No. 20-937

In the Supreme Court of the United States

ROBERT ANDREWS,

Petitioner,

v.

STATE OF NEW JERSEY,

Respondent.

ON PETITION FOR WRIT OF CERTIORARI TO THE SUPREME COURT OF NEW JERSEY

BRIEF IN OPPOSITION

Gurbir S. Grewal
Attorney General of New Jersey
Jeremy M. Feigenbaum*
State Solicitor
Angela Cai
Deputy State Solicitor
Lila B. Leonard
Deputy Attorney General
Office of the Attorney General
of New Jersey
25 Market Street
Trenton, NJ 08625
(609) 984-6500
jeremy.feigenbaum@njoag.gov

Theodore N. Stephens, II
Acting Essex
County Prosecutor
Frank J. Ducoat
Director, Appellate Section
Caroline C. Galda
Assistant Prosecutor
Office of the Essex County
Prosecutor
50 West Market St.
Newark, NJ 07102

* *Counsel of Record*

QUESTION PRESENTED

Whether the Fifth Amendment's foregone conclusion doctrine permits compelled decryption of Petitioner's phones, when the State has a valid search warrant for the phones' contents.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTRODUCTION

Six months ago, this Court denied a petition raising the questions presented here: whether the Fifth Amendment's foregone conclusion doctrine can apply to an encrypted phone's passcode, and if so, whether the lodestar of the analysis is defendant's knowledge of the device's passcode or contents. See Pet. for Cert., *Pennsylvania v. Davis*, No. 19-1254 (Apr. 20, 2020); 141 S. Ct. 237 (2020) (order denying certiorari). By the time the *Davis* petitioner filed its reply brief, the New Jersey Supreme Court had already issued the decision below, and the *Davis* petitioner raised it as part of the split alleged. See Reply Br. at 1-2, *Pennsylvania v. Davis*, No. 19-1254 (Sept. 21, 2020). But this Court denied certiorari in October 2020, and no intervening developments have happened since—that is, no new circuits or state supreme courts have weighed in.

Petitioner claims a different result is nevertheless warranted, but he faces a significant threshold problem: Petitioner has not yet gone to trial, let alone been convicted and sentenced. The lack of a final judgment means this Court lacks jurisdiction to take up the case on this posture. And there is no basis to treat this interlocutory state court decision as reviewable: while the state courts below did decide that decryption of the phone could be compelled, future proceedings before the trial court may obviate the need for review of any Fifth Amendment issues in this case. Petitioner may claim that he no longer remembers the passcodes. The phones may contain no evidence that materially adds to the case against Petitioner. Or the jury may acquit Petitioner of all charges, even after the State presents its case. There is thus no basis for review at this time,

and at the very least, these factors confirm why this case is a poor vehicle for review.

Even absent this threshold problem, review is not warranted. Although Petitioner primarily urges certiorari to resolve two splits as to whether and how the foregone conclusion doctrine applies to an encrypted phone's passcode, this case does not implicate either one. Petitioner alleges a split over whether a suspect could be required to verbally "communicate" the "pure testimony" of his device's passcode. Pet. 1, 2, 7. Yet in this case, Petitioner will be allowed to directly enter the passcode *without* divulging it—a situation Petitioner himself says does not implicate a split. And although Petitioner also asserts a subsidiary split over whether the "conclusion" that must be "foregone" is a defendant's knowledge of his device's passcode or his knowledge of its contents, the court below determined the result here would be the same either way. Because relatively few courts have addressed the question presented to date, this Court can allow further percolation—and, if it sees fit, address these issues in a case that more cleanly presents them.

Finally, the decision below was correctly decided under precedent and first principles. For four decades, this Court and lower courts have agreed that the act of producing documents in response to a subpoena does not run afoul of the Fifth Amendment when "the existence and location of the papers are a foregone conclusion." *Fisher v. United States*, 425 U.S. 391, 411 (1976). That makes good sense: the testimony implied by the act of production itself is only that the records exist and the defendant possesses them. But if that is information known to the State, the self-incrimination

concerns at the heart of the Fifth Amendment are not implicated. And the same is true here. Whenever a suspect enters his passcode, he is only confirming that he, in fact, knows the code. If the government knows as much, that suspect has not incriminated himself and the Fifth Amendment is not offended. Whether the State can then search the documents produced in response to a subpoena, and whether it can search the contents of a now-unlocked phone, become issues under the *Fourth Amendment*—as they involve no testimony at all. A contrary rule would elevate form over substance, allowing the State to enforce a search warrant if a device is protected by biometrics but not by a passcode. And it would offer those seeking to evade a lawful search warrant a path to do so. That has not, and has never been, the law.

STATEMENT OF THE CASE

1. Petitioner Robert Andrews was an officer in the Essex County Sherriff's Office ("ECSO"). Notwithstanding his duty to uphold the law, according to the State's allegations, Petitioner was actively aiding the targets of a law enforcement investigation—divulging whether, when, and how law enforcement was investigating them. Pet. 1a-3a, 78a.

The record reveals the following about the State's investigation so far, which is ongoing. In May 2015, detectives with the Essex County Prosecutor's Office were investigating a narcotics-trafficking network in Newark, New Jersey. During their surveillance, detectives watched their target, Quincy Lowery, operate a motorcycle and Jeep. Detectives uncovered that both vehicles were registered to Petitioner. Pet. 2a, 78a.

