine whether the Fifth Amendment contemplates a broader protection against the compelled production of incriminating evidence.

The advent of the foregone conclusion rationale fundamentally altered the scope of the Fifth Amendment’s protection in a way that only this Court can clarify. Part of the foundation for the conflicts over applying the rationale is the interpretation of *Fisher*, and the extent to which it rejected the standard previously recognized in *Boyd v. United States*, 116 U.S. 616, 630, 633-35 (1886), that Fifth Amendment protection encompassed an individual’s private books and papers. *Fisher* did not expressly overrule *Boyd*, and the question of whether the Fifth Amendment might protect against compelled disclosure of purely private material was left undecided. *Id.* at 414. To the extent this resulted in confusion as to the proper application of the foregone conclusion rationale, and a narrowing of the right against-self-incrimination, this case presents an opportunity for this Court to reconsider the question left open in *Fisher* and clarify the original meaning of the Fifth Amendment’s self-incrimination clause as it applies to the production of private materials.

Application of the foregone conclusion rationale as an exception that permits compelled decryption flows from the act-of-production doctrine, which arose from the statement in *Fisher* that only testimonial communications were protected by the Fifth Amendment. 425 U.S. at 408-09. The *Fisher* court determined that the act of producing evidence only enjoyed Fifth Amendment protection to the extent that it had “communicative aspects of its own[.]” *Id.* at 410. However, some legal scholars, including at least two current members of this Court, have expressed serious concerns with the idea that the Fifth Amendment permits the compelled production of private incriminating documents and evidence. See Richard A. Nagareda, *Compulsion “To Be a Witness” and the Resurrection of Boyd*, 74 N.Y.U. L. Rev. 1575, 1577-1579 (1999); *Hubbell*, 530 U.S. at 49-56 (Thomas, J., joined by Scalia, J., concurring); *Carpenter v. United States*, 138 S. Ct. 2206, 2271 (2018) (Gorsuch, J., dissenting). Instead, as Professor Nagareda argued, the historical understanding of the Fifth Amendment’s prohibition against being compelled to “be a witness” is not simply providing oral or written testimony, but included being compelled to “give evidence” against oneself in the form of documents and other items. See Nagareda, *supra*, at 1603-23.

Indeed, the interpretation of *Fisher* as limiting the right against self-incrimination to testimony, without a protection for privately held material, formed a key basis for the dissent in this case. Pet. App. 43a-55a, ¶¶ 169-202. While the majority of the Illinois Supreme Court adhered to the state’s “lockstep” doctrine for interpreting parallel constitutional rights, and rejected Mr. Sneed’s argument that it should not apply *Fisher* to the extent that it limited constitutional protection for private papers (Pet. App. 17a-18a, ¶¶ 64-67), Justice Neville disagreed. Pet. App. 31a, ¶ 127. Among other reasons for his

dissent, Justice Neville argued that *Fisher*, and the majority, ignored the purpose of the constitutional protection against self-incrimination—that criminal proceedings be conducted “upon a plane of dignity, humanity and impartiality.” Pet. App. 45a-46a, ¶ 179 (quoting *United States v. White*, 322 U.S. 694, 698 (1944)). In particular, the protection was designed to prevent forcing evidence from an accused, and to force prosecutors to “search for independent evidence instead of relying upon proof extracted from individuals by force of law.” Pet. App. 45a-46a, ¶179 (quoting *White*, 322 U.S. at 698). Justice Neville concluded that applying *Fisher* in this case would undermine the purpose of the right as previously understood by this Court and Illinois courts; to the extent that *Fisher* would not apply the right against self-incrimination to demands for documents a defendant had written or kept—including the kind of documents that would be decrypted by permitting compulsion here—Justice Neville believed it should be rejected. Pet. App. 46a-49a, ¶¶ 180, 184-87.

Even if the right does not encompass protection against the production of all evidence by an accused, applying it to prevent the compelled production of purely private information, as opposed to information that has been shared or created with third parties, would not be inconsistent with the holding of *Fisher*. The tax documents this Court determined could be compelled in *Fisher* were prepared by third party accountants, and it was through the accountants that the government obtained information about them, independent of any production compelled from the taxpayers. *Fisher*, 425 U.S. at 394-95, 411. This Court specifically stated that “[w]hether the Fifth Amendment would shield the taxpayer from producing his own tax records in his possession is a question not involved here; for the papers demanded here are not his *private papers*[.]” *Id.* at 414 (quotation marks omitted, emphasis added).

