07

E-FILED
11/30/2022 3:43 PM
CYNTHIA A. GRANT
SUPREME COURT CLERK

No. 127968

IN THE
SUPREME COURT OF ILLINOIS

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

MOTION OF INDIANA, ARKANSAS, FLORIDA, IDAHO, LOUISIANA, MINNESOTA, MISSISSIPPI, NEW JERSEY, NORTH DAKOTA, OKLAHOMA, OREGON, SOUTH CAROLINA, SOUTH DAKOTA, UTAH, AND VIRGINIA FOR LEAVE TO FILE BRIEF AS *AMICI CURIAE* IN SUPPORT OF PLAINTIFF-APPELLEE

Pursuant to Illinois Supreme Court Rule 345(a), the States of Indiana, Arkansas, Florida, Idaho, Louisiana, Minnesota, Mississippi, New Jersey, North Dakota, Oklahoma, Oregon, South Carolina, South Dakota, Utah, and Virginia respectfully request leave to file the accompanying brief as *amici curiae* in support of Plaintiff-Appellee the People of the State of Illinois. In support of the motion, *amici* States state the following:

1. This case concerns whether it violates the Fifth Amendment to order a person to unlock a device where the prosecution establishes that the person knows the device's passcode. *See People v. Sneed*, 2021 IL App (4th) 210180, ¶¶ 1–2.

2. As sovereigns charged with upholding criminal laws, *amici* States have a significant interest in the issue's resolution. They also bring a unique perspective on how the issue impacts law enforcement's ability to investigate, prosecute, and prevent crimes. The

accompanying brief explores some of those impacts, explaining how orders like the one the Appellate Court authorized here are important for accessing vital evidence pursuant to judicial warrants and how the orders are consistent with Fifth Amendment principles. Accordingly, consideration of the *amici* States' brief would give the Court the benefit of the States' perspective and experience on an issue of significant importance to law enforcement.

3. This motion is filed and the proposed brief is submitted on the due date of Plaintiff-Appellee's brief in this case.

Wherefore the *amici* States respectfully request leave to file the accompanying brief of *amici curiae* in support of Plaintiff-Appellee.

Respectfully submitted,

THEODORE E. ROKITA
Attorney General of Indiana

THOMAS M. FISHER
Solicitor General

/s/ Patricia Orloff Erdmann
PATRICIA ORLOFF ERDMANN
(ARDC #6196294)
Chief Counsel of Litigation

Office of the Attorney General
IGC South, Fifth Floor
302 W. Washington Street
Indianapolis, IN 46204
(317) 232-6318
Patricia.Erdmann@atg.in.gov

Counsel for Amici *States*

No. 127968

IN THE
SUPREME COURT OF ILLINOIS

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

ORDER

THIS CAUSE COMING TO BE HEARD on motion of the States of Indiana, ___, and ___, for leave to file a brief of *amici curiae* in support of Plaintiff-Appellee, due notice having been given, and the court being fully advised.

IT IS HEREBY ORDERED that the motion is GRANTED/DENIED.

ENTER:

JUSTICE

Exhibit 1

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 Judicial District, No. 4-21-0180 There on Appeal from the Circuit of the Sixth Judicial Circuit, DeWitt County, Illinois No. 21 CF 13 Honorable Karle E. Koritz, Judge Presiding.

BRIEF OF INDIANA, ARKANSAS, FLORIDA, IDAHO, LOUISIANA, MINNESOTA, MISSISSIPPI, NEW JERSEY, NORTH DAKOTA, OKLAHOMA, OREGON, SOUTH CAROLINA, SOUTH DAKOTA, UTAH, AND VIRGINIA AS *AMICI CURIAE* IN SUPPORT OF PLAINTIFF-APPELLEE

Office of the Attorney General
IGC South, Fifth Floor
302 W. Washington Street
Indianapolis, IN 46204
(317) 232-6318
Patricia.Erdmann@atg.in.gov

