No. _____

IN THE

Supreme Court of the United States

ROBERT ANDREWS,

Petitioner,

—v.—

STATE OF NEW JERSEY,

Respondent.

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

PETITION FOR A WRIT OF CERTIORARI

Robert L. Tarver, Jr.
LAW OFFICES OF
ROBERT L. TARVER, JR.
66 South Main Street
Toms River, NJ 08757

Jeanne LoCicero
Alexander Shalom
AMERICAN CIVIL LIBERTIES
UNION OF NEW JERSEY
FOUNDATION
Post Office Box 32159
Newark, NJ 07102

Mark Rumold
Andrew Crocker
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Jennifer S. Granick
Counsel of Record
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94114
(415) 343-0758
jgranick@aclu.org

David D. Cole
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
915 15th Street, NW
Washington, D.C. 20005

Brett Max Kaufman
Jennesa Calvo-Friedman
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street
New York, NY 10004

QUESTION PRESENTED

While investigating Petitioner Robert Andrews for state criminal offenses, the prosecutor obtained a court order requiring Petitioner to disclose his passcodes to two iPhones. Respondent State of New Jersey believes the passcodes will enable it to find evidence that Petitioner committed a crime. Petitioner refused to disclose his passwords, invoking his Fifth Amendment privilege against self-incrimination. The Supreme Court of New Jersey held that the Fifth Amendment privilege does not protect Petitioner from being compelled to communicate his memorized passcodes to the government, ruling that the privilege was overcome because the passcodes' existence, possession, and authentication were "foregone conclusions."

The Question Presented is:

Does the Self-Incrimination Clause of the Fifth Amendment protect an individual from being compelled to recall and truthfully disclose a memorized passcode, where communicating the passcode may lead to the discovery of incriminating evidence to be used against him in a criminal prosecution?

PARTIES TO THE PROCEEDING

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

RELATED PROCEEDINGS

State v. Andrews, Supreme Court of New Jersey, No. A-72-18 (082209). Judgment entered August 10, 2020;

State v. Andrews, Superior Court of New Jersey Appellate Division, No. A-0291-17T4. Judgment entered November 15, 2018;

State v. Andrews, Superior Court of New Jersey Law Division, Criminal Part, County of Essex, Indictment No. 16-06-01781-I. Judgment entered May 22, 2017.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

CONSTITUTION

OTHER AUTHORITIES

OPINION BELOW

The opinion of the Supreme Court of New Jersey is published at 234 A.3d 1254 (N.J. 2020), and is reprinted at App. 1a. The opinion of the Superior Court of New Jersey Appellate Division is published at 197 A.3d 200 (N.J. Super. Ct. App. Div. 2019) and is reprinted at App. 77a. The opinion of the Superior Court of New Jersey, Criminal Division, Essex County is unpublished and is reprinted at App. 99a.

STATEMENT OF JURISDICTION

The decision of the Supreme Court of New Jersey was issued on August 10, 2020. App. 1a. The jurisdiction of this Court is invoked under 28 U.S.C. § 1257(a).

CONSTITUTIONAL PROVISION INVOLVED

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

U.S. Const. Amend. V.

INTRODUCTION

This case involves a demand that Petitioner provide *pure testimony* of a potentially incriminating nature despite his invocation of his Fifth Amendment rights. The order at issue would require Mr. Andrews to communicate his memorized passcodes to the prosecutor. The Supreme Court of New Jersey, in a 4–3 decision, held that the Fifth Amendment privilege against self-incrimination does not shield an individual from being compelled to communicate one's passcodes—the very "contents of [the] mind" that the self-incrimination privilege protects. *Curcio v. United States*, 354 U.S. 118, 128 (1957). The court reasoned

that the passcodes were of "minimal testimonial value," and that they could therefore be compelled because their existence, possession, and authentication were "foregone conclusions."

That decision squarely conflicts with the decision of the Pennsylvania Supreme Court in *Commonwealth v. Davis*, 220 A.3d 534 (Pa. 2019), *cert denied*, No. 19-1254, 2020 WL 5882240 (2020). *Davis* held, on indistinguishable facts, that an individual could *not* be compelled to disclose a passcode. *Id.* at 550.

