


No. 19-1254

---

---

IN THE  
*Supreme Court of the United States*

---



PENNSYLVANIA,

*Petitioner,*

—v.—

JOSEPH J. DAVIS,

*Respondent.*

---

ON PETITION FOR WRIT OF CERTIORARI TO  
THE SUPREME COURT OF PENNSYLVANIA

---

**BRIEF IN OPPOSITION**

---

David D. Cole  
AMERICAN CIVIL LIBERTIES  
UNION FOUNDATION  
915 5th Street, NW  
Washington, D.C. 20005

Jennifer S. Granick  
AMERICAN CIVIL LIBERTIES  
UNION FOUNDATION  
39 Drumm Street  
San Francisco, CA 94114

Peter Goldberger  
*Counsel of Record*  
50 Rittenhouse Place  
Ardmore, PA 19003  
peter.goldberger@verizon.net  
(610) 649-8200

Brett Max Kaufman  
Jenessa Calvo-Friedman  
AMERICAN CIVIL LIBERTIES  
UNION FOUNDATION  
125 Broad Street, 18th Floor  
New York, NY 10004

*Counsel for Respondent*

---

---

**QUESTION PRESENTED**

After formally charging respondent Joseph Davis with state criminal offenses, the prosecutor obtained an order requiring respondent to tell police the password to his personal computer, on which the petitioner Commonwealth believed he had stored contraband electronic image files. Respondent refused to disclose his password, invoking his state and federal constitutional rights against self-incrimination. The Supreme Court of Pennsylvania held that the Fifth Amendment privilege protects respondent from being compelled to reveal a memorized password where doing so would assist the prosecution in amassing evidence to be used against him in a criminal trial. The Question Presented is:

Does the Self-Incrimination Clause of the Fifth Amendment protect a criminal defendant from being compelled to reveal his computer password to the government where the testimony could itself be incriminating or could lead to the discovery of incriminating evidence to be used against him in his criminal case?

**TABLE OF CONTENTS**

	PAGE
QUESTION PRESENTED .....	i
TABLE OF AUTHORITIES .....	iv
INTRODUCTION .....	vi
STATEMENT OF THE CASE.....	2
REASONS FOR DENYING THE PETITION .....	4
I.    THE PENNSYLVANIA SUPREME COURT’S DECISION DOES NOT CONFLICT WITH DECISIONS OF OTHER STATE SUPREME COURTS OR FEDERAL COURTS OF APPEALS.....	4
A.  The Petitioner Fails to Distinguish Between Compelled Testimony as to the Contents of a Password and an Order to Produce Encrypted Documents or to Unlock an Encrypted Device.....	5
B.  The Federal Circuit Court and State Supreme Court Cases that Have Considered the Fifth Amendment and Computer Passwords Have Done So Only in the Context of Orders to Physically Decrypt Documents or Devices, Not Orders to Verbally Reveal One’s Password.....	7

	PAGE
II. THIS CASE IS AN INAPPROPRIATE VEHICLE TO ADDRESS QUESTIONS REGARDING COURT ORDERS DEMANDING THE PRODUCTION OF ENCRYPTED DOCUMENTS OR THE UNLOCKING OF ENCRYPTED DEVICES. ....	10
III. THE DECISION BELOW IS CORRECT. ....	11
CONCLUSION .....	15

## TABLE OF AUTHORITIES

PAGE(S)

