No. 127968

IN THE
SUPREME COURT OF ILLINOIS

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

BRIEF OF THE AMERICAN CIVIL LIBERTIES UNION, THE AMERICAN CIVIL LIBERTIES UNION OF ILLINOIS, THE ELECTRONIC FRONTIER FOUNDATION, THE NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, AND THE ILLINOIS ASSOCIATION OF CRIMINAL DEFENSE LAWYERS AS *AMICI CURIAE* IN SUPPORT OF DEFENDANT–APPELLANT

Rebecca K. Glenberg
ARDC No. 6322106
Roger Baldwin Foundation
of ACLU, Inc.
150 N. Michigan Ave., Suite 600
Chicago, IL 60601
(312) 201-9740
rglenberg@aclu-il.org

Counsel for Amici Curiae

E-FILED
6/14/2022 10:22 AM
CYNTHIA A. GRANT
SUPREME COURT CLERK

Additional counsel listed on following page.

On the Brief:

Alexandra Block
ARDC No. 6285766
Rebecca K. Glenberg
Roger Baldwin Foundation of ACLU, Inc.
150 N. Michigan Ave., Suite 600
Chicago, IL 60601

Brett Max Kaufman
American Civil Liberties Union Foundation
125 Broad Street
New York, NY 10004

Jennifer Stisa Granick
American Civil Liberties Union Foundation
39 Drumm Street
San Francisco, CA 94111

Andrew Crocker
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109

William Wolf
William Loeffel
Jonathan M. Brayman
Illinois Association of Criminal Defense Lawyers
1440 W. Taylor St., Suite 811
Chicago, IL 60607

Jonathan M. Brayman
ARDC No. 6302461
Breen & Pugh
National Association of Criminal Defense Lawyers
53 W. Jackson Blvd., Suite 1215
Chicago, IL 60604

POINTS AND AUTHORITIES

FACTUAL BACKGROUND

The State charged the defendant, Keiron K. Sneed, with two counts of forgery, alleging that he had written two false paychecks totaling about $700 from a local Dairy Queen (where his wife, but not he, worked). *People v. Sneed*, 2021 IL App (4th) 210180, ¶¶ 5, 8. During the State's investigation, the bookkeeper for the Dairy Queen franchise provided the State with a text message from the defendant's wife demonstrating her awareness of the false checks. The State obtained a warrant to search the defendant's and his wife's phones to confirm who deposited the false checks and to confirm the authenticity of the text message to the bookkeeper. *Id.* ¶ 9. After obtaining the warrants, the State determined that the defendant's and his wife's phones were locked and password-protected. *Id.* ¶ 12.

The State filed a motion to compel the defendant to enter the passcode to his phone, but the trial court denied the motion. *Id.* ¶ 18. The trial court determined that the compelled entry of a password to unlock and decrypt a digital device was testimonial. *Id.* It further determined that even if the foregone conclusion doctrine applied to this context, the State had not met its burden to satisfy the doctrine in this case because it could not establish with reasonable particularity that it had knowledge of the evidence sought on defendant's phone. *Id.* ¶ 19.

The Appellate Court reversed, holding that compelled entry of a device password is not testimonial, and even if it was, the foregone conclusion doctrine applied to this context and allowed the State to compel the defendant to enter his password to unlock and decrypt his phone. *Id.* ¶¶ 22–24. The Appellate Court expressly disagreed with the rationale

of *People v. Spicer*, 2019 IL App (3d) 170814, ¶ 21, which held that the State could not require a defendant to reveal or enter his phone passcode.

SUMMARY OF ARGUMENT

This case presents important questions of first impression in this Court: whether the privileges against self-incrimination found in the Fifth Amendment to the United States Constitution and article I, section 10 of the Illinois Constitution[1] preclude the State from forcing a criminal defendant to recall and enter the passcode to his encrypted cell phone, thereby delivering the phone's contents to the government for use against him in a criminal proceeding. They do. Under long-standing precedent, the State cannot compel a suspect to assist in his own prosecution through recall and use of information that exists only in his mind. *See Curcio v. United States*, 354 U.S. 118, 128 (1957). The realities of the digital age only magnify the concerns that animate these state and federal privileges. Here, however, the Appellate Court rejected the application of those privileges, holding that the State could compel Mr. Sneed to deliver information to be used against him in his own prosecution. *Sneed*, 2021 IL App (4th) 210180.

This Court should reverse the Appellate Court's decision for two reasons. First, as numerous state and federal courts have held, entering or disclosing the passcode to a cell phone is testimonial for purposes of the Fifth Amendment because it requires the disclosure of the "contents of one's mind." Courts have only applied the narrow foregone conclusion

[1] As Mr. Sneed points out, article I, section 10 of the Illinois Constitution receives a similar construction to the Fifth Amendment privilege against self-incrimination, but the wording is not identical, and this Court has at times interpreted the state constitution to confer broader rights than the federal privilege. *People v. McCauley*, 163 Ill. 2d 414, 436 (1994). *Amici* take no position on this question.

limitation to acts of production, which this is not. Second, even as applied to acts of production, the foregone conclusion limitation is extremely narrow. The United States Supreme Court has only once ever applied it, and it has no history of application in the lower courts beyond already known and existing business or financial documents. Moreover, even if the foregone conclusion rationale does have bearing in this context, the Appellate Court misapplied.

