No. 23-5827

IN THE

Supreme Court of the United States

KEIRON K. SNEED,

Petitioner,

v.

ILLINOIS,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE SUPREME COURT OF ILLINOIS

BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PETITIONER

ANDREW CROCKER
Counsel of Record
ELIZABETH FEMIA
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
andrew@eff.org

Attorneys for Amicus Curiae

324842

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

TABLE OF CONTENTS

Table of Contents

TABLE OF CITED AUTHORITIES

Page

CASES

Cited Authorities

Page

Cited Authorities

Page

Page

Page

STATUTES

OTHER AUTHORITIES

STATEMENT OF IDENTITY AND INTEREST OF AMICUS CURIAE[1]

The Electronic Frontier Foundation ("EFF") is a member-supported, nonprofit civil liberties organization that works to protect free speech and privacy in the digital world. Founded in 1990, EFF has over 39,000 active donors and dues-paying members across the United States. EFF has appeared before this Court and other state and federal courts in numerous cases addressing the Fifth Amendment right against self-incrimination and the compelled decryption of digital devices. *State v. Andrews*, 234 A.3d 1254 (N.J. 2020) (amicus), cert. denied, 141 S. Ct. 2623 (2021) (co-counsel); *Eunjoo Seo v. State*, 148 N.E.3d 952 (Ind. 2020) (amicus); *State v. Pittman*, 367 Or. 498 (2021) (amicus); *State v. Valdez*, No. 20210175-SC (Utah oral argument held Mar. 8, 2023) (amicus); *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012) (amicus).

SUMMARY OF ARGUMENT

The order at issue in this case would require Petitioner Keiron Sneed to honestly recall and enter his memorized cellphone passcode to aid in his own prosecution. Despite the modern technological context, therefore, the case turns on one of the most fundamental protections in

1. Pursuant to Sup. Ct. R. 37.2, EFF notified the counsel of record for the parties that it intended to file this brief at least 10 days before its filing. No counsel for a party authored this brief in whole or in part, and no such counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than amicus curiae, or its counsel, made a monetary contribution intended to fund its preparation or submission.

our constitutional system: an accused person's ability to exercise his Fifth Amendment rights by refusing to become a witness against himself.

The Supreme Court of Illinois held that the Fifth Amendment privilege against self-incrimination does not shield Mr. Sneed from being compelled to enter his passcode, even though it reveals the very "contents of the mind" that the self-incrimination privilege protects. *See Curcio v. United States*, 354 U.S. 118, 128 (1957). Although compelling entry of the passcode would require Mr. Sneed to provide information unknown to the State to further his own prosecution, the court reasoned that the passcode could be compelled because the existence, possession, and authentication of the passcode itself was a "foregone conclusion." In so holding, the court deepened a split of authority between state supreme courts and federal courts of appeal about whether and how the "foregone conclusion" analysis applies to compelled disclosure or entry of a passcode. Only this Court can resolve this split.

The decision below is inconsistent with a long line of this Court's precedents, all of which prohibit the government from compelling a person to provide information that could be incriminating or lead to the discovery of incriminating evidence. Those precedents recognize no distinction between compelling someone to provide his birthdate, *Pennsylvania v. Muniz*, 496 U.S. 582, 597 (1990), "the combination to a wall safe," *United States v. Hubbell*, 530 U.S. 27, 43 (2000), or the password to his phone or computer. Indeed, this Court has *never* applied the "foregone conclusion" analysis to pure testimony, or even to an "act of production" beyond the specific context in which it was first applied—a subpoena

for preexisting, physical business documents. *Fisher v. United States*, 425 U.S. 391, 411 (1976); *see also Hubbell*, 530 U.S. at 44; *United States v. Doe* ("*Doe I*"), 465 U.S. 605, 614 n.13 (1984). Creating a broad new "foregone conclusion exception" to the privilege against self-incrimination would dramatically undermine bedrock Fifth Amendment protections.

The question is indisputably important. Only three years ago, 22 states urged this Court to grant certiorari to decide this very issue. *See* Br. of *Amici Curiae* States of Utah *et al.* at 1, *Pennsylvania v. Davis*, No. 19-1254 (U.S. May 26, 2020) ("As the top law enforcement officials of their respective jurisdictions, *amici* State Attorneys General have a strong interest in getting clarity on the important Fifth Amendment question here. Its answer could affect almost every criminal case.").