THEODORE E. ROKITA
Attorney General of Indiana

THOMAS M. FISHER
Solicitor General

PATRICIA ORLOFF ERDMANN
(ARDC #6196294)
Chief Counsel of Litigation

Counsel for Amici *States*
(additional counsel listed in addendum)

TABLE OF CONTENTS

POINTS AND AUTHORITIES

INTRODUCTION

In the modern world, digital evidence from phones, computers, and the cloud is vital to many criminal investigations. Increasingly, however, modern encryption technologies thwart efforts to execute search warrants for devices and data, preventing timely access to critical information needed to investigate, prosecute, and prevent crimes. As *amici* States know from experience, victims of sexual abuse, narcotics trafficking, and other serious crimes suffer as a result. Search warrants for digital evidence do law enforcement and the public no good without the practical ability to access that evidence.

As the Appellate Court recognized, a permissible solution to these problems is for a court to order a user of a password-protected device to unlock the device without revealing the password. Binding precedent establishes that the Fifth Amendment's protections against self-incrimination extend only to "*testimonial* communication[s] that [are] incriminating." *Fisher v. United States*, 425 U.S. 391, 408 (1976). And crucially conduct does not "rise[] to the level of testimony within the protection of the Fifth Amendment" where it merely conveys information the State already knows. *Id.* at 411. Thus, where it is a foregone conclusion that a user can unlock a device, the Fifth Amendment permits orders compelling the user to unlock it.

The Appellate Court appropriately held that Keiron Sneed could be ordered to unlock a password-protected phone once Illinois proved he knew the phone's password.

ARGUMENT

I. Securing Assistance with Unlocking Encrypted Devices Is Important for the Effective Investigation, Prosecution, and Prevention of Crimes

Digital evidence is increasingly vital to investigating, prosecuting, and preventing serious crimes. Today, however, sophisticated digital locks secure data found on

smartphones, tablets, computers, servers, applications, messaging services, and websites. *See* Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 Geo. L.J. 989, 990, 993–94 (2018). And while law enforcement can attempt to bypass those locks, the technology for accessing devices can be slow, costly, and ineffective. Without the legal ability to compel persons to unlock devices that law enforcement already knows they can access, investigations, prosecutions, and innocent bystanders will suffer.

A. Digital evidence is vital to investigating, prosecuting, and preventing crimes

As the former U.S. Attorney for the Central District of Illinois observed, digital evidence is essential for "all types of criminal cases—white collar and elder fraud, child sexual exploitation, gun and drug traffickers and terrorism." John C. Milhiser, *Peoria Journal Star Op-Ed: Warrant-Proof Encryption Threatens Public Safety*, U.S. Dep't of Just. (Dec. 10, 2019), https://www.justice.gov/archives/doj/blog/peoria-journal-star-op-ed-warrant-proof-encryption-threatens-public-safety.

Perhaps most obviously, digital evidence is foundational to the investigation and prosecution of crimes involving the internet—financial crimes, online scams, child pornography, and the like. As prosecutors have documented, evidence from websites, computers, and messaging services is critical to investigations into child pornography and ending the sexual abuse of children. *See, e.g.*, Milhiser, *supra*; Scott Brady, *Pittsburgh Post-Gazette Op-Ed: Facebook Encryption Could Endanger Victims*, U.S. Dep't of Just. (Jan. 10, 2020), https://www.justice.gov/archives/doj/blog/pittsburgh-post-gazette-op-ed-facebook-encryption-could-endanger-victims. For example, digital evidence obtained from a warrant recently allowed police to stop a man from Decatur, Illinois, who was

extorting two girls to provide him with sexually explicit images. Milhiser, *supra*. He is now serving a 20-year sentence for his crimes. *Id.*

Digital evidence is no less important to investigating, preventing, and prosecuting crimes that occur offline. To cite a few examples, smartphone evidence "unavailable via any other means" has placed murderers at homicide scenes, corroborated the testimony of child sexual-assault victims, and shown sexual assaults to have been premeditated. *See Third Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety* 8–9 (2017), https://www.manhattanda.org/wp-content/themes/dany/files/2017%20Report%20of%20the%20Manhattan%20District%20Attorney%27s%20Office%20on%20Smartphone%20Encryption.pdf (*Third Report*). Timely access to digital evidence has also helped to exonerate the innocent, allowing police and prosecutors to pursue other leads and apprehend the actual perpetrators. *See id.* at 9.