Despite the modern technological context, this case turns on one of the most fundamental protections in our constitutional system: an accused person's ability to exercise his Fifth Amendment rights by refusing to become a witness against himself. The Founders adopted the Fifth Amendment out of concern about "Star Chamber" practices in England, which compelled individuals to testify against themselves, and thereby imposed on them "the cruel trilemma" of telling the truth, committing perjury, or refusing to answer and facing contempt. *Couch v. United States*, 409 U.S. 322, 327–28 (1973). As the U.S. Supreme Court has summarized, the privilege against self-incrimination "reflects many of our fundamental values and most noble aspirations." *Murphy v. Waterfront Comm'n of N.Y. Harbor*, 378 U.S. 52, 55 (1964), *abrogated on other grounds by United States v. Balsys*, 524 U.S. 666 (1998).

Absent the protection of the Fifth Amendment, the order in this case imposes precisely that "cruel trilemma" on Mr. Sneed. The decision below wrongly allows law enforcement to circumvent this protection and intrude into the inviolable domain of the defendant's mind. This Court should reverse that decision and ensure that the privilege

against self-incrimination enshrined in the Fifth Amendment and article I, section 10 of the Illinois Constitution continue to protect all those accused of crimes in this State.

ARGUMENT

I. Compelling a criminal suspect to enter a passcode is testimony privileged by the Fifth Amendment.

A. The Fifth Amendment prohibits compelled recollection and use of the contents of a suspect's mind to assist in his own criminal prosecution.

The Fifth Amendment guarantees that "[n]o person shall be . . . compelled in any criminal case to be a witness against himself." U.S. Const., amend. V. The privilege against self-incrimination is rooted in our nation's "unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt," "our respect for the inviolability of the human personality and of the right of each individual 'to a private enclave where he may lead a private life,'" and "our realization that the privilege, while sometimes 'a shelter to the guilty,' is often 'a protection to the innocent.'" *Doe v. United States* (*Doe I*), 487 U.S. 201, 212–13 (1998) (quoting *Murphy*, 378 U.S. at 55). Compelled testimony also encroaches on "the right of each individual to a private enclave where he may lead a private life." *Couch*, 409 U.S. at 616 (citing *Murphy*, 378 U.S. at 55 (quotation marks omitted)).

To force a suspect to use his thoughts and memories to assist in a prosecution against himself violates the long-standing principles preserved in the Fifth Amendment. Indeed, compelled entry of a password constitutes a modern form of testimony, which is categorically protected by the Fifth Amendment. Any contrary rule would have drastic consequences for the values that the Fifth Amendment privilege against self-incrimination was meant to safeguard. It would be pure spectacle, and an affront to human dignity, to permit the prosecution to force an accused to answer incriminating questions, make

confessions of guilt, or bring evidence against himself to the police, merely because the authorities believed they already had reliable information concerning the matter. *See, e.g.*, *Pennsylvania v. Muniz*, 496 U.S. 582, 595 (1990) (footnote omitted) (quoting *Doe I*, 487 U.S. at 213) (privilege "spare[s] the accused from having to reveal, directly or indirectly, his knowledge of facts relating him to the offense or from having to share his thoughts and beliefs with the Government"). The privilege is not just about information, let alone information useful to the prosecution—it is about a core of individual autonomy into which the State may not encroach. *See, e.g.*, *United States v. Nobles*, 422 U.S. 225, 233 (1975) ("The Fifth Amendment privilege against compulsory self-incrimination is an 'intimate and personal one,' which protects 'a private inner sanctum of individual feeling and thought and proscribes state intrusion to extract self-condemnation.'" (quoting *Couch*, 409 U.S. at 327)); *Muniz*, 496 U.S. at 596 (privilege prevents cruelty "that defined the operation of the Star Chamber, wherein suspects were forced to choose between revealing incriminating private thoughts and forsaking their oath by committing perjury"); *Doe I*, 487 U.S. at 219 n.1 (Stevens, J., dissenting) (explaining that the Fifth Amendment protects against compelled "intrusion[s] upon the contents of the mind of the accused" because they "invade the dignity of the human mind").

Without the privilege, the defendant and others who use encryption to protect their personal privacy on digital devices would face an unacceptable choice: either truthfully recall and disclose or enter information that will be used to incriminate them; lie about their inability to do so; or be held in contempt for failure to cooperate. The privilege is intended precisely to prevent suspects from facing this "cruel trilemma." *See Doe I*, 487 U.S. at 212

(quoting *Murphy*, 378 U.S. at 55). The Fifth Amendment privilege, and the values that animate it, prohibit this type of government compulsion—full stop.

B. A demand for a suspect's compelled entry of a password to unlock and decrypt a digital device is a demand for his testimony.

To invoke the privilege, an individual must show that the evidence sought is (1) compelled, (2) testimonial, and (3) self-incriminating. *United States v. Hubbell*, 530 U.S. 27, 34 (2000); *People v. Spicer*, 2019 IL App (3d) 170814. Only the second factor is at issue here.