Detectives arrested Lowery for a variety of narcotics offenses on June 30, 2015. In a formal statement, Lowery claimed that an officer in the ECSO, who he knew only as "Bolo," helped him conceal his drug trafficking. Lowery knew "Bolo" for about a year. Using a photograph, Lowery identified Petitioner as "Bolo," the officer who helped him and others evade law enforcement. Pet. 1a-2a, 78a, 109a.

Lowery went on to explain that Petitioner assisted him in his illicit operation in several ways: revealing the identity of an undercover officer; warning Lowery about various wiretaps and encouraging Lowery and his affiliates to discard their phones; registering vehicles for Lowery; running license-plate numbers of a vehicle Lowery believed was following him, which turned out to be registered to the Essex County Prosecutor's Office; and suggesting Lowery look for, and get rid of, global positioning system devices under his vehicles. Pet. 3a-5a, 78-79a.

Detectives confirmed much of Lowery's statement through a consensual search of Lowery's phone. The phone revealed the photo of the license plate Lowery had texted to Petitioner. It also revealed a phone number Lowery had saved as "Bolo," which corresponds to the number of one of Petitioner's phones. Lowery told detectives that aside from in-person meetings, Petitioner would often use text messages or Facetime to offer his assistance. Pet. 3-4a, 79a.

Later that night, ECSO's Internal Affairs Department confronted Petitioner and asked him to surrender his two phones—an iPhone 5s and an iPhone 6 Plus. Petitioner handed over the two phones but refused to surrender the passcodes to them, or to input

them and allow Internal Affairs access. Pet. 3a, 79a. Detectives obtained search warrants for the phones from a judge on July 7, 2015, but could not open the iPhones without the passcodes. Pet. 6a, 80a.

In June 2016, a grand jury returned a six-count indictment against Petitioner, charging him with two counts of: second-degree official misconduct, N.J. Stat. Ann. § 2C:30-2 (counts one and two); third-degree hindering apprehension, N.J. Stat. Ann. § 2C:29-3a(2) (counts three and four); and fourth-degree obstruction of the administration of law, N.J. Stat. Ann. § 2C:29-1 (counts five and six). Pet. 5a, 79a-80a.

Efforts to unlock the phones continued but failed. Although detectives obtained search warrants, New Jersey's Telephone Intelligence Unit, the New York Police Department's Technical Services Unit, and Cellebrite, a private company, were unable to access the phones' contents. Left with no other option, the State applied to the trial court for an order compelling Petitioner to grant them access. Pet. 6a. In support, the State cited Lowery's records, which showed 187 phone calls and numerous text messages between Petitioner and Lowery during the 30-day period before Lowery's arrest. But the State lacked the texts themselves because, on Petitioner's advice, Lowery reset his phone a month before his arrest. Pet. 80a, 110a.

2. The trial court granted the State's motion, rejecting Petitioner's defense that the Fifth Amendment and New Jersey law barred any order that he enter or supply his passcode. Pet. 99a-116a. Still, the court's order did not give the State unfettered access to Petitioner's phones; access is limited "to that which is contained within (1) the 'Phone' icon[s] and application[s]

on [Petitioner's] two iPhones and (2) the 'Messages' icon[s] and/or text messaging applications." The order requires the State to perform the search of the phones in camera and in the presence of the judge and defense counsel. Pet. 7a, 81a, 115a-116a.

Petitioner sought and was granted leave to file an interlocutory appeal. Pet. 7a, 81a. The Superior Court of New Jersey, Appellate Division, affirmed the trial court order. See Pet. 77a-97a.

The Supreme Court of New Jersey affirmed. Pet. 1a-75a. As a threshold matter, the majority noted that Petitioner "does not challenge the search warrants issued for his cellphones. He does not claim that the phones were unlawfully seized or that the search warrants authorizing the State to comb their contents were unsupported by probable cause." Pet. 12a. "Neither," the court added, "does defendant challenge the particularity with which the search warrants describe the 'things subject to seizure.'" *Id*. It follows that "the State is permitted to access the phones' contents . . . in the same way that the State may survey a home, vehicle, or other place that is the subject of a search warrant." Pet. 12a-13a; see also Pet. 31a ("[T]he lawfully issued search warrants—the sufficiency of which Andrews does not challenge—give [the State] the right to the cellphones' purportedly incriminating contents as specified in the trial court's order."). The only issue was whether Petitioner had to enter or supply his passcode so that the State could effectuate its lawful warrant.

The majority concluded that Petitioner could be required to enter or supply a passcode without running afoul of the Fifth Amendment. The court explained

that its decision followed from the holding of *Fisher v. United States*, 425 U.S. 391 (1976), which determined that an individual could be required to make a production in response to a document subpoena for tax documents. According to *Fisher*, while the act of answering a document subpoena had "communicative aspects," the act of production was of "minimal testimonial significance." *Id.,* at 412. In particular, *Fisher* reasoned that because "the Government is in no way relying on the 'truth-telling' of the taxpayer to prove the existence of or his access to the documents" by requiring compliance with the subpoena, "the existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers." *Id.*, at 411. Thus, "no constitutional rights are touched," and "[t]he question is not of testimony but of surrender." *Id.* (citation omitted).