B. Modern encryption renders technological efforts to access encrypted devices uncertain, costly, and time-consuming

As important as digital evidence is, however, law enforcement cannot always access it even when armed with search warrants. Modern encryption schemes securing evidence found on phones, computers, and websites rely on complex mathematics that are all but impervious to brute-force attacks. *See* Kerr & Schneier, *supra*, at 993–94. "In the arms race between encryption and brute force attacks, the mathematics overwhelmingly favors encryption." *Id.* at 994. Data secured with 128- and 256-bit encryption schemes—the "most commonly used" schemes today—cannot be broken by "any current or near-future technologies." *Id.* Attempting to break 256-bit encryption using current technology would take "billions of years." Kirstyn Watson, *Under Digital Lock and Key: Compelled Decryption and the Fifth Amendment*, 126 Penn St. L. Rev. 577, 583 (2022).

Although difficult-to-break encryption prevents predatory hackers from stealing financial information, it can frustrate legitimate efforts by law enforcement to execute search warrants for devices, websites, and data. To bypass encryption schemes, investigators can attempt to guess a user's password. Kerr & Schneier, *supra*, at 997–98. But that is not always an option. Every time technology companies release a new device or operating system—something, for instance, Apple does annually—"it takes months, and sometimes years, for lawful hacking solutions to catch up." *Third Report*, *supra*, at 10.

Moreover, as this case illustrates, not every law-enforcement agency can afford those tools. *See People v. Sneed*, 2021 IL App (4th) 210180, ¶ 15. Law-enforcement agencies can spend "hundreds of thousands of dollars"—and sometime much more—to access encrypted data, which puts many tools beyond the reach of all but a "small minority of well-funded agencies." *Third Report*, *supra*, at 9. And scarce resources can force even better funded agencies to ration. In this case, the Illinois State Police would not attempt to unlock Sneed's phone because the investigation did not involve narcotics. *See Sneed*, 2021 IL App (4th) 210180, ¶ 15.

Even where law enforcement has access to the technologies needed to guess a passcode, the enterprise can be extremely time consuming and prone to failure. By default, iPhones are secured with a six-digit numerical passcode. Guessing that passcode using sophisticated tools takes on average 11 hours. Jack Nicas, *Does the F.B.I. Need Apple to Hack Into iPhones?*, N.Y. Times (Jan. 17, 2020), https://www.nytimes.com/2020/01/17/technology/fbi-iphones.html. Longer eight-digit passcodes take on average 46 days to guess, and ten-digit passcodes take on average 12.5 years. *Id.* Passwords that combine numbers with other characters are even more difficult to crack. *See* Kristen M. Jacobsen,

Game of Phones, Data Isn't Coming: Modern Mobile Operating System Encryption and Its Chilling Effect on Law Enforcement, 85 Geo. Wash. L. Rev. 566, 585 (2017).

Countermeasures found on phones and other devices further complicate matters, potentially preventing law enforcement from unlocking devices no matter how much money, time, and effort are expended. iPhones allow users to enable a setting that disables a "phone for one minute after five wrong passcode entries." Kerr & Schneier, *supra*, at 1000. "The delay period grows for the next four successive wrong entries, from five minutes for the sixth wrong entry, to fifteen minutes each for the seventh and eighth wrong entries, to an hour for the ninth wrong entry." *Id.* "After the tenth wrong entry, the phone's data is permanently erased and cannot be accessed." *Id.* Android phones likewise offer security settings that erase all data after a certain number of incorrect guesses. Jacobsen, *supra*, at 585. Such settings "obviously limit[] the opportunity investigators have to access [a] phone's contents by guessing." Kerr & Schneier, *supra*, at 1000.