If it is necessary for a person to make extensive use of "the contents of his own mind" in producing information, it is testimonial. *Hubbell*, 530 U.S. at 43 (citing *Curcio v. United States*, 354 U.S. 118, 128 (1957)). The State's demand that Mr. Sneed enter his passcode to open a device necessarily compels him to make use of the contents of his mind by truthfully recalling and entering a memorized passcode. That alone makes the demand one for testimony, even without a verbal disclosure.

Further, the demand would require Mr. Sneed to reveal information about the device and his possession, control, and knowledge of it, as well as about the particular files found there. That is also a demand for his testimony. Therefore, the Appellate Court's conclusion that the State is merely seeking a non-testimonial "act of production" rather than compelled, self-incriminating testimony, is incorrect. *Sneed*, 2021 IL App (4th) 210180, ¶¶ 47–63.

As an initial matter, it is clear that forcing a defendant to *tell* the State his passcode is testimonial because it would "compel [him] to make an express verbal or written statement"; thus, "an order requiring such a statement would be an order compelling testimonial evidence." *State v. Pittman*, 479 P.3d 1028, 1038–39 (Or. 2021);

Commonwealth v. Davis, 220 A.3d 534, 543 (2019), *cert. denied sub nom. Pennsylvania v. Davis*, 141 S. Ct. 237 (2020) ("[t]he vast majority of verbal statements thus will be testimonial"); *see Fisher v. United States*, 425 U.S. 391, 409 (1976) (an order to "compel oral testimony" would violate the Fifth Amendment). On this point, federal courts agree: production of computer passwords is testimonial because it requires the suspect "to divulge[,] through his mental processes[,] his password." *United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010); *see also, e.g.*, *United States v. Wright*, 431 F. Supp. 3d 1175, 1187 (D. Nev. 2020); *United States v. Warrant*, No. 19-MJ-71283-VKD-1, 2019 WL 4047615, at *2 (N.D. Cal. Aug. 26, 2019); *SEC v. Huang*, No. 15-cv-269, 2015 WL 5611644, at *3 (E.D. Pa. Sept. 23, 2015); *Commonwealth v. Baust*, No. CR14-1439, 2014 WL 10355635, at *4 (Va. Cir. Ct. Oct. 28, 2014). The verbal statement would of course include the passcode itself. But it would also communicate defendant's knowledge of the means to open the device, and, impliedly, his control over the phone in addition to its contents.

The defendant would reveal that same information through his mental efforts by truthfully recalling and entering a password into a cell phone. *See Pittman*, 479 P.3d at 1043; *see also G.A.Q.L. v. State*, 257 So. 3d 1058, 1061 (Fla. D. Ct. App. 2018); *In re Marriage of Roney*, 332 Ill. App. 3d 824, 827–28 (4th Dist. 2002) (reversing order holding defendant in contempt for refusing to turn over tapes of illegally recorded phone calls, as "[t]urning over any recordings would amount to compelled testimonial communication

because that act would implicitly concede the existence, source, and authenticity of the materials").[2]

Requiring a defendant to use information stored in his mind to incriminate himself is a demand for testimony privileged by the Fifth Amendment—however that use is accomplished. Non-verbal acts can be testimonial when they communicate information relying on the contents of the mind.[3] Opening a lock with a memorized passcode is testimonial regardless of whether the State learns the combination. Indeed, in *United States v. Green*, 272 F.3d 748 (5th Cir. 2001), the Fifth Circuit held that there is "no serious question" that asking an arrestee to disclose the locations of and open the combination locks to cases containing firearms demands "testimonial and communicative" acts as to his "knowledge of the presence of firearms in these cases and of the means of opening these cases." *Id.* at 753–54. Similarly, a decade ago, the Eleventh Circuit applied this principle in a case similar to this one, holding that "the decryption . . . of the hard drives would require the use of the contents of [the accused's] mind and could not be fairly characterized as a physical act that would be nontestimonial in nature." *In re Grand Jury Subpoena Dated Mar. 25, 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012).

The Appellate Court therefore erred when it concluded that, unlike cases in which police seek to force a suspect to *disclose* the password itself, the Constitution allows the

---

[2] Indeed, the State's own conduct in this case makes clear that entry of Mr. Sneed's passcode would have testimonial value. Depending on the circumstances, his possession of the passcode for the phone may indicate that the defendant was aware of relevant files, distributed them, or created them—facts that might otherwise require evidence from other sources.

[3] *See Schmerber v. California*, 384 U.S. 757, 761 n.5 (1966) ("A nod or headshake is as much a 'testimonial' or 'communicative' act in this sense as are spoken words."). This is in contrast to mere physical acts that do not reveal the contents of an individual's mind, such as putting on a shirt. *Holt v. United States*, 218 U.S. 245, 252–53 (1910).

