## In the Supreme Court of the United States

STATE OF UTAH,

Petitioner,

v.

ALFONSO VALDEZ,

Respondent.

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

## Petition for a Writ of Certiorari

SEAN D. REYES Utah Attorney General STANFORD E. PURSER Utah Solicitor General Counsel of Record CHRISTOPHER A. BATES ANDREW F. PETERSON **Deputy Solicitors General** JEFFREY D. MANN CONNOR NELSON DAVID A. SIMPSON Assistant Solicitors General 350 N. State Street, Suite 230 P.O. Box 142320 Salt Lake City, UT 84114-2320 Telephone: (801) 538-9600 spurser@agutah.gov

**Counsel for Petitioner** 

#### **QUESTIONS PRESENTED**

Police arrested Respondent Alfonso Valdez for kidnapping, robbery, and assault. They obtained a valid search warrant for his cellphone—which they seized from him when he was arrested—so they could access text messages he had used to arrange the meeting with his victim. But they were unable to execute the warrant because Valdez refused to disclose his phone's passcode, which was a nine-dot swipe pattern. Alternative attempts to unlock the phone also failed. At trial, the State introduced evidence about Valdez's refusal to disclose his passcode and invited the jury to draw adverse inferences from his refusal. The Utah Supreme Court held that this violated Valdez's Fifth Amendment privilege against self-incrimination.

The Fifth Amendment protects a person from being "compelled in any criminal case to be a witness against himself." U.S. Const., amend. V. To receive Fifth Amendment protection, a communication must be testimonial and the "testimony" in the communication must add "to the sum total of the Government's information." *Fisher v. United States*, 425 U.S. 391, 411 (1976). That is, the testimony must be more than a foregone conclusion. *Id.* 

The questions presented are:

1. Is disclosing a cellphone passcode that has no substantive meaning testimonial under the Fifth Amendment when the only information communicated is the passcode?

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

## PARTIES TO THE PROCEEDING

All parties appear in the caption of the case on the cover page.

#### **RELATED PROCEEDINGS**

*State v. Valdez*, Utah Supreme Court, No. 20210175-SC. Judgment entered December 14, 2023.

*State v. Valdez*, Utah Court of Appeals, No. 20181015-CA. Judgment entered Feb. 11, 2021.

State v. Valdez, District Court, Second Judicial District, Weber County, Utah, No. 171901990. Judgment entered December 10, 2018.

# TABLE OF CONTENTS

5
QUESTIONS PRESENTEDi
PARTIES TO THE PROCEEDINGii
RELATED PROCEEDINGSii
TABLE OF AUTHORITIESiv
OPINIONS BELOW1
JURISDICTION1
CONSTITUTIONAL PROVISION INVOLVED1
STATEMENT OF THE CASE1
REASONS FOR GRANTING THE PETITION6
I. Whether disclosing a cellphone passcode with no substantive meaning is testimonial when the only information communicated is the passcode is an important question of federal law that should be settled by this Court
II. State supreme courts are divided over whether the foregone-conclusion doctrine applies to the disclosure of a passcode when the government has evidence the device belongs to the suspect14
III.These questions are important and recurring21
IV. This case presents an excellent vehicle to address these extremely important questions24
V. The decision below is incorrect26

A. Disclosing a cellphone passcode is not testimonial when the passcode has no substantive meaning and the only information communicated is the passcode
B. The foregone-conclusion doctrine readily applies to disclosure of a cellphone passcode when the government has evidence the phone belongs to the suspect
CONCLUSION
APPENDIX
Appendix A
Opinion of the Utah Supreme Court, <i>State v.</i> <i>Valdez</i> , No. 20210175-SC (Dec. 14, 2023)1a
Appendix B
Opinion of the Utah Court of Appeals, <i>State</i> v. Valdez, No. 20181015-CA (Feb. 11, 2021)38a
Appendix C
Excerpt from Transcript of Trial Proceedings, District Court, Second Judicial District, Weber County, Utah, <i>State v.</i> <i>Valdez</i> , No. 171901990 (Oct. 19, 2018)79a

# TABLE OF AUTHORITIES

Page(s)

# **Federal Cases**

Andrews v. New Jersey,
No. 20-937, cert. denied 141 S. Ct. 2623 (2021) 25
Carpenter v. United States,
585 U.S. 296 (2018)
Doe v. United States,
487 U.S. 201 (1988) (Doe II)
30, 31, 32, 34
Doyle v. Ohio,
426 U.S. 610 (1976) 5
Fisher v. United States,
425 U.S. 391 (1976)4, 6, 12, 15, 16, 21,
27, 30, 32, 33, 34
Gilbert v. California,
388 U.S. 263 (1967)
Hiibel v. Sixth Jud. Dist. Ct.,
542 U.S. 177 (2004)
In re Grand Jury Subpoena Duces Tecum Dated
Mar. 25, 2011,
670 F.3d 1335 (11th Cir. 2012)
In re Harris,
221 U.S. 274 (1911) 16, 34
Pennsylvania v. Davis,
No. 19-1254, cert. denied 141 S. Ct. 237 (2020) 25
Pennsylvania v. Muniz,
496 U.S. 582 (1990) 27, 28, 31
Riley v. California,
573 U.S. 373 (2014)
Schmerber v. California,
384 U.S. 757 (1966) 6

# **State Cases**

Commonwealth v. Davis,
220 A.3d 534 (Pa. 2019) 9, 17, 21
Commonwealth v. Gelfgatt,
11 N.E.3d 605 (Mass. 2014) 13, 19, 20, 33
People v. Davis,
438 P.3d 266 (Colo. 2019) 22
People v. Sneed,
N.E. 3d, 2023 IL 127968 12, 13, 14, 20, 26
People v. Sneed,
187 N.E.3d 801 (Ill. App. Ct. 2021) 11, 12
Reynolds v. State,
516 P.3d 249 (Okla. Crim. App. 2022) 20
Seo v. State,
148 N.E.3d 952 (Ind. 2020) 13, 20
State v. Andrews,
234 A.3d 1254 (N.J. 2020) 9, 11, 17, 19, 33

State v. Gonzales-Bejarano,	
427 P.3d 251 (Utah Ct. App. 2018)	22
State v. Johnson,	
576 S.W.3d 205 (Mo. Ct. App. 2019)	23
State v. Stahl,	
206 So. 3d 124 (Fla. Dist. Ct. App. 2016)	10

# **Federal Statutes**

28 U.S.C.	§ 1	1257	1,	25
-----------	-----	------	----	----

# Federal Constitutional Provisions

U.S.	Const.,	amend.	V		1	L
------	---------	--------	---	--	---	---

## **Other Authorities**

Pew Rsch. Ctr., Mobile Fact Sheet (Jan. 31, 2024),	
https://www.pewresearch.org/internet/fact-	
sheet/mobile	22
U.S. Census Bureau, Computer and Internet Use	
in the United States: 2018 (Apr. 21, 2021),	
https://www.census.gov/newsroom/press-	
releases/2021/computer-internet-use.html	22

#### **OPINIONS BELOW**

The opinion of the Utah Supreme Court is reported at 2023 UT 26, --- P.3d --- (App. 1a-37a). The opinion of the Utah Court of Appeals is reported at 2021 UT App 13, 482 P.3d 861 (App. 38a-78a). The relevant rulings of the district court were delivered orally (App. 79a-87a).