The *Davis* and *Andrews* courts divided over *whether* the "foregone conclusion" exception can ever apply to an order that an individual disclose his passwords where they would lead to incriminating evidence. On similar facts, the Indiana Supreme Court recently indicated its agreement with *Davis*. *See Seo v. State*, 148 N.E.3d 952, 958 (Ind. 2020). Only this Court can resolve that 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 answer a question whose answer 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, 598–99 (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. As long as the answer might lead to incriminating evidence, it is protected.

This Court has *never* applied the "foregone conclusion" exception 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 (1976); *see also Hubbell*, 530 U.S. at 44 (declining to find "foregone conclusion"); *United States v. Doe* ("*Doe I*"), 465 U.S. 605, 614 n.13 (1984) (government did not meet "foregone conclusion" showing). Extending that reasoning to the compulsion of direct answers would dramatically disturb settled Fifth Amendment protections. The police cannot require a suspect to answer "do you own the murder weapon?" by contending that the answer is a "foregone conclusion"—even if it has unimpeachable evidence that the answer must be "yes." No different rule applies here.

The decision below also implicates a second, interrelated split over *how* the "foregone conclusion" exception should apply to compelled disclosure or entry of a passcode, if it applies at all. Some courts, like the court below, have ruled that the government need only show that the *password* itself exists and that the suspect knows it. Others have ruled that the government must show that it knows of the existence, ownership, possession, and authenticity of the *files* on the locked device that it seeks. Indeed, in the wake of the New Jersey Supreme Court's opinion in this case, one close observer of the issue admitted that he is simply "unable to say what the law is." Orin S. Kerr, *The Law of Compelled Decryption Is a Mess: A Dialogue—Why the Supreme Court Needs to Step In*, Volokh Conspiracy (Aug. 10, 2020), https://reason.com/volokh/2020/08/10/the-law-of compelled-decryption-is-a-mess-a-dialogue. Again, only this Court can resolve this important and increasingly common issue.

The question is indisputably important. Just last year, New Jersey itself, along with 21 other states, urged this Court to grant certiorari to decide this very issue. *See* Br. of *Amici Curiae* States of Utah *et al.* at 1, *Commonwealth of Pennsylvania v. Davis*, No. 19-1254 (U.S. May 26, 2020) (hereinafter "Br. of *Amici Curiae* States of Utah *et al.*") ("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 writ should be granted.

STATEMENT OF THE CASE

During a narcotics investigation in May and June of 2015, the Essex County Prosecutor's Office obtained information that Petitioner Andrews, a law enforcement officer, was allegedly passing confidential information about the investigation to the subject of the investigation. Internal affairs investigators seized two of Petitioner's phones, but Petitioner did not consent to a search nor unlock the phones. New Jersey asserts that it is unable to obtain the data stored on the phones.

In June 2016, an Essex County grand jury returned a six-count indictment charging Petitioner with the crimes of second-degree official misconduct; third-degree hindering of the apprehension or prosecution of another person; and fourth-degree obstruction of the administration of the law or government function.

In January 2017, the State moved for a discovery order compelling Petitioner to disclose the

passcodes to his iPhones. Petitioner opposed the motion, arguing that compelling him to disclose the passcodes would violate his Fifth Amendment right against self-incrimination as well as privileges under New Jersey law. On May 22, 2017, the trial court granted the State's motion for discovery. App. 115a. The trial court held that providing the passcode was "not a testimonial act where the Fifth Amendment or New Jersey . . . law affords protection." App. 111a. It further held that "any testimonial act contained in the act of providing the . . . passcode is a foregone conclusion because the State has established with reasonable particularity that it already knows that (1) the evidence sought exists, (2) the evidence was in the possession of the accused, and (3) the evidence is authentic." *Id.*

The Appellate Division of the Superior Court affirmed. App. 77a. It reasoned that the "act of producing the passcodes has testimonial aspects," but that "by producing the passcodes, [Petitioner] is not implicitly conveying any information the State does not already possess." App. 88a.

