No. 23-1020

IN THE
Supreme Court of the United States

STATE OF UTAH,

Petitioner,

v.

ALFONSO VALDEZ,

Respondent.

On a Petition for a Writ of Certiorari to the Supreme Court of Utah

BRIEF OF INDIANA AND 16 OTHER STATES AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

Office of the
Attorney General
IGC South, Fifth Floor
302 W. Washington St.
Indianapolis, IN 46204
(317) 232-0607
James.Barta@atg.in.gov

THEODORE E. ROKITA
Attorney General
JAMES A. BARTA
Solicitor General
Counsel of Record

Counsel for Amici *States*

QUESTIONS PRESENTED

1. Whether disclosing a cell phone passcode is testimonial under the Fifth Amendment.

2. Whether the Fifth Amendment foregone-conclusion doctrine applies to the disclosure of a cellphone passcode when the government has evidence the phone belongs to the suspect.

TABLE OF CONTENTS

QUESTIONS PRESENTED i

TABLE OF AUTHORITIES v

INTEREST OF THE AMICI STATES 1

SUMMARY OF ARGUMENT..... 2

ARGUMENT 3

I. Efficiently Unlocking Encrypted Devices Is Vital for Crime Prevention, Prosecution, and Victim Protection..... 3

A. Digital evidence is vital to investigating, prosecuting, and preventing crimes 4

B. Modern encryption makes hacking an encrypted device expensive and time consuming—if it even works at all 6

C. Orders requiring persons to provide access to devices with digital evidence are important investigatory tools 12

II. States Need This Court To Resolve Conflicts Regarding the Rules for Unlocking Devices 13

A. This Court's precedents establish that the Fifth Amendment extends only to incriminating, testimonial acts and statements..... 13

B. Lower courts are deeply divided over what granting access to a device conveys 14

C. The decision below adds to the disarray by making communicative value depend on how an action is carried out 18

CONCLUSION 21

TABLE OF AUTHORITIES

CASES

Andresen v. Maryland,
427 U.S. 463 (1976).....17

Commonwealth v. Davis,
220 A.3d 534 (Pa. 2019).....16, 18

Commonwealth v. Jones,
117 N.E.3d 702 (2019) 15

Doe v. United States,
465 U.S. 605 (1984).....17

Doe v. United States,
487 U.S. 201 (1988).....13, 14, 18

Fisher v. United States,
425 U.S. 391 (1976).....2, 14, 17

In re Grand Jury Subpoena,
826 F.2d 1166 (2d Cir. 1987) 18

In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011,
670 F.3d 1335 (11th Cir. 2012).....16

In re Harris,
221 U.S. 274 (1911).....14

People v. Sneed,
--- N.E.3d ---, 2023 WL 4003913 (Ill. June 15, 2023).....12, 13, 15, 18

CASES [CONT'D]

People v. Sneed,
187 N.E.3d 801 (Ill. Ct. App. 2021).....7, 8

Riley v. California,
573 U.S. 373 (2014).....18

Seo v. State,
148 N.E.3d 952 (Ind. 2020).....13, 16, 17

State v. Andrews,
234 A.3d 1254 (N.J. 2020), ...12, 15, 17, 18, 19

State v. Stahl,
206 So. 3d 124 (Fla. Dist. Ct. App. 2016).....15, 19

United States v. Eldarir,
--- F. Supp. 3d. ---, 2023 WL 4373551 (E.D.N.Y. July 6, 2023).....20

United States v. Oloyede,
933 F.3d 302 (4th Cir. 2019).....15

United States v. Whipple,
92 F.4th 605 (6th Cir. 2024).....9

United States v. White,
2023 WL 7703553 (N.D. Ga. Nov. 15, 2023).....9

United States v. Wright,
431 F. Supp. 3d 1175 (D. Nev. 2020).....20

CONSTITUTIONAL PROVISIONS

U.S. Const. amend. V 13

OTHER AUTHORITIES

Chris Smith, *How to make a secure iPhone passcode that's almost impossible to hack*, BGR (Jan. 30, 2023), https://bgr.com/tech/how-to-make-a-secure-iphone-passcode-thats-almost-impossible-to-hack/ 8

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 10

Fourth Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety, 6 (2019), https://www.manhattanda.org/wp-content/uploads/2019/10/2019-Report-on-Smartphone-Encryption-and-Public-Safety.pdf 6, 11