#### JURISDICTION

The Utah Supreme Court entered judgment on December 14, 2023. App. 1a. Petitioner invokes this Court's jurisdiction under 28 U.S.C. § 1257(a).

#### CONSTITUTIONAL PROVISION INVOLVED

"No person . . . shall be compelled in any criminal case to be a witness against himself . . . ."

U.S. Const., amend. V.

#### STATEMENT OF THE CASE

Respondent Alfonso Valdez and Jane<sup>1</sup> dated and lived together briefly. Valdez was often violent during their relationship. Eventually they separated. App. 6a, ¶11.

Two months after they separated, Valdez texted Jane and asked her to meet him. Valdez said he had some mail for her. They agreed to meet outside Jane's workplace. App. 6a-7a, ¶12.

When Jane arrived, rather than handing over her mail, Valdez pointed a gun at her and told her to get in his SUV. Jane complied. Valdez drove away with Jane in the vehicle, verbally and physically assaulting her. When Valdez stopped the car at one point, Jane

<sup>&</sup>lt;sup>1</sup> A pseudonym.

was able to escape. She called police from a nearby residence. App. 7a, ¶13.

Police arrested Valdez, took him to the police station, and Mirandized him. App. 7a, ¶¶14-15. They also seized his phone from him when he was arrested. App. 42a-43a, ¶7. Police obtained a search warrant for his phone, but they could not open the phone because it was protected by a nine-dot swipe-pattern passcode. App. 7a-8a, ¶16.

A detective interviewed Valdez and asked him to provide the passcode. Valdez refused. Initially police thought they could unlock the phone using a "chip-off" procedure, but that didn't work. App. 8a,  $\P\P17$ -18. The phone was also designed to reset itself and wipe all data after too many unsuccessful attempts to unlock it. App. 42a-43a,  $\P7$ .

Police never could unlock the phone to carry out the search warrant and thus were unable to access the texts between Valdez and Jane. They also never located Jane's phone, which Valdez had taken from her during the assault. App. 7a-8a, ¶¶13, 18.

The State charged Valdez with aggravated kidnapping, aggravated robbery, and aggravated assault. App. 43a, ¶8.

At trial, the State called the detective as a witness. He testified that although police had a search warrant for Valdez's phone, they were unable to access the data on the phone. When the detective began to explain why, defense counsel requested a sidebar. App. 8a-9a, ¶19.

Defense counsel argued Valdez had "a Fifth Amendment right" not to provide the passcode. The prosecutor responded the jury had "a right to know why the officers were unable to access the phone." The court overruled defense counsel's objection. App. 9a, ¶20; *see also* App. 80a-83a.

The detective proceeded to testify about the State's efforts to obtain the passcode. He said he told Valdez the State had a search warrant for the phone and asked him for the passcode. Valdez refused to provide the passcode and instead told him to "destroy the phone." App. 9a, ¶21. The police never could access the phone. App. 82a.

After the State rested, defense counsel moved for a mistrial based in part on the detective's testimony that Valdez had refused to provide his cellphone passcode, again invoking Fifth Amendment protections. The court responded it was not "inclined" to treat Valdez's refusal to provide his passcode as protected by the Fifth Amendment but would give the matter further thought. App. 9a-10a, ¶22; see also App. 83a-87a. Neither the parties nor the court raised the motion again, so the court did not make a final ruling on it. App. 9a-10a, ¶22.

During the defense's case, Valdez called his exwife—who was also Jane's coworker—as a witness. The ex-wife testified that shortly before the assault, Jane showed her text messages between Jane and Valdez that were "sexual" in nature and "kind of a makeup." This testimony suggested Valdez's encounter with Jane was consensual. The State argued in response that the ex-wife's testimony was not credible because the texts weren't in evidence. App. 10a-11a,  $\P$ 23-24.

The jury convicted Valdez of aggravated assault and the lesser included offenses of kidnapping and robbery. App 12a, ¶25. The Utah Court of Appeals reversed. App. 38a-78a. It reasoned that the Fifth Amendment protected Valdez's refusal to provide his passcode because disclosing a passcode is a "testimonial" act. App. 50a-51a, 53a-60a, ¶¶22, 27-35. It further reasoned that the foregone-conclusion doctrine—which provides that an otherwise testimonial act lacks Fifth Amendment protection when the testimony involved in the act is a foregone conclusion, *see Fisher v. United States*, 425 U.S. 391, 410-13 (1976)—did not apply. App 60a-68a, ¶¶36-44. Thus, the court concluded that admitting evidence of Valdez's refusal to disclose his passcode violated his Fifth Amendment rights. App.50a-51a, 77a, ¶¶22, 58.

The Utah Supreme Court affirmed. App. 1a-37a. It noted that the Fifth Amendment applies to communications that are "testimonial, incriminating, and compelled," *Hiibel v. Sixth Jud. Dist. Ct.*, 542 U.S. 177, 189 (2004), and that the only disputed element before the court was whether disclosing a cellphone passcode is "testimonial." App. 18a-19a, ¶¶38-39.<sup>2</sup>

The court concluded that disclosing a passcode is testimonial because it involves an "oral or written communication that explicitly conveys information from the suspect's mind." App 24a, ¶48. It further determined that "the best reading of the record is that the detective asked Valdez to verbally provide his passcode." App. 24a-25a, ¶49. That was distinguishable from a "compelled act of producing evidence" such as turning over documents or handing over an

<sup>&</sup>lt;sup>2</sup> The State did not argue that disclosing the passcode would not have been incriminating or compelled. App. 19a-20a, ¶39 n.8; see also App. 52a-53a, ¶¶25-26. The State also did not argue harmless error. See App. 37a, ¶74.

unlocked phone—which may or may not have "testimonial value" based on "whether the act implicitly conveys information." App. 24a, ¶48. In the court's view, "[d]irectly providing a passcode to law enforcement is not an 'act," but rather a "traditional testimonial communication." App. 26a-27a, ¶51.

The court also concluded that the foregone-conclusion doctrine did not apply. It reasoned that this Court "has never applied the" doctrine "outside of the context of assessing the testimoniality of a nonverbal act of producing documents." App. 33a, ¶64. And it viewed the doctrine "as being inapplicable outside" the context of the physical act of producing evidence. App. 33a, ¶65. Because Valdez had been asked to verbally disclose his passcode, not turn over physical evidence, that meant the doctrine did not apply.