Lengthy delays in accessing devices are not uncommon. In 2015, for example, a group of terrorists located in the United States exchanged 100 text messages with affiliated terrorists located overseas before attacking the 'Draw Mohammed' contest in Garland, Texas. James B. Comey, *Expectations of Privacy: Balancing Liberty, Security, and Public Safety*, FBI (Apr. 6, 2016), https://www.fbi.gov/news/speeches/expectations-of-privacy-balancing-liberty-security-and-public-safety. Over a year later, the FBI had still not gained access to the terrorists' encrypted phones. *Id.* After the 2017 church shooting in Sutherland Springs, Texas—the fifth deadliest shooting in the United States at that time—the FBI "applied the most advanced commercial tool available to crack the [gunman's] code." Christopher Wray, *The Way Forward: Working Together to Tackle Cybercrime*, FBI (July

25, 2019), https://www.fbi.gov/news/speeches/the-way-forward-working-together-to-tackle-cybercrime. Over 600 days passed with no success. *Id.*

Such delays inflict real-world costs, potentially causing leads to go cold, preventing evidence from being available in time for trial, and prolonging victims' suffering. A recent case involving child sex trafficking illustrates some of those consequences. In that case, a suspect locked his phone moments before being arrested. Joseph D. Brown, *Dallas Morning News Op-Ed: Legislators Must Not Allow Warrant-Proof Encryption to Make America More Dangerous*, U.S. Dep't of Just. (Jan. 19, 2020), https://www.justice.gov/archives/doj/blog/dallas-morning-news-op-ed-legislators-must-not-allow-warrant-proof-encryption-make-america. It took law enforcement over a year to access the suspect's phone, on which law enforcement discovered hundreds of messages about the ongoing sexual abuse of children. *Id.* Only then were officers able to begin "the job they should have been able to do months before—investigating th[e abusers]" and "rescuing children." *Id.* The importance of timely access cannot be overstated.

As an alternative to guessing passcodes, investigators can attempt to exploit security flaws. Kerr & Schneier, *supra*, at 1005. To exploit a flaw, however, law enforcement must first identify a vulnerability in security systems created by leading technology companies like Apple, Google, and Microsoft. *Id.* at 1006. Identifying such vulnerabilities "ordinarily requires technological expertise or the resources to buy access" that are beyond what even some of the most sophisticated, well-funded agencies have. *Id.* at 1007; *see Third Report*, at 9. Reportedly, the FBI had to pay a private company at least $1 million for an exploit needed to access an iPhone used by San Bernardino shooter, Syed Farook. Kerr & Schneier, *supra*, at 1007. And even if law enforcement manages to identify and to

exploit a flaw once, there is no guarantee that it will work again. Technology and security companies are constantly working to identify, patch, and remove potential vulnerabilities. *See id.* at 1006–07.

C. Orders compelling persons to unlock devices are an important tool for obtaining access to digital evidence

Because attempting to guess a password or exploit a flaw is not a viable way to obtain digital evidence in many situations, other legal tools for bypassing encryption are important. One of those tools is an order compelling a user to unlock a device for which the user knows the password. As this case illustrates, such an order can be used to access a device when law enforcement lacks the technology to unlock it. Or it can allow law enforcement to access a device quicker than it could than through technological means. A user who knows a phone's passcode can enter that passcode far faster than investigators can blindly guess the correct passcode from among millions of potential options. As *amici* States know from their own experience, orders like the one the Appellate Court approved here can be very valuable for timely obtaining digital information vital to investigating, prosecuting, and preventing crimes.