By contrast, the information contained within a person’s phone can be considered privately held, containing almost anything and everything personal that someone might hold. *See Seo*, 146 N.E.3d at 959-60 (stating that smartphones “can contain, in digital form, the ‘combined footprint of what has been occurring socially, economically, personally, psychologically, spiritually and sometimes even sexually, in the owner’s life.’” (*quoting United States v. Djibo*, 151 F. Supp. 3d 297, 310 (E.D.N.Y. 2015))). At least one scholar has even suggested that cellular phones in particular should be uniquely protected from compelled production because they functionally operate as a mental prosthetic—an extension of a person’s mind. *See* Bryan H. Choi, *The Privilege Against Cellphone Incrimination*, 97 Tex. L. Rev. Online 73 (2019). The extent to which compelling the production of such private information is permissible remains an open question under *Fisher*.

Further, the validity of using the forgone conclusion rationale as an exception that could overcome the Fifth Amendment right is highly suspect. No exceptions to the right against self-incrimination appear in the text of the Fifth Amendment. U.S. Const. amend. V. Rather, it places a categorical bar on a particular type of governmental action; the compulsion to be a witness against oneself. But lower courts, including the Illinois Supreme Court in this case, have specifically interpreted the foregone conclusion rationale to be an exception to the Fifth Amendment right—a mechanism through which the government is allowed to compel evidence from a person based on a showing of knowledge about the evidence it seeks to compel, even where the action compelled would be testimonial. Pet. App. 22a, ¶ 87 (*citing Fisher*, 425 U.S. at 411).

Yet, permitting compulsion based on the government’s ability to obtain separate evidence poses the danger of obviating any practical protection provided by the right. Essentially, this would be like permitting a confession to be compelled from a suspect

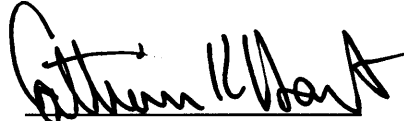
based on the government making some kind of showing that it had amassed sufficient independent evidence to complete its prosecution regardless of the compelled action. *See Goldsmith v. Superior Court*, 152 Cal. App. 3d 76, 87 n.12, 89-90 (3d Dist. 1984) (vacating a trial court order compelling the production of a firearm) *quoting Commonwealth v. Hughes*, 380 Mass. 583, 594 (1980) (“This would be to encourage present infringements of the Constitution on the excuse that they might or would be held ‘harmless’ after trial and conviction.”). By permitting the right against self-incrimination to be overcome by the collection of other independent evidence, application of this exception poses the serious risk of swallowing the constitutional right entirely. *See Commonwealth v. Davis*, 656 Pa. 213, 238 (2019).

This Court should reconsider *Fisher*’s impact on the boundaries of the right against self-incrimination and, if necessary, overrule its limitation of the right to only testimonial evidence. Even if overruling *Fisher* is not necessary, the proper scope and application of the foregone conclusion rationale are important matters for this Court to address in order to mitigate the dangers inherent in its use as an exception to the Fifth Amendment right. This case is an excellent vehicle for reviewing the questions presented about the application of the foregone conclusion rationale, and for clarifying the impact of *Fisher*. As such, this Court should grant Mr. Sneed’s petition, and resolve the conflicts that have plagued lower courts for over a decade (*see* Argument I, *supra*).

CONCLUSION

For the foregoing reasons, petitioner, Keiron K. Sneed, respectfully prays that a writ of certiorari issue to review the judgment of the Illinois Supreme Court.

Respectfully submitted,



CATHERINE K. HART
Counsel of Record
Deputy Defender
Office of the State Appellate Defender
Fourth Judicial District
400 West Monroe Street, Suite 303
Springfield, IL 62704
(217) 782-3654
4thDistrict@osad.state.il.us

JOSHUA SCANLON
Assistant Appellate Defender
Office of the State Appellate Defender
Fourth Judicial District
400 West Monroe Street, Suite 303
Springfield, IL 62704

COUNSEL FOR PETITIONER