State to compel Mr. Sneed to "simply enter his passcode into his phone and thereby make its contents accessible to the police without ever telling the police the passcode." *Sneed*, 2021 IL App (4th) 210180, ¶ 61. As the cases cited above illustrate, that is a distinction without a difference. *See, e.g.*, *Green*, 272 F.3d at 753 (opening case with combination lock was testimonial even though the government did not learn the combination). Entering the passcode communicates potentially inculpatory information, including the defendant's control over the phone and the means of unlocking it.

Moreover, the Fifth Amendment protects testimony even if its literal content is of no real import to the government. For example, in *Muniz*, 496 U.S. 582, the United States Supreme Court held that a motorist suspected of intoxication could not be compelled to answer a question about the date of his own sixth birthday. *Id.* at 598–99. Law enforcement was not interested in the date itself (in fact, they knew it); rather, they sought his response as evidence of mental impairment. *Id.* at 599 & n.13. But the question still demanded a testimonial answer. *See Allred v. State*, 622 So. 2d 984, 987 (Fla. 1993) (adopting *Muniz* rationale in holding that compelling a motorist to recite the alphabet would be testimonial because it was "the *content* (incorrect recitation) of the speech that is being introduced, rather than merely the *manner* (slurring) of speech" (emphasis in original)). Accordingly, the government could not compel the defendant to speak in a fashion that would incriminate him.

The Appellate Court also incorrectly reasoned that recalling and using a passcode may be merely the "rote application of a series of numbers" that "may be used so habitually that its retrieval is a function of muscle memory rather than an exercise of conscious thought." *Sneed*, 2021 IL App (4th) 210180, ¶ 59. But as the facts of *Muniz* demonstrate,

"roteness" is not the legal standard. Indeed, much of everyday small talk is rote, such as answers to questions about one's siblings, place of employment, or place of birth. If such statements were the result of state compulsion designed to lead to an incriminating result, rather than water-cooler politeness, they would surely be protected by the Fifth Amendment. Rote communication is no less revealing, and no less testimonial, than communication requiring mental effort.

If the Appellate Court's ruling stands, Mr. Sneed will be put to the classic "'trilemma' of truth, falsity, or silence." *Muniz*, 496 U.S. at 597. If he provides or enters the passcode to the phone, he could incriminate himself. If he refuses, he could be held in contempt. *See People v. Johnson*, 2017 IL App (1st) 162876, ¶ 17 (affirming trial court order holding defendant in direct civil contempt for failing to enter passcode to unlock phone); *see also Eunjoo Seo v. State*, 148 N.E.3d 952, 953 (Ind. 2020) (trial court held defendant in contempt for refusing to enter her password). The Fifth Amendment does not allow criminal defendants to be forced into this situation. *See Muniz*, 496 U.S. at 597 ("[T]he definition of 'testimonial' evidence . . . must encompass all responses to questions that, if asked of a sworn suspect during a criminal trial, could place the suspect in the 'cruel trilemma.'").

For all of these reasons, compelled disclosure or use of a password constitutes a modern but straightforward form of testimony that is categorically protected from compulsion under the federal and state privileges against self-incrimination.

II. The foregone conclusion rationale does not apply in this case.

The Appellate Court erroneously concluded that there "is a second and separate reason" that the State can compel Mr. Sneed to unlock and decrypt his phone: "the foregone

conclusion doctrine." *Sneed*, 2021 IL App (4th) 210180, ¶ 66. But this Court should reject application of the foregone conclusion rationale in this case for two reasons.

First, the foregone conclusion rationale is an exceedingly narrow concept applied just once by the U.S. Supreme Court, almost fifty years ago, in the context of a demand for known, specific business records. *See Fisher*, 425 U.S. 391. Its justification and its application were dependent on the context of that case. Invoking it outside of that narrow context makes little sense and would swallow the foundational rule that the government cannot force suspects to give testimony against themselves. For that reason alone, the foregone conclusion rationale has no application here.

Second, even assuming the foregone conclusion rationale could apply in this context, the Appellate Court was wrong about the proper focus of that analysis. Disagreeing with the Third District's decision in *People v. Spicer*, 2019 IL App (3d) 170814, the Fourth District here concluded that the proper focus of the foregone conclusion analysis is the State's knowledge of facts about the defendant's passcode, rather than the State's knowledge about specific files stored on the device. But if the foregone conclusion rationale is ever to apply, its proper focus is on the specific contents of the device, not the passcode.

A. The foregone conclusion analysis applies only to the production of specified, pre-existing business records—not to the compelled production of digital device passwords.

1. *Fisher* is a unique and isolated case.

The foregone conclusion analysis originated in a single United States Supreme Court case—*Fisher*. There, the government sought to compel the defendants' attorneys to produce tax documents created by accountants preparing the defendants' tax returns. 425 U.S. at 412–13. The Court recognized that "[t]he act of producing evidence,

[specifically documents,] in response to a subpoena . . . has communicative aspects" protected by the Fifth Amendment—including implicit admissions concerning the existence, possession, and authenticity of the documents produced. *Id.* at 410. Under the unique circumstances of the case, the Court held that the act of producing the subpoenaed documents was *not* testimonial, since the government already had independent knowledge of the existence and authenticity of the specific documents at issue. *Id.* at 412–13. In other words, the government already *knew* the very thing that the compelled act at issue would reveal to it, rendering the testimonial value of that act to be legally insignificant under the particular circumstances. *See id.* at 411 (finding that to succeed, the government must show that the sought-after information is a "foregone conclusion" in that it "adds little or nothing to the sum total of the Government's information").