The court noted that because Valdez had refused to disclose his passcode after he had been Mirandized, under other circumstances the question before the court might be whether admitting evidence about his refusal violated his due process rights under *Doyle v*. *Ohio*, 426 U.S. 610 (1976), and its progeny. App. 14a-17a, ¶¶29, n.6, 34 n.7. But because the parties had litigated the case under a traditional Fifth Amendment analysis, the court decided the case on those grounds. *See* App. 16a-17a, ¶34 n.7 ("[W]e address only the Fifth Amendment arguments that the parties have made.").<sup>3</sup>

<sup>&</sup>lt;sup>3</sup> The court also rejected the State's argument that the prosecution's use of Valdez's refusal to disclose his passcode was a "fair response" to an argument Valdez made at trial. App. 33a-36a, ¶¶66-72. The State has not petitioned for certiorari on that issue.

#### **REASONS FOR GRANTING THE PETITION**

## I. Whether disclosing a cellphone passcode with no substantive meaning is testimonial when the only information communicated is the passcode is an important question of federal law that should be settled by this Court.

1. To receive Fifth Amendment protection, a communication must be "testimonial, incriminating, and compelled." *Hiibel*, 542 U.S. at 189. Failure to satisfy any one of those elements means Fifth Amendment protections don't apply. *See id.* at 189-91.

That in turn means a suspect's refusal to disclose a cellphone passcode is protected by the Fifth Amendment only if disclosing the passcode is testimonial. Stated differently, if disclosing a cellphone passcode is *not* testimonial, then a suspect can be compelled to turn the passcode over to police. And the refusal to do so can be addressed through contempt sanctions or adverse use of the defendant's refusal at trial.

Although this Court has addressed testimoniality in other contexts, see, e.g., Schmerber v. California, 384 U.S. 757, 761 (1966) (blood draw); Gilbert v. California, 388 U.S. 263, 266-67 (1967) (handwriting sample); Fisher, 425 U.S. 391, 408-14 (document production), it has not yet answered whether disclosing a cellphone passcode is testimonial. This is an extremely important question given the ubiquity of cellphones in modern life and the fact that, as in this case, cellphones often contain evidence critical to trial proceedings. (Here, text messages between the defendant and the victim arranging their meeting. App. 6a-7a,  $\P12$ .)

Most cellphone passcodes have no substantive meaning. They're a random or meaningless set of

numbers—or in this case, a swipe pattern—with no independent meaning and no purpose other than to unlock the phone. The passcode itself reveals nothing about the crime. It's merely a means to open the phone.

But whether the Fifth Amendment protects that means is an extremely important question. It's the difference between allowing a suspect to lock up a cellphone and its contents forever—even when law enforcement has a valid warrant to search the phone and requiring a suspect to surrender the means needed to access the phone and its contents. And central to that extremely important question is whether disclosing a passcode is testimonial. If disclosing a passcode with no substantive meaning is *not* testimonial when the only information communicated is the passcode, then the Fifth Amendment analysis need proceed no further: the passcode is not protected.

The Court should grant certiorari to answer this extremely important question of federal law.

**2.** The Court should also grant certiorari to address the continued validity of a decades-old analogy from this Court's cases that has distorted lower courts' analysis of this question.

With one notable exception, state appellate courts that have considered the question have concluded disclosing a passcode with no substantive meaning is testimonial. In reaching this conclusion, they've relied heavily on an analogy first suggested by Justice Stevens in a 1988 dissent in *Doe v. United States*, 487 U.S. 201 (1988) (*Doe II*).<sup>4</sup>

The question in *Doe II* was whether it was testimonial to sign a statement authorizing a bank to disclose records of any accounts the signer may have had at the bank. *Id.* at 204-06. Signing the statement was not testimonial because the statement did not, either "explicitly or implicitly, relate a factual assertion or disclose information." *Id.* at 210. The statement did not indicate that any such accounts existed or that the bank had any records of such accounts. It merely authorized disclosure *if* the accounts existed and *if* the bank had records. *See id.* at 215.

Writing only for himself, Justice Stevens argued in dissent that the statement was testimonial because it compelled Doe to "use his mind to assist the Government in developing its case." Id. at 220 (Stevens, J., dissenting). He drew an analogy between a key and a safe combination: "[I]n some cases," Justice Stevens wrote, a suspect can "be forced to surrender a key to a strongbox containing incriminating documents" because doing so would not require the suspect "to use his mind to assist the prosecution." Id. at 219. But compelling a suspect to "reveal the combination to his wall safe" would be different because that would require the use of the suspect's mind. Id. The majority did not disagree with the analogy, but said that in its view. signing the statement was more like

<sup>&</sup>lt;sup>4</sup> The State adopts the convention of referring to the 1988 *Doe* decision as *Doe II* to avoid confusion with an earlier 1984 decision with the same party names. *See United States v. Doe*, 465 U.S. 605 (1984) (*Doe I*).

surrendering a key than revealing a safe combination. *Id.* at 210 n.9.

Twelve years later, in United States v. Hubbell, 530 U.S. 27 (2000), Justice Stevens repeated his analogy in a majority opinion. In Hubbell, the government served the respondent with a subpoena for various categories of documents, in response to which he produced over 13,000 pages. Id. at 31. Writing for the majority, Justice Stevens concluded the act of producing the documents was "testimonial" insofar as it revealed the existence and location of the documents and the respondent's control over them. Id. at 40-45. He further wrote that the respondent "unquestionably" had to "make extensive use of 'the contents of his own mind" in responding to the subpoena and that assembling the documents was "like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox." Id. at 43.

State appellate courts have heavily relied on Justice Stevens's analogy in concluding that disclosing a passcode—even when the passcode has no substantive meaning—is testimonial. The New Jersey Supreme Court, for example, held that communicating a passcode is a "testimonial act of production" because a "cellphone's passcode is analogous to the combination to a safe." State v. Andrews, 234 A.3d 1254, 1273 (N.J. 2020). "Communicating or entering a passcode," the court reasoned, "requires facts contained within the holder's mind-the numbers, letters or symbols composing the passcode." Id. The Pennsylvania Supreme Court similarly concluded that "the disclosure of a password" is "testimonial" because it constitutes "the electronic equivalent to a wall safe—the passcode to unlock" the device. Commonwealth v. Davis, 220 A.3d 534, 548 (Pa. 2019); see also id. at 551 n.10 ("[T]here is no meaningful distinction between the government compelling a suspect to provide the combination to access a safe, and the government forcing one to disclose a password to access a computer."). And in this case, the Utah Supreme Court used Justice Stevens's analogy to explain the framework the court applied in concluding that disclosing a passcode is testimonial. *See* App. 23a-24a, ¶¶46-48.