### Cases

<i>Booker v. S.C. Dep’t of Corr.</i> , 855 F.3d 533 (4th Cir. 2017) .....	9
<i>Boyle v. Smithman</i> , 23 A.397 (Pa. 1892) .....	11
<i>Carpenter v. United States</i> , 138 S.Ct. 2206 (2018) .....	14, 15
<i>Commonwealth v. Gelfgatt</i> , 11 N.E.3d 605 (Mass. 2014) .....	9
<i>Commonwealth v. Molina</i> , 104 A.3d 430 (Pa. 2014) .....	11
<i>Curcio v. United States</i> , 354 U.S. 118 (1957) .....	12
<i>Doe v. United States</i> , 487 U.S. 201 (1988) .....	3, 11, 12
<i>Fisher v. United States</i> , 425 U.S. 391 (1976) .....	6
<i>Galbreath’s Lessee v. Eichelberger</i> , 3 Yeates 515 (Pa. 1803).....	11
<i>In re Grand Jury Subpoena Duces Tecum</i> <i>Dated Mar. 25, 2011</i> , 670 F.3d 1335 (11th Cir. 2012) .....	8
<i>Ohio v. Reiner</i> , 532 U.S. 17 (2001) (per curiam).....	5
<i>Pennsylvania v. Muniz</i> , 496 U.S. 582 (1990) .....	3, 6, 12

	PAGE(S)
<i>Seo v. State</i> , No. 18S-CR-595, 2020 WL 3425272 (Ind. June 23, 2020) .....	9
<i>United States v. Apple MacPro Computer</i> , 851 F.3d 238 (3d Cir. 2017) .....	8, 9
<i>United States v. Doe</i> , 465 U.S. 605 (1984) .....	7
<i>United States v. Gavegnano</i> , 305 F. App'x 954 (4th Cir. 2009) (per curiam) .....	9
<i>United States v. Hubbell</i> , 530 U.S. 27 (2000) .....	3, 7, 12
<i>United States v. Warrant</i> , 2019 WL 4047615 (N.D. Cal. Aug. 26, 2019) .....	13
 <b>Constitutions and Statutes</b>	
U.S. Const. amend. V .....	passim
Pa. Const., art. I, § 9 .....	2, 11
18 Pa. Cons. Stat. § 6312(c) .....	2
18 Pa. Cons. Stat. § 7512(a) .....	2
 <b>Other Authorities</b>	
<i>Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy</i> , S. Judiciary Comm. (2015) (Statement of Peter Swire, Huang Professor of Law and Ethics at Ga. Inst. of Tech. Scheller C. of Bus.), available at <a href="https://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Swire%20Testimony.pdf">https://www.judiciary.senate.gov/imo/media/ doc/07-08-15%20Swire%20Testimony.pdf</a> .....	14

U.S. Req. for Review at 12, *In the Matter of the  
Search of a Residence in Oakland,  
California*, 354 F. Supp. 3d 1010  
(N.D. Cal. 2019) (No. 4:19-MJ-70053-KAW),  
ECF. No. 2 ..... 14

## INTRODUCTION

The Pennsylvania Supreme Court held that when the State seeks to compel an individual to disclose to it his password, and the password could lead to incriminating evidence, the Fifth Amendment privilege against self-incrimination applies. That unremarkable decision is consistent with a long line of cases holding that the Fifth Amendment prohibits the government from compelling a person to answer a question whose answer could be incriminating.

Pennsylvania contends that this decision conflicts with opinions of two courts of appeals and two state supreme courts, but it does not. Those cases did not involve a demand that an individual disclose his password to the government through direct testimony. Rather, they involved legally and factually distinct situations in which the government either seeks to compel an individual to produce decrypted versions of encrypted documents, or orders an individual to decrypt a device by typing in his password, *without disclosing the password to the government*. Because these situations do not involve the direct verbal communication of privileged information to the government, but acts that may have inherent or implied testimonial features, they pose distinct legal questions. And with the exception of a single sentence in an unpublished and nonprecedential Fourth Circuit opinion, no federal circuit court or state supreme court has even *addressed* the question the Pennsylvania Supreme Court resolved here, much less reached a different result.

It has long been accepted that compelling an individual to provide a verbal response to an incriminating question triggers the Fifth



Amendment's protection. This case involves nothing more than that. The Court should deny certiorari.

### STATEMENT OF THE CASE

Joseph Davis was arrested on October 20, 2015 and charged with two counts of disseminating child pornography in violation of 18 Pa. Cons. Stat. § 6312(c), and two counts of criminal use of a communication facility in violation of 18 Pa. Cons. Stat. § 7512(a). Pet. App. 1d–2d. The charges stem from two incidents in which investigators with the Pennsylvania Office of the Attorney General identified an illicit video shared on a peer-to-peer Internet platform called “eDonkey2000/eMule.” Pet. App. 2c–3c n.1.