For these reasons, the petition should be granted.

ARGUMENT

I. STATE SUPREME COURTS AND THE FEDERAL COURTS OF APPEALS ARE DIVIDED ON THE SCOPE OF THE FIFTH AMENDMENT'S PROTECTIONS AGAINST COMPELLED DISCLOSURE AND ENTRY OF A PASSCODE.

The Illinois Supreme Court's decision below conflicts with decisions of the federal courts of appeals and state supreme courts in two significant ways.

First, courts are divided on whether the testimony involved in the compelled disclosure or entry of a digital

passcode can ever be subject to a "foregone conclusion" analysis derived from this Court's decision in *Fisher*.

Second, even where courts have conducted a foregone conclusion analysis, they are deeply divided over *how* it applies and, in particular, which facts must be a "foregone conclusion" to overcome the privilege. The court below held that the government must merely be able to demonstrate *the existence of a passcode and ownership of the phone*. Other courts have concluded that the government must demonstrate *knowledge about the contents of the files it seeks that are stored on the device*.

These differing interpretations have resulted in significant jurisdictional discrepancies in Fifth Amendment protections against the compelled disclosure or use of a passcode. Only this Court can resolve this inconsistency.

A. State Supreme Courts Are Divided Over Whether a Foregone Conclusion Analysis Is Applicable to the Compelled Disclosure or Entry of a Passcode.

The Illinois Supreme Court decision below contributes to a significant state supreme court split over whether there is a "foregone conclusion exception" derived from this Court's decision in *Fisher* that can ever apply to the compelled disclosure or entry of a passcode. The split stems from disagreement both about the testimonial nature of compelled disclosure or entry of a passcode and whether the foregone conclusion analysis should apply beyond its original, narrow context.

The order at issue here involves written testimony; it requires Mr. Sneed to truthfully recall and type the passcode to his phone. However, the Illinois Supreme Court held that the Fifth Amendment privilege against self-incrimination does not protect Mr. Sneed from this compulsion, even though it requires him to disclose the contents of his mind and could provide a link in a chain to incriminating evidence. The court held that complying with the order is testimonial, but *only* "to the extent that performing the act implicitly asserts that the person entering it has the ability to unlock the phone." *People v. Sneed*, No. 127968, 2023 WL 4003913, at *12 (Ill. Jun. 15, 2023). Thus, it concluded, the Fifth Amendment applies, but only in regard to the implicit assertions regarding the suspect's ability to unlock the cellphone.

The New Jersey Supreme Court reached a similar holding in *State v. Andrews*, 234 A.3d 1254 (N.J. 2020). In *Andrews*, the order at issue required the defendant to honestly communicate, from his internal thoughts, his memorized cellphone passcodes. *Id.* at 1259. Although the court acknowledged that disclosing a cellphone passcode would be testimonial, it nevertheless deemed it of "minimal testimonial value." *Id.* at 1274. It therefore treated the trial court order as requiring an "act of production," rather than pure testimony.

Both the Illinois and New Jersey Supreme Courts' decisions conflict with the Supreme Court of Pennsylvania's conclusion in *Pennsylvania v. Davis*, 220 A.3d 534 (2019), *cert. denied*, No. 19-1254, 2020 WL 5882240 (U.S. Oct. 5, 2020). On the same facts as those in New Jersey, the Pennsylvania court reached the opposite conclusion. In *Davis*, the court reasoned that because complying with an

order to disclose the defendant's password would require him to reveal the contents of his mind, the compelled disclosure was itself testimonial. *Id.* at 548.