II. Where a Person's Knowledge of a Device's Passcode Is a Foregone Conclusion, an Order Compelling the Person To Unlock the Device Does Not Violate the Fifth Amendment's Prohibition on Compelled Testimony

The orders are also consistent with the Fifth Amendment. In this case, the police obtained a search warrant for the information on Sneed's phone, and Sneed never challenged that warrant. *See People v. Sneed*, 2021 IL App (4th) 210180, ¶ 89. So there is no Fourth Amendment issue with accessing the information. The only dispute concerns whether the Fifth Amendment precludes a court from ordering a person who knows a device's password to unlock it. The Appellate Court correctly held that such an order is

consistent with the Fifth Amendment where it is a foregone conclusion that the person compelled can unlock a device.

A. The Fifth Amendment does not protect non-testimonial conduct, including Sneed's action of unlocking a phone

The Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." U.S. Const. amend. V. As the term "witness" implies, the Fifth Amendment's protection is limited "to a *testimonial* communication that is incriminating." *Fisher v. United States*, 425 U.S. 391, 408 (1976) (emphasis in original). The Fifth Amendment is not "a general protector of privacy." *Id.* at 400; *see United States v. Doe*, 465 U.S. 605, 618 (1984) (*Doe I*) (O'Connor, J., concurring) ("[T]he Fifth Amendment provides absolutely no protection for the contents of private papers of any kind."). Non-testimonial acts, "though incriminating, are not within [its] privilege." *Doe v. United States*, 487 U.S. 201, 210 (1988) (*Doe II*). Thus, courts may order persons to perform a wide variety of actions—from producing documents to signing consent directives to handing over keys to strongboxes—so long as the actions themselves are not testimonial. *See id.* at 210–11 & n.9, 215.

In determining whether conduct has "testimonial significance," a critical consideration is whether the *conduct* "*itself,* explicitly or implicitly, relate[s] a factual assertion or disclose[s] information." *Doe II*, 487 U.S. at 210 (emphasis added). Whether conduct conveys such information can depend "on the facts and circumstances of the particular case." *Id.* at 214–15. But any information conveyed does not "rise[] to the level of testimony within the protection of the Fifth Amendment" where that information is "a foregone conclusion" such that the conduct itself "adds little to nothing to the sum total of the Government's information." *Fisher*, 425 U.S. at 411; *see, e.g., United States v. Bright*,

596 F.3d 683, 692–94 (9th Cir. 2010); *United States v. Apple MacPro Computer*, 851 F.3d 238, 247 (3d Cir. 2017); *State v. Andrews*, 234 A.3d 1254, 1275 (N.J. 2020); *Commonwealth v. Jones*, 117 N.E.3d 702, 709 (Mass. 2019).

Fisher v. United States, 425 U.S. 391 (1976), illustrates that important qualification on the meaning of "testimonial." There, the U.S. Supreme Court held that a subpoena requiring a taxpayer to produce specific documents did not compel "incriminating testimony within the production of the Fifth Amendment." *Id.* at 414. "The act of producing evidence in response to a subpoena," the Court acknowledged, tacitly communicates some information, including "the existence of the papers demanded" and "their possession or control by the taxpayer." *Id.* at 410. But any tacit admission did not "rise[] to the level of testimony" because the government was not "relying on the 'truth-telling' of the taxpayer to prove the existence of or his access to the documents." *Id.* at 411 (citation omitted). "The existence and location of the papers [was] a foregone conclusion," and the taxpayer's conduct would "add[] little or nothing to the sum total of the Government's information." *Id.* Thus, the Court explained, enforcing the subpoena would not "touch[]" any "constitutional rights." *Id.* (quoting *In re Harris*, 221 U.S. 274, 279 (1911)).

As the Appellate Court recognized, *Fisher*'s holding applies with equal force to orders compelling persons to unlock devices. *See Sneed*, 2021 IL App (4th) 210180, ¶¶ 87–103. The act of unlocking a phone can implicitly convey that a person knows a passcode. But the action is *not testimonial* where it is a "foregone conclusion" that knowledge of the passcode is in the person's possession. *Fisher*, 425 U.S. at 411; *see Andrews*, 234 A.3d at 1275; *Jones*, 117 N.E.3d at 709. That is especially true where the passcode is entered privately, without revealing whatever letters or numbers are contained within it. *See United*

States v. Oloyede, 933 F.3d 302, 309 (4th Cir. 2019). The Appellate Court appropriately recognized that requiring Sneed to unlock a device using a password established to be within his possession would not be testimonial.