At the time of his arrest, investigators seized a computer from Mr. Davis' residence, but later discovered that all of the data on the computer was encrypted and could therefore not be searched without a password. Pet. App. 2d–3d. On December 17, 2015, after he had been formally charged, the Commonwealth of Pennsylvania filed a “Motion to Compel Defendant to Provide Password for Encryption Enabled Device.” Pet. App. 5a, 1d. Mr. Davis invoked his Fifth Amendment privilege against compelled self-incrimination, as well as the similar privilege protected by Pennsylvania's Declaration of Rights, Pa. Const., art. I, § 9. Pet. App. 8d.

On June 30, 2016, the trial court issued an opinion and order directing Mr. Davis to provide the password, despite his invocation of the Fifth Amendment privilege. Pet. App. 15d. The trial court acknowledged that the password was testimonial, but concluded that “the Commonwealth has prior knowledge of the existence as well as the whereabouts of the

documents,” and thus “Defendant’s act of production loses its testimonial character because the information is a ‘foregone conclusion.’” Pet. App. 14d. Mr. Davis took a timely interlocutory (collateral order) appeal, as authorized by state law. Pet. App. 7a n.3.

On November 30, 2017, a panel of the Pennsylvania Superior Court affirmed the trial court’s order. Pet. App. 1c. That court concluded that the “act of providing the password in question is not testimonial in nature and [Mr. Davis] Fifth Amendment right against self-incrimination would not be violated.” Pet. App. 18c–19c.

In a November 20, 2019 opinion, the Pennsylvania Supreme Court reversed. It held that the Fifth Amendment prohibited compelling Mr. Davis to disclose a passcode that would enable investigators to access encrypted data on the seized computer. Pet. App. 1a. The court reasoned that the compelled disclosure of Mr. Davis’s password was testimonial because, “[d]istilled to its essence, the revealing of a computer password is a verbal communication, not merely a physical act.” *Id.* at 24a. Invoking an analogy relied on by this Court, it concluded that “under United States Supreme Court precedent, we find that the Commonwealth is seeking the electronic equivalent to a combination to a wall safe — the passcode to unlock Appellant’s computer.” *Id.* Because the government was compelling a direct testimonial answer to a question, the court held that the “foregone conclusion exception” was inapplicable, as this Court has applied it only in “act of production” cases. Pet. App. 27a–28a (citing *Doe v. United States*, 487 U.S. 201, 210 (1988) (“*Doe II*”); *United States v. Hubbell*, 530 U.S. 27, 44 (2000); *Pennsylvania v. Muniz*, 496 U.S. 582, 588–89 (1990)). The court added in the alternative that even if the “foregone conclusion

exception” could in theory be applied to the compulsion of pure testimony, the Commonwealth failed to establish that the answer or the evidence it might lead to were “foregone conclusions” here. Pet. App. 31a–32a n.9.

Pennsylvania filed this petition for a writ of certiorari.

## **REASONS FOR DENYING THE PETITION**

### **I. THE PENNSYLVANIA SUPREME COURT’S DECISION DOES NOT CONFLICT WITH DECISIONS OF OTHER STATE SUPREME COURTS OR FEDERAL COURTS OF APPEALS.**

The decision below does not conflict with any other precedential decision of the federal courts of appeals or state supreme courts. The only decisions from such courts that even address the Fifth Amendment implications of computer passwords 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. Those cases present questions of what constitutes testimony, what constitutes an act of production, and whether and how the “foregone conclusion” inquiry should apply.

This case, by contrast, involves the straightforward issue of whether the Fifth Amendment precludes an individual from being compelled to answer a question by providing a direct verbal answer that could be incriminating. A verbal response is by definition testimonial, and the Court has never applied the “foregone conclusion” rationale to direct testimony. There is simply no split of authority on that question.