The New Jersey Supreme Court concluded that the same was true here: while it held that entering or supplying a passcode constitutes "a testimonial act of production," the court held that the "foregone conclusion" doctrine applied to this kind of act of production. Pet. 34a. After all, the court found, just as the conclusion that was "foregone" in *Fisher* was the testimonial act of producing a response to the subpoena rather than the actual documents produced, so too the only "compelled act of production in this case [is] that of producing the passcodes." Pet. 33a; see also Pet. 32a (noting that under "the Supreme Court case law that gave rise to the exception . . . the foregone conclusion test applies to the production of the passcodes themselves"). And based on *Fisher*, there would be no constitutional

barrier "if the passcodes' existence, possession, and authentication are foregone conclusions." Pet. 34a.

That analysis was satisfied in this case with "little difficulty." *Id.* As the majority found, "[t]he State established that the passcodes exist—they determined the cellphones' contents are passcode-protected. Also, the trial court record reveals that the cellphones were in [Petitioner's] possession when seized and that he owned and operated the cellphones, establishing his knowledge of the passcodes and that the passcodes enable access to the cellphones' contents." *Id.* Moreover, "to the extent that authentication is an issue in this context, the passcodes self-authenticate by providing access to the cellphones' contents." *Id.*[1] The record-based "demonstration of the passcodes' existence, [Petitioner's] previous possession and operation of the cellphones, and the passcodes' self-authenticating nature render the issue here one of surrender, not testimony." Pet. 34a-35a. Under *Fisher*, the Fifth Amendment presented no bar.

Finally, the majority added, "[a]lthough we reach that decision by focusing on the passcodes, we note that, in this case, we would reach the same conclusion if we viewed the analysis to encompass the phones' contents." Pet. 35a. "The search warrants and record evidence of the particular content that the State knew the phones contained provide ample support for that

[1] The court below noted that the parties did not raise authentication as an issue. See Pet. App. 8a, n.3.

determination." *Id.* (citing *United States v. Apple Mac-Pro Computer*, 851 F.3d 238, 248 (CA3 2017); *Seo v. State*, 148 N.E.3d 952, 958 (Ind. 2020)).[2]

Three justices dissented, reasoning that the foregone conclusion doctrine did not apply. Pet. 40a-75a. This petition for certiorari followed.

REASONS FOR DENYING THE PETITION

Just as this Court denied certiorari in *Pennsylvania v. Davis* six months ago, the same result is proper here—and nothing in this petition justifies a different course. Most importantly, the interlocutory nature of this petition means there is no state court final judgment for the Court's review. While the state court decided the Fifth Amendment issue, actions yet to unfold at the trial court may obviate the Court's need to review that issue in this case—depriving this Court of jurisdiction and making the petition at the very least a poor candidate for certiorari. Further, this case does not squarely present either split Petitioner identifies. This Court should allow these Fifth Amendment questions to percolate—and if it sees fit, address the issues in a case that better presents them. And in any event, the court below correctly resolved the questions before it by faithfully applying the foregone conclusion doctrine this Court discussed in *Fisher*.

---

[2] The Court also concluded that although New Jersey's common law privilege "offers broader protection than its federal counterpart under the Fifth Amendment," it does not protect Petitioner because any privacy considerations "have already been . . . overcome through the unchallenged search warrants granted in this case." Pet. 39a-40a. The majority thus held that "neither federal nor state protections against compelled disclosure shield [Petitioner's] passcodes." Pet. 40a.

I. This Case Is A Poor Vehicle Because The Court Lacks Jurisdiction.

This Court's jurisdiction to review state-court decisions is limited to "[f]inal judgments or decrees rendered by the highest court of a State in which a decision could be had." 28 U.S.C. § 1257(a). But this petition arrives on an interlocutory posture. And it does not fit into the "four categories of . . . cases in which the Court has treated" a state interlocutory decision on a federal issue "as a final judgment . . . without awaiting the completion of the additional proceedings anticipated in the lower state courts." *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469, 477 (1975).

In the context of a state prosecution, "[t]he general rule is that finality . . . is defined by a judgment of conviction and the imposition of a sentence." *Fort Wayne Books, Inc. v. Indiana*, 489 U.S. 46, 54 (1989). Here, neither has occurred, and Petitioner has therefore not met his burden to file a petition that "demonstrate[s] to this Court that it has jurisdiction to review the judgment." *Johnson v. California*, 541 U.S. 428, 431 (2004) (per curiam). Indeed, the lack of finality of judgment is apparent from the proceedings that have yet to take place. For one, Petitioner has yet to comply with the trial court's order and might claim that, given the passage of time, Petitioner no longer remembers his passcode; such a claim would have to be adjudicated based on a fact-intensive inquiry by a trial court. For another, it is not certain whether the phones contain evidence that materially adds to the case against Petitioner, or only includes evidence the State already has. And finally, there remains the possibility that the

jury might acquit Petitioner of all charges, even after the State presents evidence against him.

None of the exceptions under *Cox Broadcasting*—which governs the review of state court judgments—apply. First, this is not a case "where for one reason or another the federal issue is conclusive or the outcome of further proceedings preordained." 420 U.S., at 479. Each of the events described above are independent ways in which the Fifth Amendment issues presented would not determine the outcome of Petitioner's case. If Petitioner can no longer remember his passcode, if there is no relevant additional evidence on the phones, or if he is acquitted, the "outcome of further proceedings" is anything but "preordained" by a ruling on the issue presented. *Id.* Moreover, this Court has only applied this exception to criminal trials in the extreme situation where a defendant "concede[d]" that he committed the conduct of which he was accused and that he "ha[d] no defense" in the trial court other than the federal constitutional claim. *Mills v. Alabama*, 384 U.S. 214, 217 (1966). Petitioner has made no analogous concession in this case.