B. The criticisms lodged against *Fisher* lack merit

The various criticisms Sneed and his *amici* have offered regarding *Fisher* provide no reason for refusing to apply it here. To begin, *Fisher* cannot be characterized as an "isolated case" applicable only to "business records." ACLU Br. 11; *see* Sneed Br. 25–26. As the U.S. Supreme Court has explained, *Fisher* "applied basic Fifth Amendment principles." *Doe II*, 487 U.S. at 209. Those principles have never been repudiated—and indeed they have been applied outside the context of financial records. *See, e.g.*, *United States v. Patane*, 542 U.S. 630, 644 n.7 (2004) (observing that there was a "reasonable argument" in favor of compelling a handgun's production and citing *Fisher*); *Baltimore City Dep't of Soc. Servs. v. Bouknight*, 493 U.S. 549, 555 (1990) (rejecting the argument that producing a child would be a testimonial act, explaining that the child's identity was a "fact the State could readily establish" and citing *Fisher*). Nothing about *Fisher*'s holding or reasoning turns on the happenstance that the case arose in the tax context.

Undifferentiated privacy concerns stemming from the "amount of information contained within modern phones" provide no reason to limit *Fisher*. Sneed Br. 26; *see* ACLU Br. 16. That objection is akin to saying that a suspect cannot be forced to produce tax records, or turn over the key to a strongbox, if a court thinks their contents might reveal too much. It "confuses" the question whether an action is "'testimonial' with the separate" question whether an action is "incriminating." *Doe II*, 487 U.S. at 208 n.6. The non-testimonial act of producing documents proved to be within a person's possession, or of

unlocking a phone using a password proved to within his possession, does not become testimonial merely "because it will lead to incriminating evidence." *Id.* (quoting *In re Grand Jury Subpoena*, 826 F.2d 1166, 1172 (2d Cir. 1987) (Newman, J., concurring)).

Nor do abstract privacy concerns supply a basis for holding that the non-testimonial act of entering a passcode violates the Fifth Amendment. The notion that the Fifth Amendment protects privacy per se was "discredited" decades ago. *Doe I*, 465 U.S. at 610 n.8 (quoting *Andresen v. Maryland*, 427 U.S. 463, 472 (1976)); *see Fisher*, 425 U.S. at 399–401. The U.S. Supreme Court has "never on any ground, personal privacy included, applied the Fifth Amendment to prevent the otherwise proper acquisition or use of evidence which . . . did not involve compelled testimonial self-incrimination of some sort." *Fisher*, 425 U.S. at 399; *see Doe I*, 465 U.S. at 610 n.8. In its view, privacy concerns are more appropriately addressed through the Fourth Amendment. *See Fisher*, 425 U.S. at 401; *see also* Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 Tex. L. Rev. 767, 797 (2019). But Sneed raised no Fourth Amendment challenge here to the warrant authorizing a search of his phone. *See Sneed*, 2021 IL App (4th) 210180, ¶ 89.

Equally unavailing is the objection that entering a passcode communicates "information stored" in a defendant's "mind." ACLU Br. 8. As the Appellate Court recognized, a defendant can enter a passcode "without ever telling the police the passcode" to ensure nothing beyond the fact the defendant knows the passcode is revealed. *Sneed*, 2021 IL App (4th) 210180, ¶ 61. Any objection that entering a passcode somehow reveals more about a defendant's mind than producing documents defies logic. Every action that conveys information implicitly communicates thoughts or beliefs. That is true whether the action is producing tax records ("I believe these are the record requested"), supplying a

handwriting exemplar ("This is my writing"), or entering a passcode ("I know the passcode"). *See Fisher*, 425 U.S. at 411–12. But *Fisher* establishes that, where the government already knows the information implied by an action, any tacit admission does not "rise[] to the level of testimony." *Id.* at 411. It specifically rejected the argument that producing tax records in response to a subpoena would be testimonial because the action would (among other things) express "the tax payer's *belief*"—a state of mind—"that the papers are those described in the subpoena." *Id.* at 410–13 (emphasis added).