Because these two categories of password cases pose distinct legal questions, there is no conflict.

**A. The Petitioner Fails to Distinguish  
Between Compelled Testimony as to the  
Contents of a Password and an Order to  
Produce Encrypted Documents or to  
Unlock an Encrypted Device.**

The Commonwealth’s assertion of a conflict rests on its conflation of two different types of cases involving computer passwords and encryption, each of which gives rise to different constitutional issues: those involving demands for *pure testimony* in the form of the disclosure of the password, and those involving *physical acts* that may have inherent or implied testimonial aspects, and that have generally been viewed as “acts of production.”

This case falls squarely into the first category. It involves a government demand that an individual directly answer a question by revealing the contents of his mind—his password—to the government. Where a court order demands an oral or written answer, the application of the Fifth Amendment privilege is straightforward: it applies if the answer could be incriminating or could lead to incriminating evidence. See *Ohio v. Reiner*, 532 U.S. 17 (2001) (per curiam).

Here, the trial court directed Mr. Davis to “supply the Commonwealth with any and all passwords used to access” a specific desktop computer and hard drive seized from his residence. Pet. App. 15d. To comply, Mr. Davis would have to directly communicate to the Commonwealth the contents of his password. As the court below observed, “[d]istilled to its essence, the revealing of a computer password is a verbal communication, not merely a physical act that would be nontestimonial in nature.” Pet. App. 24a.

The Fifth Amendment bars the state from requiring an individual to provide a potentially self-incriminating response, no matter how trivial in content or how confident the state may be that it already knows the information in question. *Muniz*, 496 U.S. at 597. Since complying with the order would require Mr. Davis to make a verbal statement and choose between telling the truth or telling a lie, it is testimonial. *Id.* This effort to *compel disclosure* of a passcode is a straightforward demand for pure testimony.

All of the federal circuit court and state supreme court cases the Commonwealth cites to support its asserted conflict with the decision below involve a second and distinct category: demands to produce encrypted documents in decrypted form, or to unlock an encrypted device so that the government can access documents stored on the device. In those cases, the government does not ask the individual to directly communicate the contents of his password to the government; rather, it asks the individual to take physical action using that password, without revealing the password to any state actor.

The federal courts of appeals and state supreme courts have generally analyzed these disputes as involving “acts of production.” The “act of production” doctrine provides that, even if documents themselves are not covered by the Fifth Amendment (because their creation was not compelled), the act of surrendering them may have implicit testimonial aspects, inasmuch as it communicates the existence, possession, and authenticity of the documents. *Fisher v. United States*, 425 U.S. 391, 410 (1976). Where the testimonial aspects of an act of production were already known to the government, or a “foregone conclusion,” the privilege did not apply. *Id.* at 413.

Where, by contrast, the testimonial aspects of an act of production are not known to the government, the privilege applies. *United States v. Doe*, 465 U.S. 605, 608, 612–14 (1984) (“*Doe I*”) (where producing subpoenaed documents would admit their existence and authenticity, Fifth Amendment privilege applies); *Hubbell*, 530 U.S. at 44–45 (finding government failed to show “foregone conclusion”).

The decision below correctly identified this case as falling squarely within the first category, presenting a straightforward question concerning the government’s ability to compel a verbal response to a specific question. This case *does not* present the distinct question whether the government may compel a suspect to *use* a passcode to assist the government, without disclosing it. The Commonwealth’s effort to conjure a conflict rests on its failure to recognize this crucial distinction.

**B. The Federal Circuit Court and State Supreme Court Cases that Have Considered the Fifth Amendment and Computer Passwords Have Done So Only in the Context of Orders to Physically Decrypt Documents or Devices, Not Orders to Verbally Reveal One’s Password.**

Only two federal circuits and two other state supreme courts have addressed the Fifth Amendment’s application to compelled decryption. All four of those cases involved orders to generate and then turn over decrypted files or to unlock a device by entering a password, without disclosing the password to the government. Because none of those cases involved compelling an individual to answer an incriminating question directly, they do not even

address the question decided below, much less conflict with its resolution.