Thus, *Fisher* stands for the proposition that if (1) a subpoena demands production of a narrow category of specific and identifiable business and financial documents, (2) production does not rely on or disclose the contents of one's mind, and (3) the State already has evidence of all facts communicated by the production, it may be able to compel the target's disclosure of those papers. Further, *Fisher* was careful to note that an order to "compel oral testimony" would violate the Fifth Amendment. *Id.* at 409.

It bears emphasizing that this constitutes the entirety of the foregone conclusion "doctrine." *See Eunjoo Seo,* 148 N.E. 3d at 956 ("*Fisher* was the first, and only, Supreme Court decision to find that the testimony implicit in an act of production was a foregone conclusion."); *Davis*, 220 A.3d at 549 ("Based upon the United States Supreme Court's jurisprudence surveyed above, it becomes evident that the foregone conclusion gloss on a Fifth Amendment analysis constitutes an extremely limited exception to the Fifth

Amendment privilege against self-incrimination."). The "doctrine" is but a single application in *Fisher*, not (as the State would have it) some long-standing and well-developed legal concept.

In the forty-six years since *Fisher*, the U.S. Supreme Court has never again denied Fifth Amendment protections because the implied testimony from an act of production was a foregone conclusion. *See Davis*, 220 A.3d at 549. In fact, only two other times has the Supreme Court even engaged with a foregone conclusion analysis—and it *rejected* forgone conclusion arguments both times, confirming the narrow scope of the analysis. *See Hubbell*, 530 U.S. at 44–45 (holding that the case "plainly [fell] outside of" the foregone conclusion rationale where the government sought "broad categories" of "general business and tax records" rather than specific, known files); *United States v. Doe* (*Doe II*), 465 U.S. 605, 612–14 (1984) (rejecting application of the foregone conclusion rationale where the subpoena sought several broad categories of general business records).

Hubbell is particularly instructive on the limited scope of the foregone conclusion analysis. There, the government subpoenaed broad categories of documents from the respondent. *Hubbell*, 530 U.S. at 40. The act of production established the existence, authenticity, and custody of produced documents, information the government claimed it did not need and would not use. *Id.* at 41. Nevertheless, the Court held that the Fifth Amendment privilege applied and prevented the government from using evidence arising out of the compelled testimony. Compliance with the subpoena required "mental and physical steps" of determining and selecting which records were responsive to the subpoena, and the obligation that the respondent "truthful[ly] reply to the subpoena." *Id.* at 42. The Court refused to apply the foregone conclusion rationale not solely because the

facts implied by the act of production were as yet unknown to the prosecution. *Id.* at 44. Rather, in *Hubbell*, as here (and in all forced decryption cases), the foregone conclusion rationale did not apply because compliance would reveal the contents of Hubbell's mind in a way that the act of production in *Fisher*—turning over a specific document already known to the government—would not.

It is unsurprising that the United States Supreme Court has never even considered the foregone conclusion rationale outside of cases involving specific, preexisting business and financial records. "[T]he Fifth Amendment privilege is foundational," and "[a]ny exception thereto must be necessarily limited in scope and nature." *Davis*, 220 A.2d at 549. As the *Davis* court explained:

> Indeed, it would be a significant expansion of the foregone conclusion rationale to apply it to a defendant's compelled oral or written testimony. As stated by the Supreme Court, "[t]he essence of this basic constitutional principle is 'the requirement that the [s]tate which proposes to convict *and punish* an individual produce the evidence against him by the independent labor of its officers, not by the simple cruel expedient of forcing it from his own lips.'" *Estelle v. Smith*, 451 U.S. 454, 462, 101 S. Ct. 1866, 68 L.Ed.2d 359 (1981) (emphasis original). Broadly circumventing this principle would undercut this foundational right.

Id. at 549. Moreover, these types of records constitute a unique category of material that, to varying degrees, have been subject to compelled production and inspection by the government for over a century. *See, e.g.*, *Braswell v. United States*, 487 U.S. 99, 104 (1988); *Shapiro v. United States*, 335 U.S. 1, 33 (1948); *Roney*, 332 Ill. App. 3d at 853 (In *Hubbell*, "the United States Supreme Court more restrictively viewed its holding in *Fisher* as tied to the particular circumstances of that case—namely, the compulsory production of documents otherwise required by tax law to have been previously prepared.").

2. Illinois courts and other trial courts have been appropriately hesitant to employ the foregone conclusion analysis.

To *amici*'s knowledge, only twice prior to the compelled decryption context has an Illinois court entertained the possibility of applying a foregone conclusion inquiry, and in both cases courts took an extremely narrow view. One case vacated a civil discovery order and remanded for an *in camera* inspection by the trial court to determine which, if any, of the business documents at issue the opposing party could demonstrate it already knew about with reasonable particularity. *Mueller Indus., Inc. v. Berkman*, 399 Ill. App. 3d 456, 474 (2010), *abrogated on other grounds by People v. Radojcic*, 2013 IL 114197. The other case held that a litigant could *not* be compelled to turn over tapes of illegally recorded telephone calls. *Roney*, 332 Ill. App. 3d 824. No published Illinois decision has compelled production of evidence other than business records because of a "foregone conclusion."