Although the Illinois court's decision below addresses compelled entry of the passcode directly into the phone, and not compelled disclosure of the passcode as in *Davis, see Sneed*, 2023 WL 4003913, at *16, n.7, its analysis of the testimonial requirement applies equally to both. The court provided three reasons as to why entering a passcode is not testimonial in and of itself: (1) the passcode may be entered regardless of the existence of any files on the phone or the person's knowledge of or control over any files on the phone; (2) entering a passcode does not delve into the contents of a person's mind because use of the passcode is so habitual that "its retrieval is a function of muscle memory"; and (3) it would put form over substance to offer greater protection to unlocking a phone with a passcode than to unlocking a phone biometrically, using fingerprint or face recognition. *Id.* at *12-13. But none of these arguments depend on compelled entry as opposed to compelled disclosure of the passcode. Indeed, the *Andrews* Court relied on these same arguments to allow the compelled disclosure. *See Andrews*, 234 A.3d at 1274. The decision below therefore conflicts with the decision in *Davis*.

These courts' disagreement further extends to whether the foregone conclusion analysis from this Court's decision in *Fisher* can ever apply on these facts. In *Fisher*, the Court held that even if the contents of certain tax documents themselves were not covered by the Fifth Amendment (because their creation was not compelled), the act of surrendering them pursuant to subpoena may

have implicit testimonial aspects, as it communicates the existence, possession, and authenticity of the documents, and to that extent may receive Fifth Amendment protection. *Fisher*, 425 U.S. at 410. However, the Court found that under the particular facts of that case, the testimonial aspects of the "act of production" were already known to the government—and were therefore a "foregone conclusion." As a result, the self-incrimination privilege did not bar production of the documents. *Id.* at 413. Since *Fisher*, the Court has never again relied on the "foregone conclusion" to overcome a privilege claim. *See Doe I*, 465 U.S. at 608, 612–14 (where producing subpoenaed documents would admit their existence and authenticity, Fifth Amendment privilege applies); *Hubbell*, 530 U.S. at 44–45 (privilege applies where production would communicate existence and location of documents).

Disregarding this precedent, the Illinois Supreme Court declared that "there is nothing in the history of the foregone conclusion doctrine to suggest that it does not apply to acts of producing passcodes to cell phones." *Sneed*, 2023 WL 4003913, at *15. It argued instead that any time a "compelled act of production is deemed testimonial . . . a foregone conclusion analysis is necessary." *Id.* at *14. *See also Andrews*, 243 A.3d at 1270–71, 1273–75 (applying foregone conclusion to compelled disclosure of passcode).

On the other hand, the Pennsylvania Supreme Court in *Davis* reasoned that the foregone conclusion rationale "constitutes an extremely limited exception to the Fifth Amendment privilege against self-incrimination," applicable only to subpoenas for business records. *Davis*, 220 A.3d at 548. The court noted that "to apply the foregone conclusion rationale in these circumstances

would allow the exception to swallow the constitutional privilege." *Id.* at 549.

Similarly, the Indiana Supreme Court has indicated that it would line up with Pennsylvania and against Illinois and New Jersey. In *Seo v. State*, a case involving compelled entry of a passcode to unlock a smartphone, the court held that even if a "foregone conclusion exception" were applicable, the State had failed to meet the necessary showing. 148 N.E.3d 952, 957–58 (Ind. 2020). But it also recognized that "[e]xtending the foregone conclusion exception to the compelled production of an unlocked smartphone" would be error because "such an expansion (1) fails to account for the unique ubiquity and capacity of smartphones; (2) may prove unworkable; and (3) runs counter to U.S. Supreme Court precedent." *Id.* at 959.

Accordingly, there is a direct split between the state supreme courts of Illinois and New Jersey on one side, and Pennsylvania on the other, over whether the "foregone conclusion" exception applies at all to orders to disclose a passcode, with the Supreme Court of Indiana strongly siding with Pennsylvania. Only this Court can resolve this split.

B. Federal Courts of Appeals and State Supreme Courts Are Divided Over How to Apply a Foregone Conclusion Analysis to the Compelled Disclosure or Entry of a Passcode.