On August 10, 2020, in a 4–3 decision, the New Jersey Supreme Court affirmed. The majority acknowledged that being compelled to provide a password, like the combination to a safe, requires the disclosure of "facts contained within the holder's mind," and is therefore "testimonial." App. 31a. But relying on *Fisher*, the court reasoned that because a password consists of a series of characters or numbers, the password itself is of "minimal testimonial value," and therefore "its testimonial value and constitutional protection may be overcome if the passcodes' existence, possession, and authentication are foregone conclusions." App. 34a. The court found that the State

had met that burden because it knew the iPhones belonged to Mr. Andrews. *Id.*[1]

Three justices dissented. They reasoned that the "foregone conclusion" exception should not be extended to demands that an individual disclose a password to the State. The dissent would instead "adhere to the [U.S. Supreme] Court's bright line: the contents of one's mind are not available for use by the government in its effort to prosecute an individual." App. 62a (LaVecchia, J., dissenting). It reasoned that "there is no real difference between forcing one to divulge the mentally stored combination of a safe—the very example that the Supreme Court has used, more than once, as a step too far in ordering a defendant to assist in his or her own prosecution—and forcing one to divulge the passcode to a smartphone." *Id*. at 45a. Therefore, the dissent would have declined to apply the "foregone conclusion" exception, and would have recognized that the Fifth Amendment privilege against compelled self-incrimination applies.

REASONS FOR GRANTING THE WRIT

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

The decision below conflicts with decisions of the federal courts of appeals and state supreme courts in two ways. First, the courts are divided over *whether*

[1] The court also rejected Petitioner's state law claims. App. 34a–40a.

the government can compel pure testimony—the disclosure of a passcode—by contending that some aspects of the information it thereby receives are a "foregone conclusion." In holding that it may, the New Jersey Supreme Court reached precisely the opposite conclusion from that reached by the Supreme Court of Pennsylvania in *Davis,* which held that the "foregone conclusion" exception does not apply to pure testimony.

Second, even where courts have conducted a "foregone conclusion" inquiry—generally in the context of orders to enter a password directly into a digital device—courts are deeply divided over *how* the inquiry 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*.

A. State Supreme Courts Are Divided Over Whether a "Foregone Conclusion" Analysis Applies to the Compelled Disclosure of a Password.

This case involves a demand for *pure testimony*. The order at issue requires Mr. Andrews to honestly communicate, from his internal thoughts, his memorized passcodes. App. 115a (trial court directing Mr. Andrews to provide "discovery of [his] iPhone PINs and passcodes" to the State). The Supreme Court of New Jersey held that the Fifth Amendment privilege against self-incrimination does not protect Mr. Andrews 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 acknowledged that answering the question would be testimonial, but deemed it of "minimal testimonial value." App. 33a. It therefore treated the trial court order as requiring an "act of production," rather than pure testimony, and applied the "foregone conclusion" exception.

On the same facts, the Pennsylvania Supreme Court reached the opposite conclusion. In *Davis*, the court reasoned that because complying with an order to disclose his password would require the defendant to make a verbal statement revealing the contents of his mind, like providing the combination to a wall safe, the compelled disclosure was testimonial. 220 A.3d at 548. But unlike *Andrews*, the Pennsylvania Supreme Court held that the "foregone conclusion" analysis does not apply to a demand that a witness communicate the contents of his mind. *Id.* at 549. The court 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. *Id.* It declined to apply the exception to pure testimony, which would extend it into "areas of compulsion of one's mental processes." *Id.*[2]

The *Andrews* decision was a 4–3 split. The *Davis* court split 4–3 in the other direction. Thus,

[2] In a footnote, the *Davis* court reasoned in the alternative that, if the "foregone conclusion" rationale were to apply, the State would have to show that it knew not merely information related to the passcode itself, but also of the existence, possession, and authenticity of the documents on the computer whose password it sought. 220 A.3d at 551 n.9.

between New Jersey and Pennsylvania, seven state supreme court justices have concluded that the Fifth Amendment allows the government to force an individual to disclose her passwords over a claim of privilege, and seven have concluded that it does not. Yet under these decisions, the privilege applies fully in Pennsylvania, but not across the border in New Jersey.