Other lower courts, too, have overwhelmingly applied the rationale only in cases concerning the compelled production of specific, preexisting business and financial records. *See, e.g.*, *United States v. Sideman & Bancroft, LLP*, 704 F.3d 1197, 1200 (9th Cir. 2013) (business and tax records); *United States v. Gippetti*, 153 F. App'x 865, 868–69 (3d Cir. 2005) (bank and credit-card account records); *United States v. Bell*, 217 F.R.D. 335, 341–42 (M.D. Pa. 2003) ("tax avoidance" materials advertised on defendant business's website); *cf. Burt Hill, Inc. v. Hassan*, No. 09-1285, 2010 WL 55715, at *2 (W.D. Pa. Jan. 4, 2010) (contents of electronic storage devices used by defendants while employed by plaintiff).

In contrast, courts have rejected the foregone conclusion inquiry in cases involving the compelled production of physical evidence, such as guns or drugs, because responding

to such requests would constitute an implicit admission of guilty knowledge. *See, e.g.*, *Commonwealth v. Hughes*, 404 N.E.2d 1239, 1244 (Mass. 1980) ("[W]e express doubt whether a defendant may be compelled to deliver the corpus delicti, which may then be introduced by the government at trial, if only it is understood that the facts as to the source of the thing are withheld from the jury."); *Goldsmith v. Super. Ct.*, 152 Cal. App. 3d 76, 87 (1984) (defendant's production of a gun was testimonial, and not a foregone conclusion).

3. The foregone conclusion rationale does not—and should not—apply to unlocking cell phones.

In *Eunjoo Seo*, the Indiana Supreme Court outlined three additional important reasons to refrain from importing a foregone conclusion analysis to the compelled decryption context. 148 N.E. 3d at 958–59. First, the compelled production of an unlocked smartphone implicates far greater privacy concerns than "a documentary subpoena for specific files," since even the 13,120 pages of documents at issue in *Hubbell* "pale[] in comparison to what can be stored on today's smartphones." *Id.* at 959–60. Second, even restricting the foregone conclusion inquiry to those instances where the government can identify specific files with reasonable particularity may prove unworkable. *Id.* at 960–61. After all, in a wide-ranging search of a device like the one authorized here, officers may come across further password-protected websites or accounts within the device, or a cloud storage service that grants law enforcement a "windfall" of evidence they "did not already know existed[.]" *Id.* at 961. Finally, as the U.S. Supreme Court recently admonished, courts should tread cautiously when "confronting new concerns wrought by digital technology." *Id.* (quoting *Carpenter v. United States*, 138 S. Ct. 2206, 2222 (2018)).

This Court should decline the State's invitation here to expand the narrow foregone conclusion analysis into a free-floating exception that can overcome the Fifth Amendment

privilege for myriad speech, writing, or other testimonial acts. Even if the police knew with reasonable certainty that someone committed a bank robbery, no one could credibly suggest that the suspect could be compelled to testify orally or in writing concerning an incriminating fact because it was a "foregone conclusion." That is because the Fifth Amendment does not allow the government to compel suspects to speak, write, type, or otherwise reproduce the contents of their minds to aid in their own prosecution. Several courts have rightly concluded that permitting the narrow foregone conclusion inquiry to circumvent the bedrock constitutional privilege would "sound 'the death knell for a constitutional protection against compelled self-incrimination in the digital age.'" *Garcia v. State*, 302 So. 3d 1051, 1057 (Fla. Dist. Ct. App. 2020) (quoting *Commonwealth v. Jones*, 117 N.E.3d 702, 724 (Mass. 2019) (Lenk, J., concurring)), *cert. granted*, 2020 WL 7230441 (Fla. Dec. 8, 2020); *see also Eunjoo Seo*, 148 N.E.3d at 958–59 (discussing why the foregone conclusion analysis "may be generally unsuitable to the compelled production of any unlocked smartphone"); *Davis*, 220 A.3d at 549 (foregone conclusion inapplicable to compel the disclosure of a defendant's password); *State v. Valdez*, 482 P.3d 861, 875 (Utah Ct. App.), *cert. granted* 496 P.3d 715 (Utah 2021).[4]

This Court should reverse the Appellate Court below and follow its counterparts in Indiana and Pennsylvania in ensuring that the highly context-dependent foregone

[4] *But see State v. Andrews*, 234 A.3d 1254, 1274 (2020) (foregone conclusion test applies to the production of the passcodes, not to the phone's contents), *cert. denied sub nom. Andrews v. New Jersey*, 141 S. Ct. 2623 (2021); *State v. Stahl*, 206 So.3d 124, 136–37 (Fla. Dist. App. Ct. 2016) (same); *Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 615–16 (2014) (facts conveyed by disclosing passcode were foregone conclusion and not protected by the Fifth Amendment); *United States v. Fricosu*, 841 F. Supp.2d 1232, 1237 (D. Colo. 2012) (same, but precluding prosecution from using fact of production of unencrypted hard drive against defendant).

conclusion analysis does not "swallow the constitutional privilege." *Davis*, 220 A.3d at 549.