Jack Nicas, *Does the F.B.I. Need Apple to Hack Into iPhones?*, N.Y. Times (Jan. 17, 2020).....8

OTHER AUTHORITIES [CONT'D]

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 9

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 4

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 10, 11

OTHER AUTHORITIES [CONT'D]

Kevin Dudley, Jr., *Monroe man accused of inappropriately texting underage girl on Facebook Messenger for 18 months; arrested*, WGNO (Mar. 22, 2024), https://wgno.com/news/crime/monroe-man-accused-of-inappropriately-texting-underage-girl-on-facebook-messenger-for-18-months-arrested/ 5

Kirstyn Watson, *Under Digital Lock and Key: Compelled Decryption and the Fifth Amendment*, 126 Penn St. L. Rev. 577, 583 (2022) 7

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).....8

Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 Geo. L.J. 989, 990, 993–94 (2018).....4, 6, 7, 8, 9, 11, 12

OTHER AUTHORITIES [CONT'D]

Patrick Lakamp, *FBI spent years unlocking accused killer's iPhone, but judge blocks 'cornucopia' of evidence*, The Buffalo News (Sept. 15, 2023) https://buffalonews.com/news/local/crime-and-courts/fbi-spent-years-unlocking-accused-killers-iphone-but-judge-blocks-cornucopia-of-evidence/article_2dec34aa-50c6-11ee-8cfc-4b4b4cf9f970.html 10

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 4

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 5, 7, 11

OTHER AUTHORITIES [CONT'D]

Tomas Rodriguez, *Voyeurism suspect must yield passcode*, The News-Press (Fort Myers, Florida), 2023 WLNR 28298562 (Aug. 17, 2023).....12

Tripp Mickle, *Apple Details Plans to Beef Up Encryption of Data in Its iCloud*, N.Y. Times (Dec. 7, 2022) https://www.nytimes.com/2022/12/07/technology/apple-icloud-encryption-security.html.....7

INTEREST OF THE *AMICI* STATES

In the modern world, digital evidence is vital to many criminal investigations.[1] And that evidence is regularly stored on cell phones and other electronic devices. Increasingly, however, modern encryption technologies thwart efforts to execute search warrants for devices and data. This hinders timely access to critical information needed to investigate, prosecute, and prevent crimes. Even if law enforcement has the technology to crack a phone without a passcode, this process is often expensive and time consuming. 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 are worthless to law enforcement without the practical ability to access that evidence.

To address the problem, courts have issued orders requiring persons to unlock devices or provide passcodes. But courts across the country are divided as to whether the Fifth Amendment bars such orders. States and law enforcement need clarity about what tools they can use in conducting investigations into serious crimes and working to protect their citizens. And to conduct investigations and protect citizens more effectively, they need the ability to seek court orders that provide access to electronic devices. The Court should grant certiorari to provide guidance on how the Fifth Amendment's guarantee against self-incrimination applies in the modern context of electronic devices.

---

[1] Pursuant to Rule 37.2, counsel of record for all parties received notice at least 10 days before the due date of the intention to file this brief.

SUMMARY OF ARGUMENT

I. Criminal investigations increasingly rely on digital evidence. Information held on cellphones, computers, and servers is critical for solving crimes that occur online, such as online scams and sexual exploitation of minors, and those that occur offline, such as kidnapping, robbery, and assault. Timely access to this information allows law enforcement to rescue victims, prevent crimes, and exonerate the innocent.

Even where law enforcement secures a warrant for this electronic information, however, they cannot always retrieve it. Sophisticated encryption schemes protect many devices, and even if police have access to technology for bypassing or breaking encryption schemes, the decryption process can take months or years—if it works at all. Law enforcement's inability to access encrypted information may prevent it from identifying additional victims, clearing innocent suspects, and obtaining key evidence in time for trial.

II. Trial courts have devised a straightforward solution to this problem: order a person who knows a device's password to grant law enforcement access. But appellate courts across the nation are conflicted over whether such an order violates the Fifth Amendment's guarantee against self-incrimination.

As this Court's precedents establish, the Fifth Amendment protects persons from testifying against themselves. Nontestimonial acts are not within its ambit. And *Fisher v. United States*, 425 U.S. 391 (1976), establishes that an act is nontestimonial if it is a "foregone conclusion" that the government knows whatever information is communicated by the act.