The second and third exceptions are inapplicable for similar reasons. This case is not one in which "the federal issue, finally decided by the highest court in the State, will survive and require decision regardless of the outcome of future state-court proceedings." *Cox*, 420 U.S., at 480. If any of the above-mentioned scenarios occur, there will be no need for further review of the Fifth Amendment issue. Nor is it one "in which later review of the federal issue cannot be had, whatever the ultimate outcome of the case." *Id.*, at 481. Even if Petitioner is convicted, he can "once more seek

review of his [Fifth Amendment] claim in the Supreme Court of [New Jersey]—albeit unsuccessfully—and then seek certiorari on that claim from this Court." *Johnson*, 541 U.S., at 431.

Finally, Petitioner's claim also fails to satisfy the fourth *Cox* exception, which involves matters "where reversal of the state court on the federal issue would be preclusive of any further litigation on the relevant cause of action rather than merely controlling the nature and character of, or determining the admissibility of evidence in, the state proceedings still to come." *Cox*, 420 U.S., at 482-83. As discussed above, reversal of the judgment below would not be "preclusive of any further litigation": the trial has yet to take place, and proceedings there could obviate the federal issue entirely. *Id.* A decision on the Fifth Amendment question might not even impact "the admissibility of evidence in[] the state proceedings still to come," as the phones may not contain relevant or admissible evidence. And because those criteria are not met, "a refusal immediately to review the state court decision" could not "seriously erode federal policy," *id.*, at 483, since the outcome of the instant case ultimately may not turn on the question presented at all. In short, Petitioner can "make no convincing claim of erosion of federal policy that is not common to all decisions rejecting a defendant's [Fifth Amendment] claim." *Johnson*, 541 U.S. at 430. And a "contrary conclusion would permit the fourth exception to swallow the rule. Any federal issue finally decided on an interlocutory appeal in the state courts would qualify for immediate review." *Flynt v. Ohio*, 451 U.S. 619, 622 (1981).

At the very least, the interlocutory posture of this case presents vehicle problems that counsel strongly against review. As laid out above, a number of issues have yet to be aired in future state court proceedings. Some are the very same considerations at play when this Court denied the most recent petition implicating compelled decryption. See Br. in Opp. at 10, *Pennsylvania v. Davis*, No. 19-1254 (July 28, 2020) (explaining that *Davis* was "an inappropriate vehicle" to address Fifth Amendment questions because the "record is unclear" as to whether that defendant "even remembered the password in question"); *id.*, at 10-11 (adding certiorari is unwarranted "because this case arises on an interlocutory appeal," such that "there is no basis to say whether the evidence the Commonwealth seeks is actually important to secure a conviction"). Because many of the same vehicle problems exist here as were present in *Davis*, the same result should follow.

And this case contains vehicle problems that go beyond the ones in *Davis*. As explained *infra* at 15-17, Petitioner's position is that there is a conflict among the lower courts as to whether a suspect can be required to verbally disclose the passcode to an encrypted device; but Petitioner does not believe a split exists as to entering that password directly into such a device. See Pet. 17. The petition argues, in particular, that verbal disclosure is especially troubling—and the court below erred in holding otherwise—because "the government would . . . learn *the contents of the password itself*, and plainly the government does not possess that information at all." Pet. 29 n.15. But none of that would be true if Petitioner directly enters his passcode in subsequent proceedings, as the State confirmed below would be entirely acceptable. See *infra*

at 17. Moreover, none of Petitioner's analysis accounts for the State's promise of use immunity, which at the very least would deprive the State of using any information learned regarding "the contents of the password itself." See generally *Fisher,* 425 U.S., at 400; *United States v. Doe*, 465 U.S. 605, 617 n.17 (1984). So not only is the case interlocutory, but further proceedings may meaningfully change—and at least inform—the constitutional issues before this Court.

This Court has often declined to review cases that arrive in an interlocutory posture. This petition confirms the wisdom of that approach.

II. This Case Does Not Implicate The Circuit Splits Petitioner Alleges.

Petitioner alleges two splits regarding the extent and application of the Fifth Amendment: whether the foregone conclusion doctrine can require disclosure of an encrypted device's passcode, and if so, whether the lodestar of that analysis turns on the device's passcode or its contents. But the instant case, especially on the current interlocutory posture, does not implicate either split. This Court can and should wait for a vehicle that better presents the Fifth Amendment issues before deciding whether to address them.

1. Petitioner alleges a split as to whether the foregone conclusion doctrine can ever allow a State to "demand that Petitioner provide *pure testimony*" by "communicat[ing] his memorized passcodes to the prosecutor." Pet. 1. Because Petitioner errs in portraying this case as a dispute about "pure testimony," he also errs in claiming the split will be implicated here.

Petitioner relies almost entirely on the Pennsylvania Supreme Court's decision in *Commonwealth v. Davis*, 220 A.3d 534 (2019). As Petitioner rightly recounts, *Davis* examined a defendant's challenge to a court order compelling him to "divulge the passcode" to his computer, which was seized in the course of a child pornography investigation. *Id.*, at 539. The question in that case was whether the defendant could be compelled to verbally communicate his passcode. *Id.*, at 540. The Pennsylvania Supreme Court held that the "revealing of a computer password is a verbal communication," and declined to apply the foregone conclusion doctrine to its disclosure on that basis. *Id.*, at 548. That is the heart of Petitioner's claim of a split—that "on indistinguishable facts," Pennsylvania prosecutors cannot "compel[] oral statements" of someone's encrypted device passcode, but the prosecutors in this case can and will do so. Pet. 10.