The Commonwealth points to two federal court of appeals decisions. Pet. 18–20. *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335 (11th Cir. 2012) (“*Grand Jury Subpoena*”); *United States v. Apple MacPro Computer*, 851 F.3d 238 (3d Cir. 2017) (“*Apple MacPro*”). Both involve compelled decryption of documents or a device, without requiring the disclosure of a password to the government.

In *Grand Jury Subpoena*, the government subpoenaed a suspect to produce the unencrypted contents of encrypted hard drives. Applying the “act of production” doctrine, the Eleventh Circuit held that producing the documents was testimonial. 670 F.3d at 1346. It then concluded that the testimonial aspects of the act of decryption were not a “foregone conclusion,” and upheld the defendant’s invocation of the Fifth Amendment privilege. 670 F.3d 1335.

In *Apple MacPro*, the Third Circuit upheld a magistrate order requiring the defendant to produce his seized electronic devices in a fully unencrypted state. 851 F.3d at 246. The court deemed the issue waived because the defendant did not file objections or appeal and had thereby failed to preserve the issue for court of appeals review. The court went on in dicta to note that—under the deferential “plain error” standard of review—it would have held that the district court did not err in concluding that any testimonial aspects of the act of production were a “foregone conclusion,” because the factual record already established the witness’s possession, access, and ownership of the devices, as well as the fact that

the hard drives contained illegal child abuse imagery. *Id.*<sup>1</sup>

Two state supreme courts other than Pennsylvania’s have addressed the Fifth Amendment in the context of passwords, but both addressed compelled decryption, not demands to provide a direct and potentially incriminating verbal answer to a question. In *Commonwealth v. Gelfatt*, 11 N.E.3d 605 (Mass. 2014), the state sought to compel the defendant to enter his password into encrypted devices under circumstances where the investigators would “not view or record the password or key in any way.” *Id.* at 611 n.10. The court held that entering an encryption key implicitly acknowledged ownership and control of the computers and their contents, but held that those facts were a “foregone conclusion” under the circumstances. *Id.* at 614–15.

Similarly, *Seo v. State*, No. 18S-CR-595, 2020 WL 3425272 (Ind. June 23, 2020), involved an order that the defendant unlock her iPhone without disclosing her password to the government. The court held that entering the password, like an “act of production,” had testimonial aspects, and found that the state had not shown that what it revealed was a “foregone conclusion.”

Thus, in the only four cases in which either a federal circuit court or a state court of last resort has ruled on

---

<sup>1</sup> The Commonwealth also cites *United States v. Gavegnano*, 305 F. App’x 954 (4th Cir. 2009) (per curiam), but that decision, which devoted only a single sentence to the issue, is unpublished and nonprecedential. Pet. 19; see *Booker v. S.C. Dep’t of Corr.*, 855 F.3d 533, 543 (4th Cir. 2017) (“[U]npublished opinions ‘are not even regarded as binding precedent in our circuit...’”). By definition, a nonprecedential decision cannot create a conflict among the circuits.



a Fifth Amendment objection to an order involving a computer password, the orders at issue compelled the physical disclosure of decrypted documents or the unlocking of a device without revealing a passcode, and not the *disclosure of the password itself through communication by the suspect*. Because these decisions do not address the compelled communication of a password to the government, they do not conflict with the decision below.

**II. THIS CASE IS AN INAPPROPRIATE VEHICLE TO ADDRESS QUESTIONS REGARDING COURT ORDERS DEMANDING THE PRODUCTION OF ENCRYPTED DOCUMENTS OR THE UNLOCKING OF ENCRYPTED DEVICES.**

Because this case involves a demand to provide a direct, incriminating answer to a government question, it would be an exceedingly poor vehicle to decide the distinct questions posed by cases where the government demands that a suspect decrypt documents by entering a password, without disclosing it to the government.