The Indiana Supreme Court has indicated that it would line up with Pennsylvania and against New Jersey on the question of whether the "foregone conclusion" exception should apply to compelled disclosure or entry of passwords. In *Seo,* a case involving compelled entry of a passcode to unlock a smartphone, the court held that even if the "foregone conclusion" exception were applicable, the State had failed to make the necessary showing. 148 N.E.3d at 957–58. 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 958–59.

The decision below also conflicts with Supreme Court precedent, which has never applied the so-called "foregone conclusion" doctrine to pure testimony. In *Fisher*, this Court held that even if business documents themselves are 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. 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. 27, 44–45 (2000) (privilege applies where production would communicate existence and location of documents).

Relying on *Fisher*, the *Andrews* court extended the "foregone conclusion" rationale to a demand for *pure testimony*. It regarded the passcode as having "minimal testimonial value," and therefore treated recitation of the passcodes as an "act of production" subject to the "foregone conclusion" exception. App. 33a. Deeming that "the passcodes' existence, possession, and authentication are foregone conclusions," it held that the defendant must comply with the order. App. 34a.

In reaching the opposite conclusion on indistinguishable facts, the Pennsylvania Supreme Court in *Davis* explained that this Court has been clear that, outside of voice exemplars, compelled oral statements are testimonial and protected by the privilege, as they require the disclosure of the contents of one's mind and place the individual in the "cruel trilemma" of "telling the truth, lying and perjuring himself, or refusing to answer and facing contempt and jail." 220 A.3d at 547 (*citing Muniz*, 496 U.S. 582, and *Doe v. United States* ("*Doe II*"), 487 U.S.

201 (1988)). The Pennsylvania court refused to extend the "foregone conclusion" rationale beyond "acts of production," to a compulsion of pure testimony.

Accordingly, there is a direct split between the New Jersey and Pennsylvania supreme courts on 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" Inquiry to Demands for the Disclosure or Entry of Passwords.

The decision below also implicates a second, closely related split, as to *how* the "foregone conclusion" exception should apply, if it applies at all. Those courts that have deemed a "foregone conclusion" inquiry appropriate are deeply split on what the government must show to meet the "foregone conclusion" exception. As the court below explained,

> many [courts] have considered whether the exception applies to compelled decryption or to the compelled production of passcodes and passwords, reaching divergent results. Among other causes for that divergence is a dispute over how to adapt the foregone conclusion analysis from the document-production context . . . Some courts to consider the issue have focused on the production of the passcode as a means to access the contents of the device, treating the contents of the devices as the

> functional equivalent of the contents of documents at issue in the . . . Supreme Court cases.
>
> App. 22a.

Other courts and commentators have also noted the confusion. *See, e.g.*, *Davis*, 220 A.3d at 553 (Baer, J., dissenting) (noting that judges "across the nation have struggled" with the issue); *Pollard v. State*, 287 So. 3d 649, 652 (Fla. Dist. Ct. App. 2019) ("Courts nationwide are struggling to find common legal ground on the constitutionality of compelled password production under the Fifth Amendment and its application in specific cases."); *see also, e.g.*, Cong. Res. Serv., *Catch Me If You Scan: Constitutionality of Compelled Decryption Divides the Courts* (Mar. 6, 2020), at https://crsreports.congress.gov/product/pdf/LSB/LSB10416; Kerr, *The Law of Compelled Decryption is a Mess, supra.*

Some courts, like the New Jersey Supreme Court here, have held that it is sufficient for the government to demonstrate merely that it knows that the *password itself* exists and that the suspect knows it.[3] 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.*[4]

---

[3] *See, e.g., Commonwealth v. Gelfgatt*, 11 N.E.3d 605 (Mass. 2014); *State v. Stahl*, 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016).