In contrast, in the one state appellate case that has concluded providing a passcode is *not* testimonial, the court expressly questioned both the analytical value of Justice Stevens's analogy and "the continuing viability of any distinction" between keys and combinations "as technology advances." State v. Stahl, 206 So. 3d 124, 135 (Fla. Dist. Ct. App. 2016); see id. ("We question whether identifying the key which will open the strongbox—such that the key is surrendered—is, in fact, distinct from telling an officer the combination."). The court noted that "[c]ompelling an individual to place his finger on" an "iPhone would not be a protected act" because it would be merely "an exhibition of a physical characteristic." Id. And it said it was "not inclined to believe that the Fifth Amendment should provide greater protection to individuals who passcode protect their iPhones with letter and number combinations than to individuals who use their fingerprint as the passcode." Id. (emphasis added).

Other courts have expressed similar doubts about the continued usefulness of Justice Stevens's analogy. The New Jersey Supreme Court, for example—even while relying on the analogy to conclude that disclosing a passcode is testimonial—said it "share[d] the concerns voiced by other courts that holding passcodes exempt from production whereas biometric device locks may be subject to compulsion creates inconsistent approaches based on form rather than substance." *Andrews*, 234 A.3d at 1274. The court continued: "The distinction becomes even more problematic when considering that, at least in some cases, a biometric device lock can be established only after a passcode is created, calling into question the testimonial/non-testimonial distinction in this context." *Id*.

The Illinois Appellate Court, in turn, has reasoned that "given the advancements in technology, a cellphone passcode is more akin to a key to a strongbox than a combination to a safe." *People v. Sneed*, 187 N.E.3d 801, 813 (Ill. App. Ct. 2021), *aff'd on other* grounds No. 127968, 2023 IL 127968, ... N.E.3d ... (Ill. June 15, 2023), *cert. denied* No. 23-5827, 2024 WL 759835 (Feb. 26, 2024). The court further observed that "perhaps in this digital age the distinction between a physical key and a combination to a safe has become blurred, with a cellular phone passcode encompassing both." *Id*.

The Court should grant certiorari to address these well-founded criticisms and decide whether a decadesold analogy that long predates the era of modern digital technology should continue to guide lower courts' Fifth Amendment analysis. Unlike wall safes, modern cellphones cannot be opened by alternative means such as physically drilling the lock. *See, e.g.*, App. 8a,  $\P\P17-18$  (describing police's failed efforts to access Valdez's phone through alternative means). Also unlike wall safes, many cellphones automatically wipe their contents after a certain number of wrong guesses. *See* App. 42a-43a,  $\P7$ .

Perhaps even more to the point, as the Illinois Supreme Court has recognized, a cellphone passcode "may be used so habitually that its retrieval is a function of muscle memory rather than an exercise of conscious thought." *Sneed*, 2023 IL 127968, at \*12 (quoting *Sneed*, 187 N.E.3d at 812). Unlike with wall safes, most people unlock their cellphones dozens or even hundreds of times a day. A "fair question" thus arises "whether the rote application of a series of numbers should be treated the same as" scenarios that require "exhaustive use of the 'contents of [one's] mind," such as the massive document production in *Hubbell*. *Sneed*, 187 N.E.3d at 812.

Finally, this Court has never provided a rationale for the key/combination analogy, nor has it grounded the analogy in text or history. The analytical value of the analogy is thus highly questionable. In both the key scenario and the safe-combination scenario the person uses "the contents of his own mind" to identify and turn over the relevant item or information. Hub*bell*, 530 U.S. at 43. In both scenarios the person engages in a physical act that communicates information: handing over the key, forming words with his mouth. The person also is not being asked to create anything new, but instead merely to "surrender" something already in his possession. Fisher, 425 U.S. at 411. The only difference is that in the key scenario the thing being surrendered is a physical object, whereas in the safe-combination scenario the thing being surrendered is a piece of information. Information whose only function is to perform the same physical act-opening the locked device. Fifth Amendment protection should not turn on such immaterial distinctions. And nothing in the amendment's text or history suggests that it should.

Yet because the analogy arises from this Court's jurisprudence, only this Court can answer whether and how the key/combination analogy should apply to devices like cellphones—or indeed, whether it should continue to apply at all. Absent such guidance, lower courts will continue to apply the analogy to defeat valid warrants despite the serious questions just raised because only this Court can reconsider and, if necessary, clarify its scope.

**3.** The Court should also grant certiorari to decide whether disclosing a passcode is testimonial because doing so will help answer another extremely important question: whether *entering* a cellphone passcode is testimonial.

Sometimes, rather than asking a suspect to disclose a passcode, law enforcement instead asks the suspect to *enter* the passcode. *See, e.g., Seo v. State*, 148 N.E.3d 952, 953 (Ind. 2020). This unlocks the phone so law enforcement can then access its contents.

Lower courts have reached varying conclusions on whether entering a passcode is testimonial. On one side is the Eleventh Circuit and at least three state supreme courts, all of which have concluded that entering a passcode (or performing an equivalent act such as decrypting data with a password) *is* testimonial. See In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012); Sneed, 2023 IL 127968, at \*11-13; Seo, 148 N.E.3d at 955-57; Commonwealth v. Gelfgatt, 11 N.E.3d 605, 614 (Mass. 2014). On the other side is the Fourth Circuit, which has suggested that entering a passcode is not testimonial. See United States v. Oloyede, 933 F.3d 302, 309 (4th Cir. 2019).

Answering whether disclosing a cellphone passcode is testimonial will also help answer whether entering a passcode is testimonial, in at least two ways. First, if disclosing a cellphone passcode is *not* testimonial when the only information communicated is the passcode, then it follows that entering a passcode is not testimonial either. If the verbal act of providing a passcode is not testimonial, *a fortiori* the nonverbal act of typing a passcode, or swiping a pattern, also is not testimonial.

Second, if disclosing a cellphone passcode *is* testimonial, the *reason* it's testimonial will help answer whether entering a passcode is likewise testimonial. If, for example, the Court adopts the key/combination analogy and concludes disclosing a passcode is like revealing the combination to a safe, then entering a passcode should *not* be testimonial because it's more like using a key. *See Sneed*, 2023 IL 127968, at \*13 (entering a passcode is "comparable to using a key to unlock a door"). Alternatively, if the Court determines disclosing a passcode is testimonial because it implicitly asserts certain facts—such as the existence of the passcode and the suspect's knowledge of it, *see id.* at \*11-13—then entering a passcode *could* be testimonial if it communicates similar information.

Answering the first question presented will thus help answer another extremely important question. For this reason too, the Court should grant certiorari.

II. State supreme courts are divided over whether the foregone-conclusion doctrine applies to the disclosure of a passcode when the government has evidence the device belongs to the suspect.

1. Under the foregone-conclusion doctrine, an otherwise testimonial act lacks Fifth Amendment protection when the "testimony" involved in the act "adds little or nothing to the sum total of the Government's

information." *Fisher*, 425 U.S. at 411. This means that even if disclosing a cellphone passcode is testimonial, no Fifth Amendment protection attaches if the "testimony" involved in the act of disclosure is a foregone conclusion.