Petitioner acknowledges, however, that there is no split as to whether a defendant can be required to actually *enter* the passcode into his encrypted device directly—without divulging the passcode to the prosecution. See Pet. 17 (noting a distinct line of cases, separate from *Davis*, "involve orders compelling a suspect to enter a passcode directly into a device, rather than communicate it directly to the state or the court"). Petitioner is right to do so: the Court in *Davis* specifically stated that whether defendants can be required to input a passcode (without divulging it) into their device was "not at issue in th[at] appeal." 220 A.3d, at 541. The respondent in *Davis* made the same point in successfully opposing certiorari—that there is no conflict between *Davis*'s prohibition on verbal disclosures and

decisions affirming orders requiring individuals to enter passcodes. See Br. in Opp. at 4, *Pennsylvania v.* Davis, No. 19-1254 (July 28, 2020) (noting those cases "all involve the distinct legal and factual situation of a demand to produce decrypted versions of encrypted documents or to 'unlock' a device by typing in the password, without disclosing the password to the government"). And the respondent in *Davis* explicitly argued that there was no lower court conflict on that separate question of entry. *Id.*[3]

But the distinction Petitioner himself is drawing—between verbal disclosure (with a split) and direct entry (splitless)—undermines his case for certiorari. Because this petition is on an interlocutory posture, Petitioner has not had to comply with any court order. Petitioner insists that he will have to "honestly communicate, from his internal thoughts, his memorized

[3] An example of cases involving entry is *Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 613 (Mass. 2014), in which the Massachusetts Supreme Judicial Court applied the foregone conclusion doctrine to an order that defendant unlock his device. Digital forensic examiners discovered file names on a defendant's computer that implicated him in fraud, but those files were passcode-protected and inaccessible. *Id.* The court concluded that any facts conveyed by a defendant through his act of decryption, namely "his ownership and control of the computers and their contents, knowledge of the fact of encryption, and knowledge of the encryption key," were already "known to the government, and thus, are a 'foregone conclusion.'" *Id.*, at 615. As a result, that court concluded, the Fifth Amendment was no obstacle to an order requiring the defendant to input the applicable passcode. *Id.* Petitioner suggests that the Indiana Supreme Court "*would* line up" against *Gelfgatt* and the decision below on issues concerning entry, but Petitioner's language is appropriately conditional, as it relies on dicta rather than a holding by that court. Pet. 9 (emphasis added) (citing *Seo*, 148 N.E.3d, at 957-58).

passcodes" through "pure testimony." Pet. 7. The record, however, establishes the opposite—that the State will permit Petitioner to enter his passcode without sharing it with anyone. At argument below, the State stressed this manner of compliance, noting:

- "We don't want to know the pass[codes]. We just want defendant to enter them."
- "We are not going to know the pass[code]."
- "We're not asking the defendant to reveal his passcode . . . What we're allowing the defendant to do here is enter the passcode himself . . . [The defendant] doesn't have to say it out loud."
- "[The government will] never hear [the iPhone passcode] from the defendant [and will] never have it written down."
- "[Defendant will be] entering the passcode, not revealing it."[4]

Because the State is seeking only Petitioner's action in unlocking his devices, this interlocutory case will *not* present the disagreement as to whether he can be required to verbally disclose that passcode.

To be sure, the decision below did allow the State to pursue either means of compliance—finding constitutional an order that Petitioner divulge his encrypted device's passcode or an order that he enter it. See Pet. 31a (concluding that "[c]ommunicating or entering a passcode" are "testimonial acts of production"); Pet. 17

[4] The recordings of the argument before the New Jersey Supreme Court can be found at https://tinyurl.com/vzssfkb2. The State's representations above can be found at 0:01:04-08, 0:08:33-35, 0:33:30-38, 0:34:46-49, and 0:39:15-18, respectively.

("The court below treated these two scenarios as indistinguishable."). And the court did expressly disagree with the holding in *Davis* as to verbal disclosures of passcodes. Pet. 24a-27a, 33a. But this Court sits to resolve concrete controversies where the facts implicate them—not abstract disagreements that will not affect the result in a specific case. Because the record makes clear Petitioner can comply by entering his passcode, this is not the appropriate posture for addressing the first split as Petitioner himself frames it.

2. Petitioner alleges a second split as to whether, if the foregone conclusion doctrine applies, the government must prove it is a foregone conclusion that a defendant knows the device's passcode or its contents. That dispute is likewise not implicated here.