[4] *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*, 851 F.3d 238 (3d Cir. 2017); *Seo*, 148 N.E.3d at 957; *G.A.Q.L. v. State*, No. 4D18-1811, 2018 WL 5291918 (Fla. Dist. Ct. App. Oct. 24, 2018);

The Supreme Judicial Court of Massachusetts, for example, has sided with the New Jersey Supreme Court, focusing only on the password itself. In *Commonwealth v. Gelfgatt*, 11 N.E.3d 605 (Mass. 2014), the court concluded that under the state's analogue to the Fifth Amendment, the compelled entry of a passcode was testimonial, but that it could be overcome if the government showed that the suspect owned and controlled the computers and their contents. *Id.* at 615; *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."). The court explained that the government's knowledge concerning "the actual files and documents that are located on the defendant's computers" was irrelevant under the "foregone conclusion" exception. 11 N.E.3d at 614 n.13.[5]

By contrast, the Eleventh Circuit, the Third Circuit, and the Indiana Supreme Court have split with New Jersey and Massachusetts, concluding that, if the "foregone conclusion" exception applies, it must be directed to the files on the computer sought to be examined, not merely to the existence and ownership of the password itself. In *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335

Pollard v. State, No. 1D18-4572, 2019 WL 2528776 (Fla. Dist. Ct. App. June 20, 2019).

[5] *See also State v. Pittman*, 452 P.3d 1011, 1014 (Or. 2019) (appeal pending) (state must prove that defendant's knowledge of the passcode, not the contents of the iPhone, was a "foregone conclusion").

(11th Cir. 2012), the government subpoenaed a suspect to produce the unencrypted contents of encrypted hard drives. The court acknowledged that "the decryption and production of the hard drives would require the use of the contents of Doe's mind and could not be fairly characterized as a physical act that would be nontestimonial in nature." *Id.* at 1346. It then 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; *id.* at 1348 (*Fisher* and *Hubbell* "require that the Government show its knowledge *that the files exist*."). The court also noted that the government had not shown it knew "that Doe is even capable of accessing the encrypted portions of the drives." *Id.* at 1346.

In *United States v. Apple MacPro Computer*, 851 F.3d 238 (3d Cir. 2017), the Third Circuit upheld a magistrate order requiring the defendant to produce his seized electronic devices in a fully unencrypted state, which would require him to recall and use his password. 851 F.3d at 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. On the facts before it, the court concluded that the state had not met the requirements to invoke the exception because it had "failed to demonstrate that any particular files on the device exist or that [the defendant] possessed those files." *Id.* at 958.[6]

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.[7]

---

[6] *See also SEC v. Huang*, No. 15-cv-269, 2015 WL 5611644, at *3 (E.D. Pa. Sept. 23, 2015) (requiring government to show that documents sought are actually located on the smartphones); *In re Boucher*, No. 2:06-MJ-91, 2009 WL 424718, at *3 (D. Vt. Feb. 19, 2009) (requiring government to demonstrate knowledge of the existence and location of subpoenaed documents).

[7] Courts are also split on the government's burden of proof when showing that testimony is a "foregone conclusion." *Compare Jones*, 117 N.E.3d at 555 (requiring proof of "foregone conclusion" beyond a reasonable doubt) *with United States v. Spencer*, No. 17-CR-00259-CRB-1, 2018 WL 1964588, at *3 (N.D. Cal. Apr. 26, 2018) (requiring proof of "foregone conclusion" by clear and convincing evidence).

II. THIS CASE IS AN EXCELLENT VEHICLE FOR THE COURT TO RESOLVE THESE CONFLICTS.

As noted above, the decision below conflicts with other state supreme courts and federal courts of appeals on two related questions: whether the "foregone conclusion" rationale applies at all to the compulsion of pure testimony, and if so, whether it requires knowledge related to the password, or to the files. The court below decided each issue on the merits, and there are no obstacles to addressing them here. The case thus provides an ideal vehicle to address both issues.

First, Mr. Andrews asserted his privilege from the outset, and all lower courts addressed the claim in full. And as the case arises pre-trial, there are no "harmless error" issues. There is therefore no procedural barrier to reaching the issue.

Second, the court below squarely addressed and resolved both issues. It held first that the "foregone conclusion" exception applies, conflicting with *Davis*. Further, it held that the government need only show that the password's existence and ownership were "foregone conclusions," and not the files on the device, thus conflicting with several courts of appeals.

If the Court resolves the first question in Petitioner's favor, and holds the "foregone conclusion" exception inapplicable to pure testimony, it may not need to reach the second. But if it rules against Petitioner on the first issue, it will then need to resolve what the government must show to satisfy the exception in this setting.