Applying this principle to modern devices, several courts have held that ordering someone to grant law enforcement access to a device does not violate the Fifth Amendment if it is a foregone conclusion that the person knows the device's passcode. Other courts, however, have required the government to prove that it knows far more. They have required the government to show that it already knows what information is on a device and who owns it, even though typing in a passcode does not communicate anything about what the device contains. These courts have allowed concerns for personal privacy to infect their Fifth Amendment analysis, contrary to this Court's admonition that the Fifth Amendment is not a general protector of privacy.

The decision below adds to this disagreement. It holds that whether granting access to a phone is testimonial depends on the method by which it is done. It ruled that telling law enforcement a passcode with no evidentiary significance constitutes a testimonial act even if the action communicates the exact same information that typing in the passcode would convey. That approach directly conflicts with the approach taken by other courts. The Court should grant review to clarify how courts should apply the Fifth Amendment's guarantees to modern encryption problems.

ARGUMENT

I. Efficiently Unlocking Encrypted Devices Is Vital for Crime Prevention, Prosecution, and Victim Protection

Digital evidence is increasingly vital to investigating, prosecuting, and preventing serious crimes. But sophisticated digital locks can secure this data. So

even if law enforcement has a warrant to search a suspect's smartphone or computer, they cannot access its contents without the key. *See* Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 Geo. L.J. 989, 990, 993–94 (2018). And while law enforcement can attempt to hack into the devices, this technology doesn't work like in the movies. Bypassing these digital locks can be slow, costly, and ineffective. Lacking the legal ability to compel persons to unlock devices that law enforcement already knows it can access has serious consequences—and may cause investigations, prosecutions, and victims to suffer.

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

As a former U.S. Attorney explained, 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, like online scams or harassment. As prosecutors have documented, this digital evidence is critical to investigating 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. That evidence is, for example, central to a case built against a Louisiana man who sent explicit Facebook messages to a minor for eighteen months. Kevin Dudley, Jr., *Monroe man accused of inappropriately texting underage girl on Facebook Messenger for 18 months; arrested*, WGNO (Mar. 22, 2024), https://wgno.com/news/crime/monroe-man-accused-of-inappropriately-texting-underage-girl-on-facebook-messenger-for-18-months-arrested/. It is also central to a case against an Illinois man who extorted two girls to provide him with sexually explicit images and is now serving a 20-year sentence. Milhiser, *supra*. After law enforcement obtained a search warrant for his Facebook account, they identified another victim who had not initially reported the messages. *Id.*

Digital evidence is no less important in investigating, preventing, and prosecuting offline crimes. Smartphone evidence unavailable via any other means has placed murderers at homicide scenes, corroborated the testimony of child sexual-assault victims, and shown that some sexual assaults were 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. Digital evidence is not only used to secure convictions. It also has helped law enforcement exonerate the innocent and apprehend the actual perpetrators. *See id.* at 9. For example, after a victim's throat was slashed in a Manhattan street, law en-

forcement initially focused on one suspect. *Fourth Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety*, 6 (2019), https://www.manhattanda.org/wp-content/uploads/2019/10/2019-Report-on-Smartphone-Encryption-and-Public-Safety.pdf. After obtaining a warrant and spending months trying to unlock the suspect's phone, law enforcement eventually accessed the phone and found video evidence that exonerated the suspect. *Id.*

B. Modern encryption makes hacking an encrypted device expensive and time consuming—if it even works at all

As important as digital evidence is, however, law enforcement officers cannot always access it even when they have procured a search warrant. If a suspect had stored information in a locked file cabinet, a search warrant would allow officers to pry the drawer open. But modern encryption schemes securing evidence on electronic devices rely on complex mathematics that are all but impervious to brute-force attempts. *See* Kerr & Schneier, *supra*, at 993–94 ("In the arms race between encryption and brute force attacks, the mathematics overwhelmingly favors encryption."). 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).

This level of protection is much needed to prevent predatory hackers from stealing personal information. But it can frustrate legitimate efforts by law enforcement to execute search warrants on digital devices. 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. And while certain phone companies (like Apple) used to provide law enforcement access to unencrypted information from the cloud, Apple now no longer does so. Tripp Mickle, *Apple Details Plans to Beef Up Encryption of Data in Its iCloud*, N.Y. Times (Dec. 7, 2022) https://www.nytimes.com/2022/12/07/technology/apple-icloud-encryption-security.html.