The decision below also implicates a second, closely related split: how to apply the foregone conclusion analysis, if it applies at all in this context. Some courts, like the Illinois Supreme Court here, have held that it is sufficient

for the government to demonstrate merely that it knows that the *passcode itself* exists and that the suspect knows it. *Sneed*, 2023 WL 4003913, at *12. *See also Andrews*, 234 A.3d at 1269; *Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 614 (Mass. 2014); *State v. Stahl*, 206 So. 3d 124, 135–36 (Fla. Dist. Ct. App. 2016). Others, however, have concluded that the government must demonstrate that it knows of the existence, possession, and authenticity of the *files on the encrypted device*. *See, e.g.*, *United States v. Doe* (*In re Grand Jury Subpoena Duces Tecum dated March 25, 2011*), 670 F.3d 1335, 1346 (11th Cir. 2012); *United States v. Apple MacPro Computer* ("*Apple MacPro*"), 851 F.3d 238 (3d Cir. 2017); *Seo*, 148 N.E.3d at 957; *G.A.Q.L. v. State*, 2018 WL 5291918 (Fla. Dist. Ct. App., Oct. 24, 2018); *Pollard v. State*, 2019 WL 2528776 (Fla. Dist. Ct. App. June 20, 2019).

For example, the Supreme Judicial Court of Massachusetts sided with the Illinois Supreme Court and concluded that, in the context of compelled entry of a computer passcode, the government's knowledge concerning "the actual files and documents that are located on the defendant's computers" was irrelevant to a "foregone conclusion" analysis. *Gelfgatt*, 11 N.E.3d at 522 n.13. *See Commonwealth v. Jones*, 117 N.E.3d 702, 710 (Mass. 2019) (discussing its holding in *Gelfgatt*) ("[T]he only fact conveyed by compelling a defendant to enter the password to an encrypted electronic device is that the defendant knows the password, and can therefore access the device.").

By contrast, the Eleventh and Third Circuits, and the Indiana Supreme Court concluded that, if the "foregone conclusion" exception applies, it must be directed to the

files on the device sought to be examined, not merely to the existence and ownership of the password itself. In *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335, the government subpoenaed a suspect to produce the unencrypted contents of encrypted hard drives. The court held that the "foregone conclusion" exception could apply to the compelled decryption of files, but that the government had not made the requisite showing because "[n]othing in the record before us reveals that the Government knows whether any files exist and are located on the hard drives." *Id.* at 1346–47 (*Fisher* and *Hubbell* "require that the Government show its knowledge that the files exist.").

In *Apple MacPro*, the Third Circuit upheld an order requiring the defendant to produce his seized electronic devices in a fully unencrypted state. 851 F.3d at 238, 246. The court reasoned that the testimonial aspects of the act of production were a "foregone conclusion," because "the Government has provided evidence to show both that [contraband] files exist on the encrypted portions of the devices and that Doe can access them . . . ." *Id.* at 248.

Similarly, in *Seo*, the Indiana Supreme Court held that—if the "foregone conclusion" exception applied to compelled entry of passcodes—it applied to the files sought and not simply to the passcodes. 148 N.E.3d at 957–58. The court explained that "*Fisher*, *Doe I*, and *Hubbell* establish that the act of producing documents implicitly communicates that the documents can be physically produced, exist, are in the suspect's possession, and are authentic," and "further confirm[] that the foregone conclusion exception must consider these broad communicative aspects." *Id.* at 957.

The courts, in short, are split both on whether the "foregone conclusion" exception ought to apply, and as to how the exception applies where it does. The decision below presents both aspects of the question, and conflicts with other state supreme courts and federal courts of appeals on both issues.

II. THE DECISION BELOW IS INCORRECT.

The Illinois Supreme Court's decision is incorrect for three reasons.

A. Compelled Entry of a Passcode Is Not an Act of Production.

First, the court below erred in holding that passcode entry is not testimonial on its face, but is merely an "act of production," and therefore testimonial *only* to the extent that there are statements implicit in the act of providing the passcode. *Sneed*, 2023 WL 4003913, at *12. But if—as here—the State orders an individual to use his thoughts and memories to assist in a prosecution against himself, that is a textbook demand for testimony. Application of the Fifth Amendment should thus be straightforward: if the compelled information could be incriminating or could lead to incriminating evidence, the privilege applies, and the "foregone conclusion" exception does not. *See Ohio v. Reiner*, 532 U.S. 17, 21–22 (2001) (per curiam).