Moreover, compelled password-disclosure cases typically arise in two different factual scenarios, and

this case would allow the Court to address the significance, if any, of that difference. Some cases, like this one, involve an order compelling a suspect to communicate a passcode—either orally or in writing—to the government. *See, e.g.*, *Davis*, 220 A.3d at 539 (order requiring Davis to "supply the Commonwealth with any passwords used to access the computer"); *State v. Stahl*, 206 So. 3d 124, 128 (Fla. Dist. Ct. App. 2016) (order to "give officers the passcode").

Other cases involve orders compelling a suspect to enter a passcode directly into a device, rather than communicate it directly to the state or the court. *See, e.g.*, *Apple MacPro Computer*, 851 F.3d at 243 (order requiring Doe to "produce his iPhone 6 Plus, his Mac Pro computer, and his two attached external hard drives in a fully unencrypted state"); *In re Grand Jury Subpoena*, 670 F.3d at 1337 (same); *Seo*, 148 N.E.3d at 954 (same).

The court below treated these two scenarios as indistinguishable. The court stated that both *"[c]ommunicating or entering* a passcode requires facts contained within the holder's mind," App. 31a (emphasis added), and treated both as "act of production" cases. It concluded that the "foregone conclusion" exception applied, meaning that direct disclosure—or, by the same logic, entry—of the passcode could be compelled. *See* App. 35a; *see also id.* at 20a. (LaVecchia, J., dissenting) ("The government should not be permitted to force defendant to cooperate in his own prosecution by obtaining, *through his entry of passcodes*, access to information the government believes will be incriminating." (emphasis added)).

Whether the difference between disclosing the passcode and entering it into the device is material to the Fifth Amendment has generated confusion and disagreement among courts and commentators alike. *Compare United States v. Jimenez*, 419 F. Supp. 3d 232, 233 (Mem.) (D. Mass. 2020) ("Whether the defendant is forced to reveal his passcode or unlock the phone . . . does not impact the analysis; both situations would force defendant to 'disclose the contents of his own mind.'"), *with United States v. Spencer*, No. 17-CR-00259-CRB-1, 2018 WL 1964588, at *2 (N.D. Cal. Apr. 26, 2018) ("[T]he government could not compel Spencer to state the password itself, whether orally or in writing. But the government is not seeking the actual passcode. Rather, it seeks the decrypted devices."); Orin Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 Tex. L. Rev. 767, 769–70 (2019) (entry communicates only knowledge of the password); Laurent Sacharoff, *What am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr*, 97 Tex. L. Rev. Online 62, 68–9 (2019) (entry communicates possession and likely knowledge of device's contents).

This case provides an excellent opportunity for the Court to shed much needed light on these important questions and to provide guidance to lower courts on the Fifth Amendment's application in these increasingly common contexts.

III. THE QUESTION PRESENTED IS IMPORTANT AND RECURRING.

The question presented is indisputably important. Cell phones 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. And government efforts to discover the contents of encrypted devices are a frequent part 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.[8]

Just last year, New Jersey and 21 other states urged this Court to grant certiorari to decide this very issue, stating that its resolution "could affect almost every criminal case." *See* Br. of *Amici Curiae* States of Utah *et al.* at 1. At that time, there was no split on the issue of compelling the direct disclosure of a passcode, and this Court denied review. But as shown above, Point I, *supra,* the split is now clear, and calls for this Court's resolution of what both sides agree is an important question. Twice in recent terms, this Court has recognized that the widespread adoption of cell phones has brought about a fundamental shift in the amount and type of personal information that is vulnerable to search by law enforcement. *Riley v. California*, 573 U.S. 373 (2014); *Carpenter v. United States*, 138 S. Ct. 2206 (2018). Because cell phones 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*,

---

[8] 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).

573 U.S. at 396, 394. They record our most intimate communications, thoughts, and interests, recording what we read, view, and listen to; who we call, text, or email; our whereabouts 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.").