The foregone-conclusion doctrine originated in *Fisher*, 425 U.S. 391. There, a group of taxpayers obtained documents from their accountants and transferred them to their attorneys. *Id.* at 393-94. When the government later subpoenaed the documents from the attorneys, the taxpayers argued that compelling disclosure would violate their Fifth Amendment rights. *Id.* at 394-95.

The Court found no Fifth Amendment violation. It noted that the creation of the documents "was wholly voluntary." *Id.* at 409. Thus, the documents themselves could not "be said to contain compelled testimonial evidence." *Id.* at 409-10.

The Court additionally observed that the "act of producing" the documents could have "communicative aspects of its own, wholly aside from the contents of the papers produced." *Id.* at 410. For example, it might "concede[] the existence of the papers," "their possession or control by the taxpayer," or "the taxpayer's belief that the papers are those described in the subpoena." *Id.* 

The Court acknowledged the possibility that, under certain circumstances, such "tacit averments" could "rise[] to the level of testimony within the protection of the Fifth Amendment." *Id.* at 410-11. But it determined that producing the taxpayers' documents in *Fisher* would not involve "testimony" because the information communicated by the act of production the "existence and location of the papers"—was "a foregone conclusion." *Id.* at 411, 414. Conceding the taxpayers' control over the documents would "add[] little or nothing to the sum total of the Government's information." *Id.* at 411. "The question [was] not of testimony but of surrender." *Id.* at 411 (quoting *In re Harris*, 221 U.S. 274, 279 (1911)).

The Court addressed the foregone-conclusion doctrine again in *Hubbell*. There, as previously explained, the government served the respondent with a subpoena for various categories of documents, in response to which he produced over 13,000 pages. 530 U.S. at 31. Unlike in *Fisher*, the government did not have prior knowledge that the documents existed or were in the respondent's possession. *Id.* at 44-45.

As in *Fisher*, the Court affirmed that the contents of the documents were not "compelled testimony" because they had been voluntarily created. *Id.* at 40; *see also id.* at 36. Rather, the question was whether the "act of producing" the documents had "testimonial" significance. *Id.* at 40. The Court concluded it did because producing the documents disclosed both their "existence and location." *Id.* at 41. The Court rejected the government's attempt to invoke the foregone-conclusion doctrine because, unlike in *Fisher*, "the Government ha[d] not shown that it had any prior knowledge of either the existence or the whereabouts of" the documents. *Id.* at 45.

*Fisher* and *Hubbell* accordingly recognize that when the "testimony" involved in a testimonial act adds little or nothing to the government's existing information, Fifth Amendment protections do not apply.

2. State supreme courts are divided over whether the foregone-conclusion doctrine applies to the disclosure of a passcode when the government has evidence the device belongs to the suspect.

On one side is the New Jersey Supreme Court, which says the "testimonial value" of producing a passcode "may be overcome if the passcode['s] existence, possession, and authentication are foregone conclusions." Andrews, 234 A.3d at 1274. In Andrews, the court found all three elements were satisfied where the phones at issue were password-protected, the government established the suspect owned and operated the phones, and the passcodes "self-authenticate[d] by providing access to the cellphones' contents." Id. at 1275. Thus, the Fifth Amendment did not protect against the passcodes' compelled disclosure. Id. In reaching this conclusion, the court rejected the argument that the *contents* of the cellphone must be a foregone conclusion, noting the "fundamental distinction" this Court drew in both Fisher and Hubbell "between the act of production and the documents to be produced." Id. at 1273-74.

The Pennsylvania and Utah Supreme Courts, by contrast, reject application of the foregone-conclusion doctrine to the disclosure of a passcode when the government has evidence the device belongs to the suspect.

In *Commonwealth v. Davis*, the Pennsylvania Supreme Court refused to apply the foregone-conclusion doctrine when law enforcement sought an order compelling the defendant to reveal the password to his computer. 220 A.3d at 549-51. The court reasoned that this Court has applied the doctrine "only in the compulsion of specific existing business or financial records" and has been "ambiguous concerning the breadth of the rationale as well as its value." *Id.* at

549. The court further reasoned that declining to apply the doctrine was "entirely consistent with" decisions from this Court, such as *Hubbell*, that protect "information arrived at as a result of using one's mind." *Id*.

In its decision below, the Utah Supreme Court applied similar reasoning in refusing to apply the foregone-conclusion doctrine to Valdez's refusal to provide his passcode.<sup>5</sup> It noted that this Court "has never applied the exception outside of the context of assessing the testimoniality of a nonverbal act of producing documents" and reasoned that this "limited context" demonstrates the doctrine's "narrow focus." App. 33a, ¶64. The court thus concluded the doctrine is "inapplicable" outside the context of the physical act of producing documents. App. 33a, ¶65.

**3.** This split has important consequences for law enforcement's ability to investigate and solve crimes. To date, every state supreme court and federal appellate court that has considered the question has held that disclosing a passcode (or performing an equivalent act) is testimonial—largely based on Justice Stevens's legacy key/combination analogy. *See supra* Part I.2. This in turn means that whether law enforcement can compel a suspect to provide the passcode to his or her phone—and thus enable law enforcement to execute lawful warrants to obtain potentially crucial and in some cases life-saving information—turns on whether the foregone-conclusion doctrine applies. All because of a decades-old metaphor.

 $<sup>^5</sup>$  There was never any dispute that the phone belonged to Valdez. Police seized it from him when he was arrested. App. 42a-43a,  $\P7$ .

In many or most cases, the government will have clear evidence the phone belongs to the suspect because it was seized from the suspect or because the number associated with the phone can be matched to the suspect. Such ownership establishes through obvious implication that the suspect knows the passcode. *See Andrews*, 234 A.3d at 1275; *Gelfgatt*, 11 N.E.3d at 615.

Thus, in cases where law enforcement has evidence the phone belongs to the suspect, the foregoneconclusion doctrine should authorize law enforcement to compel the suspect to disclose the passcode—or allow adverse use of the suspect's refusal at trial—because the existence, possession, and authenticity of the (self-authenticating) passcode are foregone conclusions. The foregone-conclusion doctrine, that is, provides law enforcement a legally sound avenue to gain access to the phone's contents even *if* providing the passcode is testimonial. But only if the doctrine applies.

Law enforcement's ability to solve crimes by accessing crucial evidence on cellphones should not turn on which state the crime occurred in. Nor should justice for crime victims depend on whether the state they were victimized in applies the foregone-conclusion doctrine to cellphone passcodes. This is precisely the sort of issue that cries out for a single uniform standard nationwide, which only this Court can provide.

4. As with the first question presented, answering the second question presented will also help answer another important question: whether the foregoneconclusion doctrine applies to *entry* of a passcode when the government has evidence the device belongs to the suspect.