As detailed above, the only other cases that have yet reached resolution by federal courts of appeals or state courts of last resort raise distinct legal questions, not presented here. And as those cases illustrate, this Court will have plenty of opportunity to address those questions in a case that actually presents them.

This case presents an inappropriate vehicle for several other reasons as well. The record is unclear on whether Mr. Davis, as of the hearing on the Commonwealth's motion, even remembered the password in question. And because this case arises on an interlocutory appeal, there is no basis to say

whether the evidence the Commonwealth seeks is actually important to secure a conviction.

Finally, even if reversed, Mr. Davis might prevail under the State Constitution. The court below granted review on that question as well but chose not to reach it. Article I of the State Constitution encompasses the full common law evidentiary rule of “*nemo tenetur prodere seipsum*” (no one is obligated to accuse himself). See *Galbreath’s Lessee v. Eichelberger*, 3 Yeates 515, 517 (Pa. 1803). Since the state provision looks to “giv[ing] evidence” rather than being a witness, it is not necessarily limited to what is testimonial. See Pa. Const., art. I, § 9; *Boyle v. Smithman*, 23 A. 397 (Pa. 1892)). The state supreme court “has specifically concluded that the protections of Section 9 exceed those in its federal counterpart.” *Commonwealth v. Molina*, 104 A.3d 430, 444 (Pa. 2014).

For these reasons as well, the petition should be denied.

### III. THE DECISION BELOW IS CORRECT.

The decision below is plainly correct. As this Court has recognized, “be[ing] compelled to reveal the combination to [petitioner’s] wall safe” necessarily communicates the contents of one’s mind directly to the state. *Doe II*, 487 U.S. at 210 n.9 (alteration in original). It is therefore testimonial. *Id.* The court below correctly recognized and applied this straightforward principle to the demand for a secret password involved here.

Where, as here, the government compels an individual to provide an answer to a question that could be self-incriminating, the privilege applies. “Whenever a suspect is asked for a response requiring

him to communicate an express or implied assertion of fact or belief, the suspect confronts the ‘trilemma’ of truth, falsity, or silence, and hence the response (whether based on truth or falsity) contains a testimonial component.” *Muniz*, 496 U.S. at 597 (footnote omitted). It does not matter how incidental or seemingly trivial is the question at issue, or whether the State believes it already knows the answer or could readily obtain it from other sources. *Id.* (Fifth Amendment privilege protects arrested person from being compelled to provide his birthdate). Outside of the voice exemplar setting, verbal statements are virtually always testimonial. *Id.* Moreover, “compelled testimony that communicates information that may lead to incriminating evidence is privileged even if the information itself is not inculpatory.” *Hubbell*, 530 U.S. at 38 (quoting *Doe II*, 487 U.S. at 208 n.6 (quotation marks omitted)). “It is the ‘extortion of information from the accused,’ the attempt to force him ‘to disclose the contents of his own mind,’ that implicates the Self-Incrimination Clause.” *Doe II*, 487 U.S. at 211 (citations omitted).

Here, Mr. Davis was ordered to provide a direct answer to the question, “What is your password?” Because his response would be testimonial, compelled, and potentially self-incriminating, the court below properly held that the answer was protected by the Fifth Amendment. The Pennsylvania Supreme Court’s conclusion that the order in this case demanded testimony is uncontroversial. As this Court held long ago, the state cannot compel a suspect to recall and share information that exists only in her mind to aid the state in its prosecution. *See Curcio v. United States*, 354 U.S. 118, 128 (1957).