The basic contours of the dispute are clear. As the New Jersey Supreme Court recognized, if the foregone conclusion doctrine applies, a court must still decide what "conclusion" must be "foregone." Under one perspective, the question is "whether the Government already knows the testimony that is implicit in the act of production"—*i.e.*, it is already aware the defendant "know[s] the password for these devices." Pet. 30a (citation omitted). Another camp believes the inquiry must focus instead on "what the police already knew would be found on those devices"—*i.e.*, that the foregone conclusion analysis focuses on knowledge of the device's contents, not its passcode. *Id.*

Petitioner's second split relies on this dichotomy. In the decision below, Petitioner rightly explains, the court found the proper "focus[]" was "the passcodes." Pet. 35a. That is, the court held the State satisfied its

burden under the Fifth Amendment's foregone conclusion doctrine by showing that Petitioner unquestionably possessed the encrypted devices at issue and knew their passcodes—so that the State gained no information of testimonial value by seeing him input it or by having him share it. Pet. 34a. Petitioner emphasizes that two courts reached a different conclusion—that the foregone conclusion doctrine relates to a device's contents, not its passcode. See *Seo*, 148 N.E.3d, at 958 (finding that the government must show that it knew "(1) Seo knows the passcode for her iPhone; (2) the files on the device exist; and (3) she possessed those files"); *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335, 1346 (CA11 2012) ("*Mar. 25 Subpoena*") (describing as the relevant question if the "Government knows whether any files exist and are located on the hard drives").[5]

The problem for Petitioner, however, is that the New Jersey Supreme Court explicitly found this dispute was not outcome-determinative in this case. Put

---

[5] Petitioner also suggests a split between the New Jersey Supreme Court and Third Circuit, but that is incorrect. *Apple MacPro* did not decide the proper application of the forgone conclusion exception. That court was constrained to a plain-error analysis, and held the district court had not committed plain error in determining that the government met the elements forgone conclusion doctrine as applied to the contents of the device. 851 F.3d, at 245-47. But the panel did not hold the focus had to be on contents, and instead acknowledged "a very sound argument can be made that the 'foregone conclusion' doctrine properly focuses on whether the Government already knows the testimony that is implicit in the act of production"—namely, whether a suspect's "knowledge of the password itself is sufficient to support application of the foregone conclusion doctrine." *Id.*, at 248 n.7.

another way, although Petitioner emphasizes the importance of resolving whether the foregone conclusion doctrine should focus upon the passcode or the files on an encrypted device, he overlooks that the court below held the State met its burden either way—even relying on the cases Petitioner says form the other side of the split. See Pet. 35a ("Although we reach that decision by focusing on the passcodes, we note that, in this case, we would reach the same conclusion if we viewed the analysis to encompass the phones' contents.") (citing *Apple MacPro*, 851 F.3d, at 248 & n.7; *Seo*, 148 N.E.3d, at 958). Because the majority concluded that "the result is the same" in this particular case regardless of "whether the inquiry is limited here to the passcodes or extended to the phones' contents," Pet. 40a, resolution of the second split Petitioner alleges will not change the result in his case.

A comparison of the facts in this case to the facts in *Seo* and *Mar. 25 Subpoena* easily justify the different results in those cases and in this one. In *Mar. 25 Subpoena*, the court determined that the doctrine applied to the contents of the computer, and that the government had not met the threshold of the doctrine because "[n]othing in the record before us reveals that the Government knows whether any files exist and are located on the hard drives; what's more, nothing in the record illustrates that the Government knows with reasonable particularity that [the defendant] is even capable of accessing the encrypted portions of the drives." 670 F.3d, at 1346. And in *Seo*, the court likewise held "the State has failed to demonstrate that any particular files on the device exist or that [the suspect] possessed those files," relying in part on a detec-

tive's confirmation "that he would be fishing for 'incriminating evidence' from the device." 148 N.E.3d, at 958; see *id.*, at 960 (expressing concerns about "unbridled access to potential evidence" on the phone).

As the New Jersey Supreme Court found, the record in this case is markedly different. As the majority laid out, "the search warrants and record evidence of the particular content that the State knew the phones contained provide ample support" for its request even relative to the phones' contents. Pet. 35a. Among other things, a co-conspirator testified before the grand jury about the content on Petitioner's phones; content recovered from that co-conspirator's phone corroborates his testimony; and records from Petitioner's phones' service provider show frequent contact between Petitioner and his co-conspirator during the timeframe the co-conspirator claims. See Pet. 35a (noting, unlike in *Seo*, "this was no fishing expedition"). Of course, Petitioner disagrees with the conclusion below that he would still lose under that alternative standard. But there is no reason for this Court to address such a fact-bound question—which is why Petitioner does not include it as a question presented here. Instead, there is every reason to decline to adjudicate which standard applies in a case where it will not change the lower court's ultimate conclusion.

That renders this entire petition unworthy of certiorari. After all, the two issues are related—which is why Petitioner frames them under a single question. Indeed, as Petitioner notes, if this Court "rules against Petitioner on the first issue"—that is, finds the foregone conclusion doctrine applies—"it will then need to resolve what the government must show to satisfy the

exception in this setting." Pet. 16. Otherwise, uncertainty will persist in the lower courts. Because this presents a poor vehicle for addressing the second split (for all the reasons given above), it logically is a poor vehicle for taking up the entire case.

3. There is also no reason for this Court to take up these issues in a case that fails to effectively present them. After all, a relatively limited number of courts have addressed the Fifth Amendment issues to date—four state supreme courts and the Eleventh Circuit.[6] As this Court has recognized, it receives great benefit "from permitting several courts of appeals [and/or several state supreme courts] to explore a difficult question before this Court grants certiorari." *United States v. Mendoza*, 464 U.S. 154, 160 (1984). That is particularly true when the petition does not squarely implicate the conflicts, and where other courts are poised to resolve these questions. With the landscape no different than when this Court declined to hear *Davis* this term, further percolation remains warranted.

III. The Decision Below Was Correct.

The New Jersey Supreme Court correctly rejected Petitioner's Fifth Amendment claim. Its decision follows from precedents and first principles alike.