Moreover, not every law-enforcement agency can afford those tools. *See, e.g.*, *People v. Sneed*, 187 N.E.3d 801 ¶ 15 (Ill. Ct. App. 2021) *aff'd*, --- N.E.3d ---, 2023 WL 4003913 (Ill. June 15, 2023), *cert denied*, --- S. Ct. ---, 2024 WL 759835 (Mem.) (Feb. 26, 2024). Law-enforcement agencies can spend "hundreds of thousands of dollars"—and sometimes 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, as a recent case from Illinois illustrates. In that case, the Illinois State Police had decryption tools but were not able to assist local law enforcement with unlocking a phone because the investigation did not involve narcotics. *See Sneed*, 187 N.E.3d ¶ 15.

Even where law enforcement has access to the technologies needed to guess a passcode, the enterprise can be 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. 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). An eleven-character iPhone password could take "up to 34 years" to crack. Chris Smith, *How to make a secure iPhone passcode that's almost impossible to hack*, BGR (Jan. 30, 2023), https://bgr.com/tech/how-to-make-a-secure-iphone-passcode-thats-almost-impossible-to-hack/.

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 is expended. iPhones allow users to enable a setting that disables a "phone for one minute after five wrong passcode en-

tries." 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. Time-delay and auto-erase 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. *See, e.g.*, *United States v. Whipple*, 92 F.4th 605, 614 (6th Cir. 2024) (uncracking cell phone of suspected bank robber took over eight months); *United States v. White*, 2023 WL 7703553, at *2 (N.D. Ga. Nov. 15, 2023) (forensics laboratory took over six weeks to discover contents of suspected drug dealer's phone). 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 messages. *Id.* The FBI knew the messages existed, but without the suspect providing a passcode, the FBI has "no idea" what the messages said. *Id.* Or 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. But even with that commitment of resources, over 600 days passed with no success. *Id.*

Such delays inflict real-world consequences. They can cause leads to go cold, prevent evidence from being available in time for trial, and prolong victims' suffering. In one recent case, the FBI spent three and a half years before cracking the passcode of an accused murderer and drug trafficker. Patrick Lakamp, *FBI spent years unlocking accused killer's iPhone, but judge blocks 'cornucopia' of evidence*, The Buffalo News (Sept. 15, 2023) https://buffalonews.com/news/local/crime-and-courts/fbi-spent-years-unlocking-accused-killers-iphone-but-judge-blocks-cornucopia-of-evidence/article_2dec34aa-50c6-11ee-8cfc-4b4b4cf9f970.html. Even though the phone included key pieces of evidence—like the defendant's repeated searches for what is needed to convict someone of murder in New York—a judge blocked the evidence from trial because law enforcement had not cracked the phone before the initial trial date.

Another case involving child sex trafficking illustrates these consequences. There, a suspect locked his phone moments before arrest. 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. Once they did, they 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.* Or in another case, the police suspected that an eighth-grade teacher was having sexual conversations with students on his personal cell phone. *Fourth Report* at 6. While he pleaded guilty to one count, the police believe there are other unknown child victims. *Id.* Even though the police have a warrant to access the suspect's phone, they have not been able to retrieve any additional evidence due to encryption. *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. *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 requiring persons to provide access to devices with digital evidence are important investigatory tools

Because attempting to guess a password or exploit a security flaw are not viable ways 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. *See, e.g.*, *People v. Sneed*, --- N.E. 3d ---, 2023 WL 4003913 ¶¶ 115–16 (Ill. June 15, 2023) (approving order requiring defendant to unlock phone); *State v. Andrews*, 234 A.3d 1254, 1262 (N.J. 2020), *cert. denied*, 141 S. Ct. 2623 (Mem.) (2021) (order compelling defendant to reveal passcode). Those orders allow law enforcement to execute valid warrants on electronic devices to complete investigations of serious crimes. *See* Tomas Rodriguez, *Voyeurism suspect must yield passcode*, The News-Press (Fort Myers, Florida), 2023 WLNR 28298562 (Aug. 17, 2023) (reporting that a defendant who placed hidden cameras inside family restrooms must unlock phone to allow access to over 277 voyeuristic videos).