B. Even if the foregone conclusion rationale could apply in this context, the State must describe with reasonable particularity the incriminating files it seeks.

Even if the foregone conclusion rationale could apply in cases involving passcodes, the State has not come close to making a showing that it applies in *this* case. Rather than simply demonstrating that an individual had possession and control over a passcode, *see Sneed*, 2021 IL App (4th) 210180, ¶¶ 86–96, the State must show with "reasonable particularity" that it "already [knows] of the materials [it will uncover], thereby making any testimonial aspect a 'foregone conclusion.'" *In re Grand Jury Subpoena*, 670 F.3d at 1346. By contrast, the government may not compel an act of production that would reveal materials of which it was previously unaware. *See Hubbell*, 530 U.S. at 45 (no foregone conclusion where government did not have "any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent").

Thus, the Eleventh Circuit has required that investigators know and be able to describe with reasonable particularity the discrete, tangible contents of a device—not merely that the defendant knows the passcode. *In re Grand Jury Subpoena*, 670 F.3d at 1346. An order requiring the defendant to produce a decrypted hard drive would be "tantamount to testimony by [the defendant] of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; and of his capability to decrypt the files." *Id.* (emphasis added). The government therefore could not rely on the foregone conclusion rationale unless it could show with "reasonable particularity" the "specific file names" of the records sought, or, at minimum, that the government seeks "a certain file," and can establish that "(1) the file

exists in some specified location, (2) the file is possessed by the target of the subpoena, and (3) the file is authentic." *Id.* at 1349 n.28; *see also Eunjoo Seo*, 148 N.E.2d at 958 (foregone conclusion analysis did not apply because the state "failed to demonstrate that any particular files on the device exist or that [defendant] possessed those files"); *cf. United States v. Apple MacPro Computer*, 851 F.3d 238, 248 (3d Cir. 2017) (finding the foregone conclusion inquiry satisfied where the government had evidence "both that files exist[ed] on the encrypted portions of the devices and that [the defendant could] access them").

That was the conclusion also of the Third District in *Spicer*. In that case, the State obtained a warrant to search the defendant's cell phone after he was arrested, during a vehicle stop over a traffic violation, for possession of drugs. 2019 IL App (3d) 170814, ¶¶ 3–5. When the defendant refused to provide his passcode, the State sought to compel production of his passcode, invoking the "foregone conclusion" rationale. The *Spicer* court rejected that argument. The court concluded that the State "does not know what information might be on [the defendant's] phone but surmises that cell phones are often used in unlawful drug distribution and such information would be available on [the defendant's] phone." *Id.* ¶ 22; *see id.* (explaining that the warrant permitted the State to access "most of the information" on the defendant's phone, and the State "[did] not identify any documents or specific information it [sought] with reasonable particularity"). That analysis was correct.

Rejecting this approach, the Appellate Court in the present case instead followed a New Jersey Supreme Court decision that concluded that the "foregone conclusion test applies to the production of the passcodes themselves, rather than to the phones' contents." *Andrews*, 234 A.3d at 1273; *see Sneed*, 2021 IL App (4th) 210180, ¶¶ 85, 87. Applying

that analysis, the court explained that to succeed in its invocation of the foregone conclusion rationale, the State would have to "establish with reasonable particularity (1) it knows the passcode exists, (2) the passcode is within the defendant's possession or control, and (3) the passcode is authentic." *Id.* ¶ 98. And the court found that the State had done so in this case. *Id.* ¶¶ 99–102.

In reaching that conclusion, the Appellate Court erroneously reasoned that the contents of the phone were essentially irrelevant at this stage because "the State has obtained a valid search warrant." *Id.* ¶ 89. The Appellate Court claimed that focusing on the contents of the phone would "allow[] the fifth amendment to swallow the fourth amendment, thereby permitting a suspect to 'hide' behind a passcode evidence to which the State is lawfully entitled pursuant to the issuance of the search warrant." *Id.* ¶ 91. But the Fourth and Fifth Amendments serve different purposes, and the State must comply with both. Requiring the state to have knowledge of the specific contents of a device ensures that the suspect's compelled testimony—providing or entering the passcode—cannot provide the State with the new, incriminating evidence against him in violation of the Fifth Amendment. Just as in *Hubbell*, the state may not disclaim reliance on a suspect's compelled testimony and make derivative use of the evidence as if it "fell like manna from heaven." 530 U.S. at 42; *see also id*. at 43 (rejecting derivative use of documents because the government did not have a "legitimate, wholly independent source" as required by *Kastigar v. United States*, 406 U.S. 441 (1972)). A contents-based foregone conclusion rule follows from *Hubbell* to ensure that the rationale does not permit the government to obtain incriminating evidence directly from a criminal defendant.