The Founders adopted the Fifth Amendment in response to inquisitorial practices in England requiring individuals to testify against themselves. *Couch v. United States*, 409 U.S. 322, 327-28 (1973). The privilege against self-incrimination thus represents an "unwillingness to

subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt." *Murphy v. Waterfront Comm'n*, 378 U.S. 52, 55 (1964). Absent the protection of the Fifth Amendment, the order in this case imposes precisely that "cruel trilemma" on Mr. Sneed by requiring the truthful recollection and use of a passcode.

At the time of the founding, the term "witness" as used in the Fifth Amendment was understood to mean "a person who gives or furnishes evidence." *Hubbell*, 530 U.S. at 50 (Thomas, J., concurring). Here, Mr. Sneed is being compelled, by state court order, to "be a witness" against himself—to furnish his cellphone passcode for the State's use in its prosecution against him.

This Court's decisions have further defined "witness" to encompass only those communications that are "testimonial"—that is, communications that tend "to reveal, directly or indirectly, [one's] knowledge of facts" or those communications that "disclose the contents of [one's] own mind." *Doe v. United States ("Doe II")*, 487 U.S. 201, 211, 213 (1988). Under that definition, compelled entry of a passcode is still clearly testimonial *in and of itself.*

It is clear that forcing a defendant to *tell* the State his passcode would be purely testimonial because it would "compel [him] to make an express verbal or written statement." *State v. Pittman*, 479 P.3d 1028, 1038–39 (2021); *Davis*, 220 A.3d at 543 "[t]he vast majority of verbal statements thus will be testimonial"). The verbal statement would of course include the passcode itself. But it would also communicate defendant's knowledge of the means to open the device, and, impliedly, his control over the phone in addition to its contents.

The defendant would reveal that same information through his mental efforts by truthfully recalling and entering a password into a cellphone. *See Pittman*, 479 P.3d at 1043; *see also G.A.Q.L.*, 257 So. 3d at 1061.[2] Non-verbal acts can be testimonial when they communicate the contents of the mind. *See Schmerber v. California*, 384 U.S. 757, 761 n.5 (1966) ("A nod or headshake is as much a 'testimonial' or 'communicative' act in this sense as are spoken words.").[3] Thus, opening a lock with a memorized passcode is testimonial regardless of whether the state learns the combination. Indeed, in *United States v. Green*, 272 F.3d 748 (5th Cir. 2001), the Fifth Circuit held that there is "no serious question" that asking an arrestee to disclose the locations of and open the combination locks to cases containing firearms demands "testimonial and communicative" acts as to his "knowledge of the presence of firearms in these cases and of the means of opening these cases." *Id.* at 753. *See also In re Grand Jury Subpoena*, 670 F.3d at 1346 ("[T]he decryption … of the hard drives would require the use of the contents of [the accused's] mind and could not be fairly characterized as a physical act that would be nontestimonial in nature.").

Moreover, the Fifth Amendment protects testimony even if its literal content is of no import to the government.

---

2. Indeed, the State's own conduct in this case makes clear that entry of Mr. Sneed's passcode would have testimonial value. Depending on the circumstances, his possession of the passcode for the phone may indicate that the defendant was aware of relevant files, distributed them, or created them—facts that might otherwise require evidence from other sources.

3. This is in contrast to mere physical acts that do not reveal the contents of an individual's mind, such as putting on a shirt. *Holt v. United States*, 218 U.S. 245 (1910).

For example, in *Pennsylvania v. Muniz*, 496 U.S. 582 (1990), this Court held that a motorist suspected of intoxication could not be compelled to answer a question about the date of his own sixth birthday. *Id.* at 598–99. Law enforcement was not interested in the date itself (in fact, they knew it); rather, they sought his response as evidence of mental impairment. *Id.* at 599 & n.13. But the question still demanded a testimonial answer. "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).

The Illinois Supreme Court also mistakenly claimed that recalling and using a passcode may be merely a rote application of a series of numbers "used so habitually that its retrieval is a function of muscle memory rather than an exercise of conscious thought." *Sneed*, 2023 WL 4003913, at *12. But as the facts of *Muniz* demonstrate, rote-ness is not the legal standard. Indeed, much of everyday small talk is rote, such as answers to questions about one's siblings, place of employment, or place of birth. If such statements were the result of state compulsion designed to lead to an incriminating result, they would surely be protected by the Fifth Amendment. Rote communication is no less revealing, and no less testimonial, than communication requiring great mental concentration. From the Fifth Amendment's standpoint, there is no material distinction between a birthdate, a safe combination, and a password. If it would lead to incriminating evidence, the answer is privileged. *Hoffman v. United States*, 341 U.S. 479, 486 (1951) (privilege extends to answers that would "furnish a link in the chain of evidence needed to prosecute").