Even if law enforcement could spend the time and money to unlock a phone, providing a password to law enforcement is the most efficient route to executing a warrant on that phone. 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. And for all

the reasons explained above, prompt access to a device's contents is essential for investigating crimes, rescuing victims, protecting the public, exonerating the innocent, and convicting the true perpetrators. If law enforcement has obtained a valid warrant for a phone, they must be able to actually execute that warrant to effectively investigate and prosecute crimes.

II. States Need This Court To Resolve Conflicts Regarding the Rules for Unlocking Devices

Despite the ubiquity and importance of digital evidence to criminal investigations, lower courts are divided over how law enforcement may constitutionally access electronic devices once they procure a warrant for their contents. Specifically, courts need to know whether they may require a suspect to provide access to his phone—either by providing a passcode or unlocking the phone and handing it to officers. In the Seventh Circuit alone, two different state supreme courts have reached opposite conclusions. *Seo v. State*, 148 N.E.3d 952, 953 (Ind. 2020); *Sneed*, 2023 WL 4003913 ¶ 115. Until the law is clarified, an order providing access may be deemed constitutional on one side of the Wabash River and unconstitutional on the other. States and law enforcement need clarity from this Court.

A. This Court's precedents establish that the Fifth Amendment extends only to incriminating, testimonial acts and statements

The Fifth Amendment bars the government from "compel[ling]" a person "in any criminal case to be a witness against himself." U.S. Const. amend. V. As this Court has explained, that provision does not shield "every written and oral statement significant

for its content." *Doe v. United States*, 487 U.S. 201, 208–09 (1988) (*Doe II*). The Fifth Amendment only bars compulsion of incriminating, testimonial communications. *Fisher v. United States*, 425 U.S. 391, 411 (1976). Non-testimonial acts, "though incriminating, are not within [its] privilege." *Doe II*, 487 U.S. at 210. Thus, as this Court has explained, 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.

Fisher v. United States, 425 U.S. at 391, illustrates this principle. There, this Court upheld summonses requiring the production of income tax returns, accountant workpapers, and other records. *Id.* at 393–96. It held that the "act of producing them . . . would not itself involve testimonial self-incrimination," "however incriminating the contents of the accountant's workpapers might be." *Id.* at 410–11. Although the act of production "implicitly admit[s] the existence and possession of the papers," the Court explained, other information in the government's possession made "[t]he existence and location of the papers . . . a foregone conclusion." *Id.* at 411. So the question raised was not one "of testimony but of surrender." *Id.* (quoting *In re Harris*, 221 U.S. 274, 279 (1911)).

B. Lower courts are deeply divided over what granting access to a device conveys

1. Applied to electronic devices, this Court's doctrine should permit orders compelling persons to unlock devices or provide a password if the government already knows whatever information exists revealed

by the act of entering or providing a passcode. But lower courts have taken diametrically opposing views as to what information unlocking a phone implicitly reveals. At least four appellate courts have held that unlocking a phone implicitly conveys only that a passcode exists and that a person "possesses or controls" it (and perhaps that it is authentic). *Sneed*, 2023 WL 4003913 ¶ 85; *see United States v. Oloyede*, 933 F.3d 302, 309 (4th Cir. 2019); *State v. Andrews*, 234 A.3d 1254, 1273 (N.J. 2020); *Commonwealth v. Jones*, 117 N.E.3d 702, 716 (2019); *State v. Stahl*, 206 So. 3d 124, 135 (Fla. Dist. Ct. App. 2016). Even when the passcode is provided in verbal or written form, it does not have testimonial significance where it is "a series of characters without independent evidentiary significance." *Andrews*, 234 A.3d at 1274.

These courts thus will uphold orders granting access to electronic devices if the government proves that it knows a passcode exists and a person has it. *See Sneed*, 2023 WL 4003913 ¶ 106; *Andrews*, 234 A.3d at 1274–75. They do not require the government to prove that it knows what the device's contents are. "[C]onsistent with the Supreme Court case law," the question for these courts is what "the production of the passcodes themselves" conveys—not what "the phone's contents" are. *Andrews*, 234 A.3d at 1273; *see Sneed*, 2023 WL 4003913 ¶ 104. (Nor do these courts require the government to prove a passcode's authenticity because, to the extent authenticity is an issue, "passcodes self-authenticate" upon entry." *Andrews*, 234 A.3d at 1275; *see Sneed*, 2023 WL 4003913 ¶ 109.)