---

[6] The Oregon Supreme Court decided the issue on state constitutional grounds. See *State v. Pittman*, 479 P.3d 1028, 1043, 1051 (Or. 2021) (holding the State had not met the "narrow circumstances" under which it could compel a defendant to unlock his phone under Oregon's constitution). And as noted above, *supra* 19 n.5, the Third Circuit did not resolve the issues raised.

1. Begin with this Court's cases. As this Court has held, the "foregone conclusion" doctrine exempts a testimonial act of production from Fifth Amendment protection if the facts communicated by the act of production itself are already known to the government, such that the individual "adds little or nothing to the sum total of the Government's information." *Fisher*, 425 U.S., at 411. For the doctrine to apply, the government must establish its knowledge of (1) the existence of the evidence demanded; (2) the possession or control of that evidence by the defendant; and (3) the authenticity of the evidence. See *id.*, at 410-13.

Critically, each time that the Court has applied the foregone conclusion doctrine, it has evaluated the testimony inherent in the act of producing documents itself, not the contents of the documents ultimately provided. See *id.*, at 409-10 (contrasting the nontestimonial nature of the taxpayer's documents with the testimonial significance of producing the documents); see also *United States v. Hubbell*, 530 U.S. 27, 40 (2000) (holding that "[t]he 'compelled testimony' that is relevant in this case is not to be found in the contents of the documents produced . . . [i]t is, rather, the testimony inherent in the act of producing those documents"); Pet. 32a (explaining this Court's precedents "explicitly predicate the applicability of the foregone conclusion doctrine on the fundamental distinction between the act of production and the documents to be produced"); Orin S. Kerr, *Compelled Decryption And The Privilege Against Self-Incrimination*, 97 Tex. L. Rev. 767, 776-78 (2019) (emphasizing this distinction in this Court's case law).

The New Jersey Supreme Court applied that rule here. The court determined that the compelled decryption ordered by the trial court was "a testimonial act of production," like providing documents in response to a subpoena is a testimonial act of production. Pet. 31a; see *Hubbell*, 530 U.S., at 45. The majority also rightly held it "problematic to meld the production of passcodes with the act of producing the content of the phones"—reiterating that, "[f]or purposes of the Fifth Amendment privilege against self-incrimination, the act of production must be considered in its own right, separate from the documents sought." Pet. 21a, 31a. When an individual enters the passcode to her phone, to the extent that act is testimonial at all, she confirms only that she knows the passcode; the separate question of whether the government can access the files contained therein is a matter for the Fourth Amendment. Pet. 32a-33a; see also Kerr, *Compelled Decryption*, 97 Tex. L. Rev., at 779 ("'I know the password' is the only assertion implicit in unlocking the device.").[7] In short, based on this Court's "current doctrine," the "Fifth Amendment poses no barrier to compelled decryption [of an encrypted device] as long as the government has independent knowledge that the suspect

[7] This conclusion is the only reasonable one, in part because Petitioner has "non-inculpatory explanations" for being able to access the device such as, "although I have access to it, that device ... [or] its contents are not mine." *In re Search of [Redacted]*, 317 F. Supp. 3d, at 535 n.9. Petitioner could know the passcodes because the phones belong to a significant other, family member, or close friend. Kerr, *Compelled Decryption*, 97 Tex. L. Rev., at 779. Ultimately, the State must show not only that Petitioner had possession and control over the devices, but that he had possession and control over the devices at the time any incriminating texts or calls were sent from them.

knows the password and the government presents the password prompt to decrypt the device to the suspect." Kerr, *Compelled Decryption*, 97 Tex. L. Rev., at 769.

In addition to correctly holding that the government's burden is to show Petitioner's knowledge of the passcode is a foregone conclusion, the court below correctly held the State met that burden here. First, the State established knowledge of the passcodes' existence because "the cellphones' contents are passcode-protected" and cannot otherwise be accessed. Pet. 34a. Second, "the trial court record reveals that the cellphones were in [Petitioner]'s possession when seized and that he owned and operated the cellphones, establishing his knowledge of the passcodes and that the passcodes enable access to the cellphones' contents." *Id.* Finally, even assuming "authentication is an issue in this context, the passcodes self-authenticate by providing access to the cellphones' contents." *Id.* The court had "little difficulty concluding that compelled production of the passcodes falls within the foregone conclusion exception." *Id.*

Contrary to Petitioner's proposal, Pet. 26-29, there is simply no basis to distinguish the application of this Court's decisions by cabining them to business records or to non-digital evidence. Such limitations make no doctrinal or logical sense. After all, the Fifth Amendment's foregone conclusion doctrine applies to testimonial acts of production, which does not turn on the business or non-digital nature of the documents being provided. Said another way, that documents are business documents, or are in digital instead of hard-copy form, is irrelevant to whether a particular act of production itself "adds little or nothing to the sum total

of the Government's information." *Fisher*, 425 U.S., at 411. In fact, the distinctions Petitioner would have the Court draw are irrelevant to *testimonial implications* entirely—the heart of the Fifth Amendment analysis. See, e.g., *United States v. Spencer*, No. 17-259, 2018 WL 1964588, at *2 (N.D. Cal. 2018) (explaining that "whether turning over material, either in the form of documents or bits, implicates the Fifth Amendment should not turn on the manner in which the defendant stores the material").