"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). Here, Mr. Sneed was ordered to enter information responsive to the question, "What is your password?" Because his response would be testimonial, compelled, and potentially self-incriminating, the answer was protected by the Fifth Amendment.

B. The Court Below Erroneously Extended the "Foregone Conclusion" Analysis Beyond Its Limited, Original Context Involving the Compelled Production of Business Records.

Even if the Court were to agree with the court below that compelled testimony like entering a password could be considered an "act of production," the Court should reverse because the "foregone conclusion" exception is limited to the facts in *Fisher* and should not be applied beyond the context of subpoenas for business and financial records. The court below erred in extending the exception, which has no basis in the text or original understanding of the Fifth Amendment, far beyond its narrow confines in this Court's jurisprudence.

This Court has only ever relied on the foregone conclusion analysis to override an individual's assertion of privilege in a single case—*Fisher*—that involved highly unusual circumstances and does not support a general "foregone conclusion" exception to the privilege against self-incrimination.

The dispute in *Fisher* arose out of a tax investigation. The taxpayers' accountants had prepared documents related to tax returns. The accountants then gave the documents that they had created to the taxpayers, who passed them along to the taxpayers' attorneys. The Internal Revenue Service then served administrative summonses on the accountants. Notably, the taxpayers asserting the privilege neither created nor possessed the documents in question. Understandably, relating these idiosyncratic facts occupies much of the Court's analysis. 425 U.S. at 393–96, 413. The Court concluded that in this unusual setting, because the accountants prepared the papers and could independently authenticate them, "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." *Id.* at 411.

In contrast, the order at issue here demands that Mr. Sneed provide from memory the contents of a passcode he created. The prosecution is entirely reliant on him truthfully recalling this passcode and it does not have an independent third party that could also provide or authenticate it. *Fisher* in no way supports application of a "foregone conclusion" exception here.

After *Fisher*, this Court has only considered foregone conclusion arguments in two cases, both of which also involved subpoenas for preexisting business and financial records. *See Hubbell*, 530 U.S. at 44–45; *Doe I*, 465 U.S. at 612–14. That the Court has never considered the foregone conclusion exception outside of cases involving subpoenas for specific, preexisting business and financial records is unsurprising: these types of records constitute a unique category of material that, to varying degrees, has been

subject to compelled production and inspection by the government for over a century. *See, e.g.*, *Braswell v. United States*, 487 U.S. 99, 104 (1988); *Shapiro v. United States*, 335 U.S. 1, 33 (1948).

Lower courts have overwhelmingly applied the exception only in cases concerning the compelled production of specific, preexisting business and financial records. *See, e.g.*, *United States v. Sideman & Bancroft, LLP*, 704 F.3d 1197, 1200 (9th Cir. 2013) (business and tax records); *United States v. Bright*, 596 F.3d 683, 689 (9th Cir. 2010) (credit-card records); *United States v. Gippetti*, 153 F. App'x 865, 868–69 (3d Cir. 2005) (bank and credit-card account records); *United States v. Bell*, 217 F.R.D. 335, 341–42 (M.D. Pa. 2003) ("tax avoidance" materials advertised on defendant business's website); *In re Grand Jury Subpoenas Served Feb 27, 1984*, 599 F. Supp. 1006, 1012 (E.D. Wash. 1984) (business-partnership records).

At the same time, lower courts have generally declined to apply the foregone conclusion exception to cases involving the compelled production of evidence other than business documents, such as guns or drugs, reasoning that responding to such requests would constitute an implicit admission of guilty knowledge. *See, e.g.*, *Green*, 272 F.3d 748,753; *Commonwealth v. Hughes*, 404 N.E.2d 1239, 1244 (Mass. 1980) ("[W]e express doubt whether a defendant may be compelled to deliver the corpus delicti, which may then be introduced by the government at trial, if only it is understood that the facts as to the source of the thing are withheld from the jury."); *State v. Dennis*, 558 P.2d 297, 301 (Wash. 1976) (defendant's act of producing cocaine in response to officer's urgings was testimonial, no foregone conclusion analysis); *Goldsmith v. Superior Court*, 152

Cal. App. 3d 76, 85–87 (1984) (defendant's production of a gun was testimonial, and not a foregone conclusion).