As noted, *see supra* Part I.3, rather than asking a suspect to disclose a passcode, law enforcement sometimes asks the suspect to *enter* the passcode. This unlocks the phone so law enforcement can then access its contents. The foregone-conclusion doctrine is relevant in that context as well because, as explained, if the doctrine applies it provides law enforcement an avenue to gain access to the phone's contents even *if* entering the passcode is testimonial.

Lower courts have reached varying conclusions about whether the foregone-conclusion doctrine should apply to entering a passcode (or performing an equivalent act such as decrypting data with a password) when law enforcement has evidence the device belongs to the suspect. Most courts that have considered the question have concluded the doctrine does apply provided the government can make the requisite showing of ownership. See, e.g., Sneed, 2023 IL 127968, at \*13-16; Gelfgatt, 11 N.E.3d at 614-16; Reynolds v. State, 516 P.3d 249, 252-54 (Okla. Crim. App. 2022). The Indiana Supreme Court, by contrast, has suggested the doctrine should not apply. See Seo, 148 N.E.3d at 958 (reasoning that the doctrine "may be generally unsuitable to the compelled production of any unlocked smartphone").

Answering whether the foregone-conclusion doctrine applies to the disclosure of a passcode when the government has evidence the device belongs to the suspect will help answer this related question as well.

First, if the doctrine *does* apply to disclosing a passcode, then *a fortiori* the doctrine should also apply to entering a passcode. When the government has

evidence a device belongs to the suspect, any "testimony" involved in the act of entering a passcode is just as much of a foregone conclusion as any "testimony" involved in the act of disclosing the passcode. In both instances the suspect's ownership of the device establishes through obvious implication that the suspect knows the passcode. *See supra* Part II.3. The existence, possession, and authenticity of the (self-authenticating) passcode is thus a foregone conclusion. Entering it "adds little or nothing to the sum total of the Government's information." *Fisher*, 425 U.S. at 411.

Second, if the foregone-conclusion doctrine does *not* apply to disclosing a passcode, the reason it doesn't apply will help answer whether the doctrine applies to entering a passcode. If, for example, the doctrine doesn't apply because it's limited to "the compulsion of specific existing business or financial records," *Davis*, 220 A.3d at 549, then the doctrine may not apply to entering a passcode either because a passcode is not an existing business or financial record. Alternatively, if the reason the doctrine doesn't apply to disclosing a passcode is because it's limited to "nonverbal" acts, App 33a, ¶64, then the doctrine *should* apply to the nonverbal act of entering a passcode, provided the government can make the necessary showing of ownership.

Answering the second question presented will thus help answer another important question. For this reason too, the Court should grant certiorari.

# III. These questions are important and recurring.

The Court should decide the questions presented now because they're recurring and directly bear on law enforcement's ability to search electronic devices recovered during criminal investigations. There is no reason to await further percolation in the lower courts.

Electronic devices are a ubiquitous feature of modern life. In 2023, 97 percent of Americans owned a cellphone. See Pew Rsch. Ctr., Mobile Fact Sheet (Jan. 31, 2024), https://www.pewresearch.org/internet/factsheet/mobile. In 2018, 92 percent of American households had at least one computer. See U.S. Census Bureau, Computer and Internet Use in the United States: 2018 (Apr. 21, 2021), https://www.census.gov/newsroom/press-releases/2021/computer-internetuse.html.

The ubiquity of these devices raises pressing questions about how constitutional protections should apply to the novel contexts they present. See, e.g., Riley v. California, 573 U.S. 373, 385-86 (2014) (search incident to arrest); Carpenter v. United States, 585 U.S. 296, 318-19 (2018) (expectation of privacy in location data). And their pervasiveness ensures that questions about how and when police may lawfully access such devices during criminal investigations will continue to arise.

Digital evidence also plays an increasingly important role in solving crime. See, e.g., State v. Gonzales-Bejarano, 427 P.3d 251, 253-54 & n.1 (Utah Ct. App. 2018) (encrypted smartphone app used to arrange drug deals); People v. Davis, 438 P.3d 266, 267-2019) (evidence from 68 (Colo. defendant's smartphone sought in murder prosecution). Indeed, in some cases, all the critical evidence, including the corpus of the crime itself, will be digital information stored electronically, such as files depicting child pornography. See, e.g., United States v. Apple MacPro *Comput.*, 851 F.3d 238, 247-48 (3d Cir. 2017)(encrypted child pornography on external hard drives).

But even when, as in this case, police have a lawful right to access digital evidence, they routinely are unable to do so without the device passcode. For all intents and purposes, the device is a black box. And so without clear rules on the subject, law enforcement's inability to obtain the passcode will mean they will be unable to access the digital evidence at all. And this problem will spread in proportion to the extent of the current majority rule.

Law enforcement can sometimes use force to break down barriers to accessing evidence in other contexts. See, e.g., United States v. Kyles, 40 F.3d 519, 522-23 (2d Cir. 1994) (affirming admission of evidence gathered where police broke lock on door inside home). But brute force alternatives often aren't possible for accessing digital contents on a password-encrypted device. See, e.g., State v. Johnson, 576 S.W.3d 205, 218 n.4 (Mo. Ct. App. 2019) (police unable to bypass passcode on iPhone). As this Court has observed, encryption can render cellphones "all but 'unbreakable' unless police know the password." Riley, 573 U.S. at 389.

Whether and when the government can compel a suspect to provide a passcode—or make adverse use of the suspect's refusal at trial—are thus critically important to law enforcement's ability to investigate, solve, and prevent crime. And essential to determining whether and when disclosure can be compelled are the two questions presented: whether disclosing a passcode is testimonial when the only information communicated is the passcode and whether the foregone-conclusion doctrine applies when the government has evidence the phone belongs to the suspect.

The Court should decide these questions now. State and federal courts have thoroughly explored both questions and further illumination seems unlikely. See supra Parts I & II. In answering the first question, courts have largely relied on a decades-old metaphor that this Court has never applied to digital evidence and that suffers significant analytical shortcomings in light of technological changes. See supra Part I.2. And on the second question, state supreme courts are divided. See supra Part II.2. Further percolation would only result in more courts reaching differing positions, deepening the split. The continuing confusion will only further frustrate law enforcement's attempts to collect critical evidence.

The time has come for this Court to decide whether it is constitutionally permissible for the government to compel a suspect to disclose his or her passcode so law enforcement can carry out a valid search warrant on the suspect's phone.

## IV. This case presents an excellent vehicle to address these extremely important questions.

This case comes to the Court without jurisdictional defects and with the issues and facts cleanly presented.

First, the Court unquestionably has jurisdiction. The State petitions for certiorari from a final judgment of the Utah Supreme Court following Valdez's trial. App. 8a-12a, ¶¶19-25; see 28 U.S.C. § 1257. That procedural posture contrasts with other cases in which petitioners have sought review from *interlocutory* decisions granting or denying Fifth Amendment protection to the production of cellphone passcodes. See Br. in Opp. at 6-11, Sneed v. Illinois, No. 23-5827, cert. denied 2024 WL 759835 (Feb. 26, 2024); Br. in Opp. at 10-13, Andrews v. New Jersey, No. 20-937, cert. denied 141 S. Ct. 2623 (2021); Br. in Opp. at 10-11, Pennsylvania v. Davis, No. 19-1254, cert. denied 141 S. Ct. 237 (2020).