The court below also correctly held that the “foregone conclusion” rationale does not apply to

demands for pure testimony. Were it otherwise, as the court explained, the exception would swallow the rule. Pet. App. 31a–32a n.9. Even if the government has overwhelming evidence that an individual is guilty of a burglary, for example, it cannot compel him to answer the question, “Did you enter that house?” by asserting that the answer is a “foregone conclusion,” because, for example, the defendant was arrested inside. The “foregone conclusion” rationale has been applied only in the context of the incidental communicative aspects of acts of production of unprivileged business documents, where the individual is not required to answer any questions with direct testimony. As the court below stated, “it would be a significant expansion of the foregone conclusion rationale to apply it to a defendant’s compelled oral or written testimony.” Pet. App. 26a–27a. The court therefore correctly held that the “foregone conclusion” inquiry is inapplicable here.<sup>2</sup>

The United States has acknowledged “a consensus has emerged that a suspect may not be compelled to divulge his or her password to law enforcement, as that would require disclosure of the contents of the suspect’s own mind.” *United States v. Warrant*, 2019 WL 4047615, at \*2 (N.D. Cal. Aug. 26, 2019) (citing U.S. Req. for Review at 12, *In the Matter of the Search of a Residence in Oakland, California*, 354 F. Supp. 3d

---

<sup>2</sup> In any event, the court below correctly held that, even if the “foregone conclusion” inquiry were applicable to a compelled answer to a question, the government did not satisfy its burden here. As the court below found, the Commonwealth failed to establish that it already knew of either the contents of the password, or the existence, possession, and authenticity of what it expected would be found on the seized computer. Pet. App. 31a–32a n.9. That fact-bound conclusion does not merit this Court’s review.

1010 (N.D. Cal. 2019) (No. 4:19-MJ-70053-KAW), ECF. No. 2).

Unlike the United States, *Amici Curiae* State Attorneys General assert that law enforcement has (or ought to have) the power to force people to answer questions revealing their passwords. It is true that encryption may impose obstacles to law enforcement in particular cases, as the States note. But that is not a reason to strip classic incriminating testimony of its longstanding constitutional protection. Constitutional protections sometimes interfere with law enforcement investigations. *Carpenter v. United States*, 138 S.Ct. 2206, 2214 (2018) (“[A] central aim of the Framers was ‘to place obstacles in the way of a too permeating police surveillance.’” (citation omitted)).

And while there may be some respects in which law enforcement has lost capabilities due to changing encryption technology, those losses “are more than offset by massive gains including: (1) location information; (2) information about contacts and confederates; and (3) an array of new databases that create digital dossiers about individuals’ lives.” *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy*, S. Judiciary Comm. (2015) (Statement of Peter Swire, Huang Professor of Law and Ethics at Ga. Inst. of Tech. Scheller C. of Bus.), available at <https://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Swire%20Testimony.pdf>.<sup>3</sup> Technology has been a boon to law

---

<sup>3</sup> Professor Swire served in 2013 as one of five members of the President’s Review Group on Intelligence and Communications Technology. He was co-chair in 2012–2013 of the global Do Not Track process for the World Wide Web Consortium. From 1999–2001, Swire was Chief Counselor for Privacy in the U.S. Office of Management and Budget.

enforcement, producing records of individuals' movements and associations that enable police to conduct previously impossible investigations. *See, e.g., Carpenter*, 138 S.Ct. at 2208 (cell-site location information used to catalog defendant's past movements for more than 127 days). The State *amici*'s hyperbolic assertion that the Pennsylvania court's decision will "drastically alter the balance of power between investigators and criminals" ignores these critical facts. Br. Amici Curiae of Utah, et al. at 5.

### CONCLUSION

The petition for certiorari should be denied.

Respectfully submitted,

Peter Goldberger  
*Counsel of Record*  
50 Rittenhouse Place  
Ardmore, PA 19003  
peter.goldberger@verizon.net  
610-649-8200

David D. Cole  
AMERICAN CIVIL LIBERTIES  
UNION FOUNDATION  
915 5th Street, NW  
Washington, D.C. 20005

Brett Max Kaufman  
Jenessa Calvo-Friedman  
AMERICAN CIVIL LIBERTIES  
UNION FOUNDATION  
125 Broad Street, 18th Floor  
New York, NY 10004

16

Jennifer S. Granick  
AMERICAN CIVIL LIBERTIES  
UNION FOUNDATION  
39 Drumm Street  
San Francisco, CA 94114

July 28, 2020