In sum, even if this Court were to conclude that a foregone conclusion inquiry is appropriate, the State cannot compel Mr. Sneed to produce the decrypted contents of his phone without first demonstrating with reasonable particularity that it knows what documents it will find there.[5]

Locked phones and laptops may impose obstacles to law enforcement in particular cases. So do window shades. It is sometimes true that constitutional protections interfere with law enforcement investigations. In many cases, police can use forensic tools to access information on electronic devices without compelling the production of a passcode. *See* Logan Koepke et al., *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* 27 (2020). But when that fails, as with any constitutional right or privilege, relevant evidence will sometimes be placed off-limits. *See Riley v. California*, 573 U.S. 373, 401 (2014) (constitutional rights are "not merely 'an inconvenience to be somehow "weighed" against the claims of police efficiency.'" (citation omitted)). This Court should not disregard a central constitutional protection because potentially relevant information is sometimes beyond law enforcement reach.

[5] The Appellate Court below concluded that even if the contents of the phone must be a foregone conclusion, the State had still satisfied the inquiry because the detective had "described the documents and evidence he was looking for [photographs of the false paychecks] and explained why he expected [them] to be found on defendant's phone." *See Sneed*, 2021 IL App (4th) 210180, ¶ 80; *see id.* ¶ 102. *Amici* agree with Mr. Sneed that conclusion was incorrect, because the testifying officer only described information he *hoped* to find, and did not *know* of any specific files on Mr. Sneed's device or their connection to the alleged crime. Thus, if Mr. Sneed were compelled to enter his passcode, he would be providing additional evidence to the State about the contents of the phone and his connection to it.

CONCLUSION

For the reasons explained above, *amici* urge the Court to rule in favor of Mr. Sneed.

Dated: June 8, 2022

Respectfully Submitted,

/s/ *Rebecca K. Glenberg*
Rebecca K. Glenberg
ARDC No. 6322106
Roger Baldwin Foundation of ACLU, Inc.
150 N. Michigan Ave., Suite 600
Chicago, IL 60601
(312) 201-9740
rglenberg@aclu-il.org

Counsel for Amici Curiae

On the Brief:

Alexandra Block (ARDC No. 6285766)
Rebecca K. Glenberg
Roger Baldwin Foundation of ACLU, Inc.
150 N. Michigan Ave., Suite 600
Chicago, IL 60601

Brett Max Kaufman
American Civil Liberties Union Foundation
125 Broad Street
New York, NY 10004

Jennifer Stisa Granick
American Civil Liberties Union Foundation
39 Drumm Street
San Francisco, CA 94111

Andrew Crocker
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109

Additional counsel listed on following page.

William Wolf
William Loeffel
Jonathan M. Brayman
Illinois Association of Criminal Defense Lawyers
1440 W. Taylor St., Suite 811
Chicago, IL 60607

Jonathan M. Brayman
ARDC No. 6302461
Breen & Pugh
National Association of
Criminal Defense Lawyers
53 W. Jackson Blvd., Suite 1215
Chicago, IL 60604

CERTIFICATE OF COMPLIANCE

I certify that this brief conforms to the requirements of Rules 345 and 341(a) and (b). The length of this brief, excluding the pages contained in the Rule 341(d) cover, the Rule 341(h)(1) table of contents and statement of points and authorities, the Rule 341(c) certificate of compliance, and the certificate of service, is 23 pages.

/s/ *Rebecca K. Glenberg*
Rebecca K. Glenberg
Counsel for Amici Curiae

E-FILED
6/14/2022 10:22 AM
CYNTHIA A. GRANT
SUPREME COURT CLERK

NOTICE OF FILING AND PROOF OF SERVICE

The undersigned, an attorney, certifies that on June 8, 2022, she caused the foregoing **Brief for the American Civil Liberties Union, et al. as *Amici Curiae* in Support of Defendant–Appellant** to be filed with the Clerk of the Supreme Court of Illinois using the Court's electronic filing system and that the same was served by e-mail to the following counsel of record:

Daniel Markwell (of Clinton)
State's Attorneys Appellate
Prosecutor's Office
100 W. Randolph St., 12th Floor
Chicago, Illinois 60601-3218
Tel.: (312) 814-5029
eserve.criminalappeals@atg.state.il.us

Counsel for Plaintiff–Appellee

James E. Chadd
Catherine K. Hart
Joshua Scanlon
State Appellate Defender's Office
400 W. Monroe St., Suite 202
Springfield, IL 62704
Tel.: (217) 782-7203
James.Chadd@osad.state.il.us

Counsel for Defendant–Appellant

Hon. Kwame Raoul
Illinois Attorney General
Criminal Appeals Division
100 W. Randolph St., 12th Floor
Chicago, Illinois 60601-3218
eserve.criminalappeals@ilag.gov

Counsel for Plaintiff–Appellee

Within five days of acceptance by the Court, the undersigned also states that she will cause thirteen copies of the Brief of *Amici Curiae* to be mailed with postage prepaid to the following address:

Clerk of the Supreme Court of Illinois
Supreme Court Building
200 E. Capitol Ave
Springfield, IL 62701

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.

/s/ *Rebecca K. Glenberg*
Rebecca K. Glenberg
Counsel for Amici Curiae