Second, the issues are cleanly presented. The only disputed Fifth Amendment element in this case is testimoniality. The parties do not contest the other Fifth Amendment elements—compulsion and incrimination—nor does the State claim harmless error. See App. 19a, 37a, ¶¶39, 74. And the Utah Supreme Court cleanly decided both questions presented. See App. 18a-30a, ¶¶38-58 (testimoniality); *id.* at 30a-33a, ¶¶59-65 (foregone-conclusion doctrine).

Moreover, the issues are cleanly presented within the Fifth Amendment framework. Under other circumstances, as the Utah Supreme Court noted, commenting on a defendant's post-Miranda refusal to provide a passcode might raise due process questions under Doyle v. Ohio and its progeny. See App. 14a-17a, ¶¶29 n.6, 34 n.7. However, because both parties framed the case as a Fifth Amendment question, the Utah Supreme Court decided it on traditional Fifth Amendment grounds. See App. 16a-17a, ¶34 n.7 ("[W]e address only the Fifth Amendment arguments that the parties have made."). This Court may therefore decide those same issues as they have been cleanly presented to the Court. See United States v. Williams, 504 U.S. 36, 41 (1992) (Court's review extends to issues "pressed or passed upon below").

Third, the facts are cleanly presented. The Utah Supreme Court determined that "the best reading of the record is that the detective asked Valdez to verbally provide his passcode." App. 24a-25a, ¶49. Neither party challenged that reading of the record below. See id. And the Utah Supreme Court decided the case based on that reading. Id.

This case thus contrasts with other cases where the suspect was ordered to either disclose or enter the passcode. See, e.g., Sneed, 2023 IL 127968, at \*10 n.5. Such cases present multiple factual scenarios that might implicate divergent Fifth Amendment analyses. See App. 24a, ¶48 (suggesting different "analytical framework[s]" depending on whether a suspect disclosed or entered a passcode). And addressing one of those scenarios could obviate the need to address the other one. See Sneed, 2023 IL 127968, at \*16 n.7 (declining to address whether disclosing passcode is testimonial because suspect could comply with order by entering passcode).

Here, both the lower court and parties agree this is a case involving *disclosure* of a passcode. The case thus presents a clean set of facts on which to decide the clean issues presented.

#### V. The decision below is incorrect.

The Utah Supreme Court wrongly concluded that the Fifth Amendment protected Valdez's refusal to provide his passcode. Disclosing a cellphone passcode with no substantive meaning is not testimonial when the only information communicated is the passcode because the passcode itself doesn't communicate anything. It's merely a meaningless set of numbers or meaningless swipe pattern. And even if disclosing the passcode is testimonial, the foregone-conclusion doctrine readily applies when, as here, the government has evidence the phone belongs to the suspect. Providing the passcode in that scenario "adds little or nothing to the sum total of the Government's information" about the existence, possession, and authenticity of the passcode. *Fisher*, 425 U.S. at 411.

## A. Disclosing a cellphone passcode is not testimonial when the passcode has no substantive meaning and the only information communicated is the passcode.

Although this Court has addressed the meaning of "testimonial" on a variety of occasions, *see*, *e.g.*, *Fisher*, 425 U.S. at 408-14; *Doe II*, 487 U.S. at 207-19; *Hubbell*, 530 U.S. at 34-37, 40-45, it has not provided a definition of the term. Several guiding principles, however, may be drawn from the Court's cases.

First, to be testimonial, something has to be communicated. See Doe II, 487 U.S. at 211 ("Unless some attempt is made to secure a communication . . . the demand made upon [the suspect] is not a testimonial one."). Second, the communication "must itself, explicitly or implicitly, relate a factual assertion or disclose information." Id. at 210. Third, the government must rely on the suspect's "consciousness of the facts and the operation of his mind in expressing it." Id. at 211. Stated differently, the government must rely on the truthfulness of the statement to prove a fact. See id. at 215 (statement authorizing release of bank records not testimonial where government was "not relying upon the 'truthtelling" of the statement to show the existence of the records or suspect's control over them). Fourth, the decision whether to provide the information must place the suspect in the "cruel trilemma of self-accusation, perjury, or contempt." Pennsylvania v. Muniz, 496 U.S. 582, 596-97 (1990) (quoting Doe II, 487 U.S. at 212). That is, it must require the suspect "to choose between revealing incriminating private thoughts," "committing perjury," or facing contempt. *Id*.

Under these principles, disclosing a passcode is not testimonial when, as here, the passcode has no substantive meaning and the only information that would be communicated by disclosure is the passcode itself. First, the passcode doesn't communicate anything. It's merely a meaningless set of numbers or meaningless swipe pattern. Second, the passcode itself doesn't relate any facts or information. It simply unlocks the phone. Third, as in this case, when ownership of the phone is not in question, the suspect's consciousness that the passcode will open the phone is of no significance. Whether or not the suspect told the "truth" when providing the passcode is irrelevant to any fact the government will need to prove at trial. Fourth, when ownership of the phone is not in question, asking for the passcode does not place the suspect in the "cruel trilemma" of self-accusation, perjury, or contempt. The suspect can disclose the code without "selfaccusation" because the code has no substantive significance and law enforcement is already able to connect the suspect to the phone. Although disclosing a passcode *might* be testimonial if the passcode itself relates information about the suspect or if disclosure communicates something beyond simply "this is how you open the phone," neither of those circumstances is present here.

In *Doe II*, this Court explained that the policies underlying the Fifth Amendment "are served when the privilege is asserted to spare 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." 487 U.S.

at 213. But when, as here, ownership of the cellphone is not in question, disclosing a passcode that has no substantive meaning does not reveal facts that relate the suspect to the offense or share the suspect's thoughts or beliefs with the government. Nor will the passcode be used against the defendant in court. It merely enables law enforcement to access the phone. That is not testimonial.

The Utah Supreme Court concluded otherwise because providing a passcode "discloses information from the person's mind." App. 17a-18a, ¶36. This simplistic reasoning overreads this Court's prior statements, leads to bizarre results, and sets a categorical rule that runs counter to this Court's precedents.