Since the Court's decisions in *Riley* and *Carpenter,* cell phones have only become more indispensable and prevalent. In the last six years, the number of Americans who own smartphones has increased by 70 percent,[9] the storage capacity of smartphones has quintupled,[10] and the average smartphone owner has at least twice as many apps on

---

[9] In 2019, 81 percent of Americans owned a smartphone. Pew Res. Ctr., *Mobile Fact Sheet* (June 12, 2019), http://www.pewinternet.org/fact-sheet/mobile/. *Cf. Riley*, 573 U.S. at 385 (citing A. Smith, Pew Res. Ctr., *Smartphone Ownership—2013 Update* (June 5, 2013) (noting "56% of American adults are now smartphone owners")).

[10] The average capacity of smartphones has increased from 16 to 80 gigabytes. *See* Sujeong Lim, *Average Storage Capacity in Smartphones to Cross 80GB by End-2019*, Counterpoint (Mar. 16, 2019), https://www.counterpointresearch.com/average-storage-capacity-smartphones-cross-80gb-end-2019; *Riley*, 573 U.S. at 394 ("current top-selling smart phone has a standard capacity of 16 gigabytes").

their phone.[11]

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 cell phones 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 375. A recent survey by the non-profit Upturn found that since 2015, law enforcement agencies have performed hundreds of thousands of cell phone "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."[12] 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."[13] In sum,

---

[11] Average smartphone users now have 90 different apps on their devices. Sarah Perez, *Top mobile apps see declines in consumer engagement amid increased competition*, TechCrunch (July 27, 2020), https://techcrunch.com/2020/07/27/top-mobile-apps-see-declines-in-consumer-engagement-amid-increased-competition; *Riley*, 573 U.S. at 396 (describing various apps and noting, at that time, that the average smartphone user "has installed 33 apps, which together can form a revealing montage of the user's life.")

[12] 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.

[13] *Id.* at 32, 40.

"[e]very American is at risk of having their phone forensically searched by law enforcement."[14]

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.

IV. THE DECISION BELOW IS INCORRECT.

The Supreme Court of New Jersey's decision is incorrect for three reasons.

A. The "Foregone Conclusion" Exception Never Applies to Oral or Written Testimony.

First, where a court orders an individual to answer a question, the application of the Fifth Amendment privilege ought to be straightforward: if the answer 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 (2001) (per curiam). The Fifth Amendment provides that "[n]o person … shall be compelled in any criminal case to be a witness against himself." A "witness" was understood at the time of the founding to mean "a person who gives or furnishes evidence." *Hubbell*, 530 U.S. at 50 (Thomas, J., concurring). Here, Mr. Andrews is being compelled, by state court order, to "be a witness" against himself—

[14] *Id.* at 32.

to furnish the passcodes for the State's use in its prosecution against him.

The Founders adopted the Fifth Amendment out of concern about "Star Chamber" practices in England, which compelled individuals to testify against themselves, and thereby imposed on them "the cruel trilemma" of telling the truth, committing perjury, or refusing to answer and facing contempt. *Couch v. United States*, 409 U.S. 322, 327–28 (1973). Absent the protection of the Fifth Amendment, the order in this case imposes precisely that "cruel trilemma" on Mr. Andrews.

This Court's decisions have narrowed the original understanding of "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 II*, 487 U.S. 201, 211, 213. But even under that definition, being compelled to disclose one's password, like "be[ing] compelled to reveal the combination to [petitioner's] wall safe," necessarily communicates the contents of one's mind directly to the state, and is testimonial. *Id.* at 210 n.9 (alterations in original).

The "foregone conclusion" exception has been applied by this Court only to a subpoena for business records. It does not apply to pure testimony, full stop. The government cannot compel a suspected burglar to answer the question, "Did you enter the house?" by asserting that the answer is a "foregone conclusion," even if the suspect was arrested inside with a bag of stolen goods.

The New Jersey Supreme Court's first error, therefore, was in applying to pure testimony the "foregone conclusion" rationale, which this Court has applied only to "acts of production" in the context of subpoenas for physical documents. As the *Davis* court stated, "it would be a significant expansion of the "foregone conclusion" rationale to apply it to a defendant's compelled oral or written testimony." 220 A.3d at 549.