The court below erred, therefore, in unjustifiably expanding the "foregone conclusion" inquiry beyond *Fisher*'s narrow application to preexisting business records.[4]

C. If the "Foregone Conclusion" Analysis Can Apply, the Court Misapplied It Here.

Assuming *arguendo* that the "foregone conclusion" rationale can apply in this context, the court below also erred in what it required the government to demonstrate: It required merely that the government show that it knew Mr. Sneed had a passcode to his phone. It reasoned that this would demonstrate that "the passcode existed" and that Mr. Sneed had "control" of the passcode. It further concluded that no prior authentication of the passcode was necessary, because if the password worked to unlock the phone, it was "self-authenticating." *Sneed*, 2023 WL 4003913, at *16. But the court clearly required far too little to satisfy the Fifth Amendment.

---

4. Alternatively, this Court should consider revisiting *Fisher* and rejecting the unfounded "foregone conclusion doctrine" altogether. The "foregone conclusion" exception is unsupported in the text or original understanding of the Fifth Amendment. For many years the privilege was understood to prohibit not merely compelled testimony, but any compelled evidence that would lead to incrimination. *Boyd v. United States*, 116 U.S. 616, 634–635 (1886). Several justices have called into question the notion that incriminating documents can be compelled, consistent with the Fifth Amendment. *See Hubbell*, 530 U.S. at 50 (Thomas, J., and Scalia, J., concurring); *Carpenter*, 138 S.Ct. at, 2271 (Gorsuch, J., dissenting).

To invoke the "foregone conclusion" exception, the government must show that it would gain nothing from the testimonial aspects of its compulsion. Thus, in *Fisher*, the Court held the "foregone conclusion" exception applied because the government showed that it already knew the entirety of what the act of producing the subpoenaed documents would communicate: their existence and ownership. Accordingly, the government would gain nothing from the testimonial aspects of the act of production. 425 U.S. at 411. By contrast, the government may not compel an act of production that would reveal materials of which the government was previously unaware. *See Hubbell*, 530 U.S. at 45 (no foregone conclusion where government did not have "any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent").

If Mr. Sneed is compelled to enter his password, he will disclose at least that (1) he possesses and controls the phone and all of its files; and (2) the existence of any number of files that may be stored on the phone. To establish that at least some of the testimonial aspects of the disclosure were a "foregone conclusion," therefore, the government would have to show at a minimum that it knows (1) that Petitioner owns and controls the phone and all of its files; and (2) the existence of particular files on the phone. Only such a showing negates the benefits the government receives from Mr. Sneed's compelled testimony, and therefore constitute a "foregone conclusion" as *Fisher* used the term. *See In re Grand Jury Subpoena*, 670 F.3d at 1346 (government must describe with "reasonable particularity the discrete, tangible contents of a device"); *Seo*, 148 N.E.3d at 958 (foregone conclusion analysis did not apply because the state "failed

to demonstrate that any particular files on the device exist or that [defendant] possessed those files"); *cf. Apple MacPro Computer*, 851 F.3d at 248 (foregone-conclusion inquiry satisfied where government had evidence both that contraband files existed on the devices and that defendant could access them).

The court below, however, did not require this showing.[5] At most, the government had reason to suspect that *some* of the contents of the phone included incriminating files or texts. The request is therefore closer to the "fishing expedition" in *Hubbell* than to the request in *Fisher* for discrete documents of which the government already was aware. *Hubbell*, 530 U.S. at 32.

Because this Court has recognized a "foregone conclusion" exception only where the government showed that it would gain "little or nothing" from the testimonial aspects of an act of production, and the court below did not require the government to meet that burden here, the court erred.