C. *Fisher* requires the State to prove only that Sneed knows the passcode

Sneed and his *amici* alternatively argue that, for *Fisher*'s "foregone conclusion" rationale to apply, the State must "describe with reasonable particularity the discrete, tangible contents of a device." ACLU Br. 18; *see* Sneed Br. 37–38. In their view, it is not enough to prove that he knows the passcode. The State must prove what is on his phone. Technologically, however, that proposal makes no sense. The State is seeking Sneed's passcode precisely because it cannot access the phone's contents without the passcode.

More important, the law does not require proof of a device's contents. U.S. Supreme Court precedent makes clear that the critical question for Fifth Amendment purposes is whether the compelled act "itself" is testimonial. *Doe II*, 487 U.S. at 215; *see, e.g.*, *United States v. Hubbell*, 530 U.S. 27, 37 (2000) (asking whether the "act of production itself" is testimonial and incriminating); *Fisher*, 425 U.S. at 410–11 (asking whether the "act of producing evidence" was testimonial "wholly aside from the contents of the papers produced"). To be testimonial the act or "communication *must itself*, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a 'witness' against himself." *Doe II*, 487 U.S. at 210 (emphasis

added) (footnote omitted); *see id.* at 211 n.10 ("The content itself must have testimonial significance."). Where the act might lead is beside the point. *See id.* at 208 n.6.

Here, the act the State seeks to compel is the entry of a passcode. Entering the passcode communicates only that Sneed "knows the passcode." *Jones*, 117 N.E.3d at 710; *see Andrews*, 234 A.3d at 1274. It does not communicate anything about whether there are files on the device or what is contained in those files. "Knowing the password and knowing the contents of a decrypted device are two different things. One person might know the device's contents but not know the password. Another person might know the password but not know the device's contents." Kerr, *supra*, at 779. Both logically and legally, "it is problematic" to treat the "production of passcodes" as a communication about "the contents of phones." *Andrews*, 234 A.3d at 1274. Requiring the State to prove what Sneed's phone contains would effectively "import[] Fourth Amendment privacy principles into a Fifth Amendment inquiry." *Id.*

CONCLUSION

The Appellate Court's judgment should be affirmed.

Dated: November 30, 2022

Respectfully submitted,

THEODORE E. ROKITA
Attorney General of Indiana

THOMAS M. FISHER
Solicitor General

By: /s/ Patricia Orloff Erdmann
PATRICIA ORLOFF ERDMANN
(ARDC #6196294)
Chief Counsel of Litigation

Office of the Attorney General
IGC South, Fifth Floor
302 W. Washington Street
Indianapolis, IN 46204
(317) 232-6318
Patricia.Erdmann@atg.in.gov