Other courts have attributed much more to the simple act of entering or providing a passcode—and

have even gone so far as to require the government to prove facts regarding the data stored on devices. Take the Indiana Supreme Court's decision in *Seo*, 148 N.E.3d at 952. There, the court held that act of turning over an unlocked phone communicated that the person not only "knows the password," but also that "files on the device exist" and that she "possessed those files." *Id.* at 957. Thus, to establish the action was non-testimonial, the State would need to prove that it already knew "any files . . . exist" and that the phone's owner "possessed th[em]." *Id.* at 962.

Other appellate courts have taken a similar view. *See Commonwealth v. Davis*, 220 A.3d 534, 551 n.9 (Pa. 2019); *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012) (decrypting hard drives would reveal "existence and location of potentially incriminating files"). For example, the Pennsylvania Supreme Court stated that the act of unlocking a computer "could lead to a trove of a presently unknown number of files." *Davis*, 220 A.3d at 551 n.9. So the court concluded that the State would need to establish not only the laptop's owner's knowledge of the password, but also "the existence of the evidence demanded" and the owner's "possession or control of the evidence." *Id.* These decisions thus require law enforcement to prove what is potentially unknowable before a device is unlocked—what a device's contents are and who owns them.

2. Underlying the debate over what the government must prove is a doctrinal divide over the relationship of the Fourth and Fifth Amendments. Decades ago, this Court "discredited" the notion that the Fifth Amendment protects privacy. *Doe v. United*

States, 465 U.S. 605, 610 n.8 (1984) (*Doe I*) (quoting *Andresen v. Maryland*, 427 U.S. 463, 472 (1976)). It 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. In fact, in *Fisher*, the Court expressly rejected the argument that seizure of "'mere evidence' . . . violated the Fourth Amendment and therefore also transgressed the Fifth." *Id.* at 409. Yet courts demanding proof of a device's contents are "import[ing] Fourth Amendment privacy principles into a Fifth Amendment inquiry." *Andrews*, 234 A.3d at 1274.

Consider again the Indiana and Pennsylvania Supreme Courts' approaches to the Fifth Amendment. In demanding that law enforcement prove what it already knows may be unknowable—facts about what a device contains—those courts have openly worried that a contrary rule would reveal too much. In *Seo*, the State had a warrant for a phone's contents, and the defendant did not challenge the warrant, such as by arguing that it was overbroad or that the police lacked probable cause. *See* 148 N.E.3d at 952. Yet a divided Indiana Supreme Court functionally treated the Fifth Amendment as imposing a separate overbreadth requirement, worrying that unlocking a phone could reveal a "combined footprint of what has been occurring socially, economically, personally, psychologically, spiritually and sometimes even sexually, in the owner's life." *Id.* at 960 (quotation omitted). The Pennsylvania Supreme Court has likewise worried that entry of a password "could lead to a trove of a

presently unknown number of files." *Davis*, 220 A.3d at 552 n.9.

As other courts have pointed out, however, the question of what the act of granting access to a device reveals is a "separate" question from questions about its contents. *Doe II*, 487 U.S. at 208 n.6; *see Sneed*, 2023 WL 4003913 ¶ 104; *Andrews*, 234 A.3d at 1274. The contents of phones were not created under compulsion, and phones themselves are objects. *Davis*, 234 A.3d at 1273. So questions about what files, programs, or messages law enforcement review on a particular phone are all Fourth Amendment questions regarding the scope of the relevant warrant. *See, e.g.*, *Riley v. California*, 573 U.S. 373, 401 (2014) (explaining that "information on a cell phone" is not "immune from search" but rather "generally require[s]" a warrant). In the Fifth Amendment context, "focusing on the contents of the phone would disregard the fact that accessing the contents previously passed a probable cause determination by the circuit court." *Sneed*, 2023 WL 4003913 ¶ 104. Unlocking a phone using a password proved to exist does not become testimonial merely "because it will lead to incriminating evidence." *Doe II*, 487 U.S. at 208 n.6 (quoting *In re Grand Jury Subpoena*, 826 F.2d 1166, 1172 (2d Cir. 1987) (Newman, J., concurring)).