III. THE QUESTION PRESENTED IS IMPORTANT AND RECURRING.

The question presented is also indisputably important. Cellphones and other digital devices play an increasingly central part in Americans' private lives, and routinely hold an unprecedented amount of private information about each of us. *See Riley v. California*, 573 U.S. 373, 394, 396 (2014).

5. The State said it was "hoping to find" photographs and other files on Mr. Sneed's phone pertaining to the mobile deposits at issue but conceded that it did not know that any such files actually existed. *Sneed*, 2023 IL 127968, at *2.

Government efforts to discover the contents of encrypted devices are a routine feature of modern-day law enforcement. As the Indiana Supreme Court put it, "[s]martphones are everywhere and contain everything." *Seo*, 148 N.E.3d at 959. Because most phones are protected with a passcode, and they are "the most frequently used and most important digital source for investigation," the issue recurs frequently.[6]

In 2020, 22 states urged this Court to grant certiorari on this issue, stating that its resolution "could affect almost every criminal case." *See* Br. of *Amici Curiae* States of Utah *et al.* at 1, *Pennsylvania v. Davis*, No. 19-1254 (U.S. May 26, 2020). At that time, there was no split on the issue of compelling the direct disclosure of a passcode, and this Court denied review. But the split is now clearly presented, *see* Section I, *supra,* calling for this Court's resolution of what both sides agree is an important question.

Twice in recent terms, the Court has recognized that the widespread adoption of cellphones has brought about a fundamental shift in the amount and type of personal information that is vulnerable to search by law enforcement. *Riley*, 573 U.S. 373; *Carpenter v. United States*, 138 S. Ct. 2206 (2018). Because cellphones can store vast quantities of personal information—managed and compiled by applications designed "for every conceivable hobby or pastime"—they frequently contain the "sum of an individual's private life." *Riley*, 573 U.S. at 394, 396. They record our most intimate communications, thoughts, and interests; what we read, view, and listen to; who we call, text, or email; our whereabouts

6. Logan Koepke, et al., *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* 7, Upturn (Oct. 2020), https://www.upturn.org/static/reports/2020/mass-extraction/files/Upturn%20-%20Mass%20Extraction.pdf (quoting *Cellebrite Annual Industry Trend Survey 2019: Law Enforcement*, at 3).

and travel; and even data about our health and fitness. These devices are "'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." *Carpenter*, 138 S. Ct. at 2220 (quoting *Riley*, 573 U.S. at 385)); *see also Riley*, 573 U.S. at 395 ("Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception.").

Correspondingly, wide-ranging searches of smartphones have become a common feature of law enforcement investigations. Due to their near ubiquity and ever-increasing storage capacity, law enforcement searches of cellphones are not "limited by physical realities" as searches of their pre-digital counterparts are, creating a much greater potential for "intrusion on privacy." *Riley,* 573 U.S. at 393. A recent survey by the non-profit Upturn found that since 2015, law enforcement agencies have performed hundreds of thousands of cellphone "mass extractions," using forensic software tools that create "a full copy of data from a cellphone—all emails, texts, photos, location, app data, and more—which can then be programmatically searched."[7] The report found "widespread adoption" of these forensic techniques by more than 2,000 law agencies in all 50 states and the District of Columbia, which use them as "an all-purpose investigative tool, for an astonishingly broad array of offenses, often without a warrant."[8] In sum, "[e]very

7. Logan Koepke et al., *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* 4, Upturn (Oct. 2020), https://www.upturn.org/static/reports/2020/mass-extraction/files/Upturn%20-%20Mass%20Extraction.pdf.

8. *Id.* at 32, 40.

American is at risk of having their phone forensically searched by law enforcement."[9]

When police encounter a locked phone as part of an investigation, they often have other avenues for obtaining evidence, including forensic extraction tools. However, as in this case, law enforcement will often seek to compel the device's owner to unlock it by disclosing or entering his passcode. Given the thousands of devices searched each year, then, it is inevitable the issues raised by this petition will continue to recur on a near-daily basis.

CONCLUSION

For the reasons stated above, the petition for writ of certiorari should be granted.

Dated: November 16, 2023

Respectfully submitted,

Andrew Crocker
Counsel of Record
Elizabeth Femia
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
andrew@eff.org

Attorneys for Amicus Curiae

9. *Id.* at 32.