Counsel for Amici *States*

ADDITIONAL COUNSEL

LESLIE RUTLEDGE
Attorney General
State of Arkansas

ASHLEY MOODY
Attorney General
State of Florida

LAWRENCE WASDEN
Attorney General
State of Idaho

JEFF LANDRY
Attorney General
State of Louisiana

KEITH ELLISON
Attorney General
State of Minnesota

LYNN FITCH
Attorney General
State of Mississippi

MATTHEW J. PLATKIN
Attorney General
State of New Jersey

DREW WRIGLEY
Attorney General
State of North Dakota

JOHN M. O'CONNOR
Attorney General
State of Oklahoma

ELLEN F. ROSENBLUM
Attorney General
State of Oregon

ALAN WILSON
Attorney General
State of South Carolina

MARK VARGO
Attorney General
State of South Dakota

SEAN REYES
Attorney General
State of Utah

JASON MIYARES
Attorney General
State of Virginia

CERTIFICATE OF COMPLIANCE

I certify that this brief conforms to the requirements of Rules 341(a) and (b). The length of this brief, excluding the pages or words contained in the Rule 341(d) cover, the Rule 341(h)(1) table of contents and statement of points and authorities, the Rule 341(c) certificate of compliance, the certificate of service, and those matters to be appended to the brief under Rule 342(a), is 3,685 words.

/s/ Patricia Orloff Erdmann
PATRICIA ORLOFF ERDMANN
Chief Counsel of Litigation

Office of the Attorney General
IGC South, Fifth Floor
302 W. Washington Street
Indianapolis, IN 46204
(317) 232-6318
Thomas.Fisher@atg.in.gov
Patricia.Erdmann@atg.in.gov

CERTIFICATE OF FILING AND SERVICE

I certify that on November 30, 2022, I electronically filed the foregoing brief with the Clerk of the Court for the Supreme Court of Illinois, by using the Odyssey eFileIL system. I further certify that the other participants in this appeal, named below, are registered service contacts on the Odyssey eFileIL system, and thus will be served via the Odyssey eFileIL system.

Counsel for Plaintiff-Appellee The People of the State of Illinois
Hon. Kwame Raoul
eserve.criminalappeals@ilag.gov
Jason F. Krigel
jason.krigel@ilag.gov
Joshua Schneider
Joshua.schneider@ilag.gov
David J. Robinson

Counsel for Defendant-Appellant Kerion K. Sneed
Catherine K. Hart
4thdistrict.eserve@osad.state.il.us
Dan Markwell
4thdistrict.eserve@osad.state.il.us

Counsel for Amici Curiae 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
Rebecca K. Glenberg
rglenberg@aclu-il.org

Under penalties as provided by law pursuant to section 1-109 of the Illinois Code of Civil Procedure, I certify that the statements set forth in this instrument are true and correct to the best of my knowledge, information, and belief.

/s/ Patricia Orloff Erdmann
PATRICIA ORLOFF ERDMANN
Chief Counsel of Litigation

Office of the Attorney General
IGC South, Fifth Floor
302 W. Washington Street
Indianapolis, IN 46204
(317) 232-6318
Patricia.Erdmann@atg.in.gov

CERTIFICATE OF FILING AND SERVICE

I certify that on November 30, 2022, I electronically filed the foregoing motion with the Clerk of the Court for the Supreme Court of Illinois, by using the Odyssey eFileIL system. I further certify that the other participants in this appeal, named below, are registered service contacts on the Odyssey eFileIL system, and thus will be served via the Odyssey eFileIL system.

Counsel for Plaintiff-Appellee The People of the State of Illinois
Hon. Kwame Raoul
eserve.criminalappeals@ilag.gov
Jason F. Krigel
jason.krigel@ilag.gov
Joshua Schneider
Joshua.schneider@ilag.gov
David J. Robinson

Counsel for Petitioner-Appellant Kerion K. Sneed
Catherine K. Hart
4thdistrict.eserve@osad.state.il.us
Dan Markwell
4thdistrict.eserve@osad.state.il.us

Counsel for Amici Curiae 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
Rebecca K. Glenberg
rglenberg@aclu-il.org

Under penalties as provided by law pursuant to section 1-109 of the Illinois Code of Civil Procedure, I certify that the statements set forth in this instrument are true and correct to the best of my knowledge, information, and belief.

/s/ Patricia Orloff Erdmann
PATRICIA ORLOFF ERDMANN
(ARDC #6196294)
Chief Counsel of Litigation

Office of the Attorney General
IGC South, Fifth Floor
302 W. Washington Street
Indianapolis, IN 46204
(317) 232-6318
Patricia.Erdmann@atg.in.gov