C. The decision below adds to the disarray by making communicative value depend on how an action is carried out

The decision below adds to the disarray about what law enforcement must establish to obtain access to a locked device under the Fifth Amendment. In this

case, the Utah Supreme Court agreed that a "passcode functions primarily like a key to unlock [a] device," Pet. App. 21a, ¶ 42—an action that does not reveal anything more than that the key exists and the person owns or controls the device, *see id.* at 22a–23a, ¶ 45. And the court conceded that there "may not be much," if any, "real-world difference" between providing a passcode to police and unlocking a phone without revealing its passcode. *Id.* at 21a, ¶ 42; *see id.* at 26a, ¶ 51 ("communicating a passcode to the police and physically providing an unlocked phone to the police may be functionally equivalent"). Yet the court attributed more significance to providing a passcode than to entering it into a phone directly. The court held that the act of providing a passcode was testimonial, even though no one cared about the "passcode itself" or thought it had "independent meaning relevant to [the] investigation." *Id.* at 21a, ¶ 42, 24a–25a, ¶ 49.

Under the Utah Supreme Court's theory, then, whether granting access to a phone's contents constitutes an incriminating, testimonial communication depends on how access is granted—by action or speech. "[W]hether the State wants [the defendant] to testify to the passcode or to enter it into the phone" changes what type of analysis applies. *Stahl*, 206 So.3d at 133 n. 9; *see* Pet. App. 26a–27a, 33a ¶¶ 51, 65. But that approach conflicts with decisions holding that providing a passcode does not make the act of granting access to a phone testimonial unless the passcode itself has "independent evidentiary significance." *Andrews*, 234 A.3d at 1274. And it implicates a larger debate over whether other methods of granting access—such as compelling suspects to unlock a

phone biometrically—affect the Fifth Amendment analysis. *Compare United States v. Wright*, 431 F. Supp. 3d 1175, 1186–88 (D. Nev. 2020), *aff'd*, 2022 WL 67341 (9th Cir. Jan. 6, 2022), *cert. denied*, 142 S. Ct. 2728 (Mem.) (2022) (holding phone to defendant's face to unlock phone was compelled "testimonial act"), *with United States v. Eldarir*, --- F. Supp. 3d. ---, 2023 WL 4373551, at *5 (E.D.N.Y. July 6, 2023) (requiring defendant to use fingerprint to unlock phone was not barred by the Fifth Amendment).

* * *

As the accumulating disagreements among lower courts make clear, this Court needs to provide clarification as to how Fifth Amendment precedents addressing keys, handwriting, and documents apply to modern devices like smartphones. As matters stand, if law enforcement obtains a warrant for a locked electronic device, law enforcement's ability to access it may depend on accidents of geography. Illinois can obtain an order requiring a person to unlock a phone. New Jersey can obtain an order requiring a phone's owner to provide a password. And Florida can require a person to use a fingerprint to open a phone. Meanwhile, other States, Indiana and Utah included, lack access to orders that facilitate timely access to data crucial to investigating and preventing crimes. And the conflicting approaches charted by lower courts leave law enforcement in other jurisdictions guessing as to what may be deemed to violate the Fifth Amendment. The issue warrants review.

CONCLUSION

The Court should grant the petition.

Respectfully submitted,

Office of the
Attorney General
IGC South, Fifth Floor
302 W. Washington St.
Indianapolis, IN 46204
(317) 232-0709
James.Barta@atg.in.gov

THEODORE E. ROKITA
Attorney General
JAMES A. BARTA
Solicitor General
Counsel of Record

APRIL 2024

ADDITIONAL COUNSEL

STEVE MARSHALL
Attorney General
State of Alabama

TREG TAYLOR
Attorney General
State of Alaska

KATHLEEN JENNINGS
Attorney General
State of Delaware

BRENNA BIRD
Attorney General
State of Iowa

KRIS KOBACH
Attorney General
State of Kansas

LIZ MURRILL
Attorney General
State of Louisiana

AARON M. FREY
Attorney General
State of Maine

DANA NESSEL
Attorney General
State of Michigan

LYNN FITCH
Attorney General
State of Mississippi

MICHAEL T. HILGERS
Attorney General
State of Nebraska

DREW WRIGLEY
Attorney General
State of North Dakota

DAVID A. YOST
Attorney General
State of Ohio

ELLEN F. ROSENBLUM
Attorney General
State of Oregon

ALAN WILSON
Attorney General
State of South Carolina

MARTY JACKLEY
Attorney General
State of South Dakota

KEN PAXTON
Attorney General
State of Texas