To start, this Court has never identified anything in the text or history of the Fifth Amendment that suggests it was intended to create blanket protection for any information drawn from a "person's mind." Appropriately then, this Court has never suggested that every communication that discloses information from a person's mind is ipso facto testimonial. And such a rule would be clearly incorrect, as this Court has identified a variety of scenarios where a person can do or say something that discloses information from the person's mind but is not testimonial. Handing over a key to a strongbox, for example, communicates that the person believes the key will open the strongbox. Providing a handwriting sample discloses information from the person's mind about how to form letters on a page. And reading a transcript provides information from the person's mind about the tone, pitch, and volume the person selected. Indeed, virtually every volitional act a person could do can rightly be said to originate in the person's mind. Yet none of those scenarios involves "testimony" protected by the Fifth Amendment. See Hubbell, 530 U.S. at 43 (strongbox key); Gilbert, 388 U.S. at 266-67 (handwriting sample); United States v. Dionisio, 410 U.S. 1, 7 (1973) (reading from transcript).

Valdez's passcode—a specific swipe pattern—is as substantively meaningless as a string of letters a person might form for a handwriting sample or a combination of words a person might speak for a voice exemplar. And, like handing over a key, it communicates nothing more than the person's belief that it will open the phone.

Next, having Fifth Amendment protection turn on whether a person discloses information from his or her mind would yield nonsensical results. For example, a voice exemplar where a person is told what to say would *not* be testimonial because the person would merely be repeating words chosen by someone else. But a voice exemplar where a person is told to say a random sentence *would* be testimonial because the exemplar would disclose information from the person's mind—even if those words are meaningless or unrelated to the criminal investigation. Having Fifth Amendment protection turn on who chose the words would do nothing to further constitutional principles. Instead, it would elevate form over substance.

Finally, a categorical rule that any communication that discloses information from a person's mind is testimonial conflicts with what this Court has said about the fact-dependent nature of the inquiry. In *Fisher*, the Court instructed that whether a statement is testimonial is not a question that "lend[s]" itself "to categorical answers." 425 U.S. at 410. Rather, resolution "often depends on the facts and circumstances of the particular case." *Doe II*, 487 U.S. at 214-15. In suggesting a categorical rule that all communications that disclose information from the mind are testimonial, the Utah Supreme Court disregarded this teaching.

The Utah Supreme Court additionally distinguished between *saying* something that conveys information and *doing* something that conveys information, suggesting that the former is always testimonial. See App. 26a-27a, ¶51 ("Directly providing a passcode to law enforcement is not an 'act.' It is a statement. There is no need to tease out whether the statement implicitly communicates information to determine whether it has testimonial value."). This reasoning again suffers multiple flaws.

To start, this Court has never said that every verbal or written statement that communicates information from the mind is testimonial. Rather, the "content" of the communication "must have testimonial significance." *Doe II*, 487 U.S. at 211 n.10. And the government must rely on the suspect's "consciousness of the facts and the operation of his mind in expressing it." *Id.* at 211.

It's also unclear under this Court's case law why there should be a difference for Fifth Amendment purposes between saying something that communicates information and doing something that communicates information. Whether a communication occurs verbally or through an act has nothing to do with whether the person is placed in the "cruel trilemma of self-accusation, perjury, or contempt." *Muniz*, 496 U.S. at 596 (quoting *Doe II*, 487 U.S. at 212). Nor does it have anything to do with whether the person has been compelled to reveal "his knowledge of facts relating him to the offense." *Doe II*, 487 U.S. at 213. As just explained, the "content" of the communication "itself must have testimonial significance." *Id.* at 211 n.10. And the content of a communication doesn't have testimonial significance just because it's verbal.

In its decision below, the Utah Supreme Court conceded that "functionally, there may not be much realworld difference between verbally speaking or writing out a passcode for the police and physically providing an unlocked device to police. Both give access to the contents of the device—the ultimate objective of law enforcement." App 24a, ¶42. Creating different Fifth Amendment regimes for these two scenarios, as the decision below does, exalts form over substance. The answer in both cases should be the same: neither is testimonial.

## B. The foregone-conclusion doctrine readily applies to disclosure of a cellphone passcode when the government has evidence the phone belongs to the suspect.

As explained, the foregone-conclusion doctrine holds that an otherwise testimonial act lacks Fifth Amendment protection when the "testimony" involved in the act "adds little or nothing to the sum total of the Government's information." *Fisher*, 425 U.S. at 411. The Court evaluates the testimony involved in the act itself, not the content of what that act *produces*, because the content—provided it was created voluntarily—lacks Fifth Amendment protection. *See id.* at 409-11.

Application of this doctrine to disclosure of a cellphone passcode is straightforward when, as here, the government has evidence the phone belongs to the suspect. The phone was seized from Valdez when he was arrested, App. 42a-43a, ¶7, and the fact that he owned the phone was never in dispute. As explained, ownership of a phone establishes through obvious implication that the owner knows the passcode. See Andrews, 234 A.3d at 1275; Gelfgatt, 11 N.E.3d at 615. The passcode's existence is self-evident, and the code self-authenticates when it opens the phone. Thus, disclosing the passcode would "add[] little or nothing to the sum total of the Government's information" about the existence, possession, and authenticity of the passcode. Fisher, 425 U.S. at 411. It is not necessary for the government to prove that it knows the contents of the passcode—or of the phone for the matter—because both the passcode and the phone's files were voluntarily created and thus lack independent Fifth Amendment protection.

The Utah Supreme Court concluded otherwise based on the view that the foregone-conclusion doctrine is "inapplicable outside" the context of the physical act of producing evidence. App. 33a, ¶65. This Court has never held that, nor has it suggested the doctrine is limited to nonverbal document production. The Utah Supreme Court's distinction between verbal and nonverbal acts of production also suffers significant flaws.

First, whether a person produces something verbally or nonverbally has nothing to do with whether the act of production "adds" "to the sum total of the Government's information." *Fisher*, 425 U.S. at 411. Second, when the thing produced was voluntarily created, it's not compelled and therefore not protected by the Fifth Amendment. *See id.* at 409. Producing it verbally rather than nonverbally does not change that. Third, this Court has expressly rejected the argument that Fifth Amendment protection for acts is "more narrow" than protection for "oral or written statements." *Doe II*, 487 U.S. at 209.

At base, the Utah Supreme Court's reasoning rests on the view that disclosing a passcode is categorically different from an "act of production." App. 6a, ¶9. But that view is simply not sound. In all relevant respects, disclosing a passcode *is* an act of production. The passcode already exists. It's already been saved on the suspect's phone. The suspect is merely being asked to *turn over* the passcode. As in *Fisher*, it's a matter "not of testimony but of surrender." 425 U.S. at 411 (quoting *Harris*, 221 U.S. at 279).

## CONCLUSION

The Court should grant the petition.

Respectfully submitted, SEAN D. REYES Utah Attorney General STANFORD E. PURSER Utah Solicitor General Counsel of Record CHRISTOPHER A. BATES ANDREW F. PETERSON **Deputy Solicitors General** JEFFREY D. MANN CONNOR NELSON DAVID A. SIMPSON Assistant Solicitors General 350 N. State Street, Suite 230 P.O. Box 142320 Salt Lake City, UT 84114-2320 Telephone: (801) 538-9600 spurser@agutah.gov

Counsel for Petitioner

Dated: March 13, 2024

35