And cabining *Fisher* in the way that Petitioner proposes risks reverberations that go beyond this case—as lower courts have relied on this doctrine in different contexts that do not implicate business records. See, e.g., *United States v. Stone*, 976 F.2d 909, 911 (CA4 1992) (concluding that while a defendant's utility bills were "documents [that] are personal, they are unprotected by the privilege against self-incrimination because their existence, possession, and authentication are a 'foregone conclusion'"); *Barrett v. Acevedo*, 169 F.3d 1155, 1168 (CA8 1999) (requiring production of journal that defendant had already admitted owning and authoring); *In re Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992*, 1 F.3d 87, 93 (CA2 1993) (allowing government to compel production of appointment book calendar, reasoning that the Government already had a photocopy of the calendar, although it suspected portions were whited out before being copied). These examples demonstrate that the doctrine can logically and faithfully be applied to non-business record cases—and undermine any basis for cabining *Fisher* to its facts.

Petitioner also urges this Court to overrule *Fisher* and its progeny. But "[o]verruling precedent is never a small matter. Stare decisis . . . is 'a foundation stone of the rule of law.'" *Kimble v. Marvel Ent., LLC*, 576 U.S. 446, 455 (2015). Undoing forty years of doctrine will disturb the "preferred course [that] promotes the evenhanded, predictable, and consistent development of legal principles, fosters reliance on judicial decisions, and contributes to the actual and perceived integrity of the judicial process." *Id.* (citing *Payne v. Tennessee*, 501 U.S. 808, 827-28 (1991)).

2. First principles are in accord. While Petitioner makes much of the import of developments in technology, Pet. 18-22, the court below properly recognized that his argument puts the form of compelled decryption over the constitutionally relevant substance. Just as a suspect can be compelled to give an accurate voice or handwriting sample, see *Gilbert v. California*, 388 U.S. 263, 266 (1967); subject himself to a blood sample drawing, see *Schmerber v. California*, 384 U.S. 757, 764-65 (1966); or sign a document executing a bank authorization to disclose records to the government, see *Doe v. United States*, 487 U.S. 201, 215 (1988), suspects can be required to provide biometric data like a fingerprint or a face scan. See Pet. 33a. But "holding passcodes exempt from production whereas biometric device locks may be subject to compulsion creates inconsistent approaches based on form rather than substance." Pet. 33a.; see *State v. Diamond*, 905 N.W.2d 870, 871-72 (Minn.), cert. denied, 138 S. Ct. 2003 (2018); *In re Search of [Redacted]*, 317 F. Supp. 3d 523, 533 (D.D.C. 2018); *Spencer*, 2018 WL 1964588, at *2. Allowing one but not the other would not be consistent with the purposes underlying the Fifth Amendment,

because both actions accomplish the same relevant result (unlocking a phone) and communicate the exact same information to the government (that the defendant has the ability to unlock the phone).

Doing so would also allow an individual wishing to conceal evidence of a crime to purposefully erect a "non-substantive barrier" out of information that is "of no testimonial interest to the government" in order to prevent law enforcement from "execut[ing] otherwise lawful searches" that comply with the Fourth Amendment. Kerr, *Compelled Decryption*, 97 Tex. L. Rev., at 767. Simply put, individuals seeking to evade a lawful search warrant can intentionally (and quickly and easily) disable biometric accessibility in order to render a device's contents unavailable to law enforcement. See Joseph Keller, *How to Quickly Disable FaceID and TouchID on iPhone and iPad*, iMore (May 30, 2020), https://tinyurl.com/u7s363dt.

Petitioner himself has attempted to shape such a "non-substantive barrier" out of his passcode, leaning on the private nature of cell phones to shield his device from law enforcement access. This approach inappropriately "imports Fourth Amendment privacy principles into a Fifth Amendment inquiry." Pet. 32a. In short, the Fifth Amendment prohibits "compelled self-incrimination," but "*not* (the disclosure of) private information" writ large. *Fisher*, 425 U.S., at 401 (emphasis added). Reading the Fifth Amendment as a "general protector of privacy" for the underlying documents law enforcement wishes to search would "completely loose [it] from the moorings of its language." *Id.* Instead, privacy for the materials on the phone is

"addressed in the Fourth Amendment," which appropriately limits law enforcement access to them. *Id.* But here, there is no Fourth Amendment issue; Petitioner has never "challenge[d] the search warrants issued for his phone." Pet. 12a. Because the instant passcode itself is (all agree) "of no testimonial interest to the government," the Fifth Amendment does not bar a search the Fourth Amendment allows.

Far from implicating grave privacy concerns, then, this case turns solely on the Fifth Amendment privilege against self-incrimination. Ultimately, the act of unlocking Petitioner's phones itself adds nothing to the government's knowledge against him. Compelling Petitioner to unlock his device is thus consistent with the Fifth Amendment, and it does nothing more than allow the government to effectuate a search warrant it validly obtained.

CONCLUSION

This Court should deny the petition.

Respectfully submitted,

Gurbir S. Grewal
Attorney General of New Jersey
Jeremy M. Feigenbaum*
State Solicitor
Angela Cai
Deputy State Solicitor
Lila B. Leonard
Deputy Attorney General

Office of the Attorney General of New Jersey

Theodore N. Stephens, II
Acting Essex County Prosecutor
Frank J. Ducoat
Director, Appellate Section
Caroline C. Galda
Assistant Prosecutor

Office of the Essex County Prosecutor

April 2, 2021