The court below concluded that the "foregone conclusion" exception should apply because it deemed the disclosure of a password of "minimal testimonial value," noting that a password consists of numbers and characters. App. 33a. That is plainly wrong. "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 the question is, or whether the State believes it already knows the answer or could readily obtain it from other sources. *Id.* In *Muniz*, therefore, the Fifth Amendment privilege protected an arrestee from being compelled to provide the date of his sixth birthday. Similarly, the Court has noted that the Fifth Amendment protects an individual from being forced to disclose the combination to a wall safe, which is also merely a series of numbers. *Hubbell*, 530 U.S. at 43. 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").

The New Jersey Supreme Court's standard of "minimal testimonial value" is unprecedented, unmanageable, and dangerous. It is also wholly untethered to the text, original understanding, or purpose of the Fifth Amendment. The privilege against compelled self-incrimination is not designed to protect "valuable" testimony. It protects individual autonomy, and is designed to preclude the government from imposing the "cruel trilemma" on an individual by requiring him to answer a question that will lead to his incrimination. *Couch*, 409 U.S. at 328; *Muniz*, 496 U.S. 582. There is no hierarchy of protection for "high-value" or "low-value" testimony. *Muniz*, 496 U.S. 582. And the Fifth Amendment affords no metric for distinguishing between compelled testimony based on its "minimal value."

Except for rote voice exemplars, verbal statements are virtually always testimonial because they reveal the contents of a suspect's mind. *Id.* at 597. 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). "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. Andrews 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 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 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.

Because the "foregone conclusion" exception has no basis in the text or the founding era understandings of the privilege against self-incrimination, it should at a minimum be limited to the facts of *Fisher*. *Fisher*, the only case of this Court that has actually applied a "foregone conclusion" exception to override the privilege, 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. *Fisher*, 425 U.S. at 393–96, 413.

The question before this Court was whether the attorneys, as agents of the taxpayer, could be forced to produce the documents. The order did not compel oral testimony, as the order at issue in this case does. Nor did the order implicitly compel the taxpayer to restate, repeat, or affirm the truth of the contents of the documents sought. *Id.* at 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 trial court order at issue here demands that Petitioner testify from memory as to the contents of passwords he created, and the prosecution is entirely reliant on him telling the truth about what he recalls his passwords to be. *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 614 n.13. 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); *cf. Burt Hill, Inc. v. Hassan*, No. CIV. A. 09-1285, 2010 WL 55715, at *2 (W.D. Pa. Jan. 4, 2010) (contents of electronic storage devices used by defendants while employed by plaintiff).

At the same time, lower courts have given individuals the full strength of the self-incrimination privilege in 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.*, *Muniz*, 496 U.S. 582; *United States v. Green*, 272 F.3d 748 (5th Cir. 2001), *Commonwealth v. Hughes*, 404 N.E.2d 1239, 1246 (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*, 199 Cal. Rptr. 366, 374 (Ct. App. 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.[15]

C. The Court Should Overrule *Fisher* Because the Fifth Amendment Privilege Against Self-Incrimination Does Not Properly Include a "Foregone Conclusion" Exception.

Any one of the above three errors is sufficient to reverse the decision below. But in the event that the Court disagrees with Petitioner on all three prior arguments, it should consider overruling *Fisher*. The "foregone conclusion" exception finds no support in the text or original understanding of the Fifth

[15] As argued above, the court's principal error was to apply the "foregone conclusion" exception at all to a demand for pure testimony. But even assuming arguendo that the "foregone conclusion" rationale could apply in this context, the court also erred in what it required the government to demonstrate. The court required merely that the government show that it knew that Mr. Andrews *had a password* to the phones (because that would be all it learned from the password's compelled disclosure). But that is incorrect, as the government would also learn *the contents of the password itself*, and plainly the government does not possess that information at all.

Amendment. It has been applied by this Court to permit compulsion exactly once. And it has created widespread confusion in the courts below.

"Foregone conclusion" is found nowhere in the text of the amendment, or in founding-era discussions or applications of the privilege. Indeed, for many years the Fifth Amendment 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). Thus, 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 49–55 (Thomas, J., and Scalia, J., concurring); *Carpenter v. United States*, 138 S. Ct. 2206, 2271 (2018) (Gorsuch, J., dissenting). As Justice Thomas has observed, *Boyd* reflects the proper understanding that "witness" means one who gives evidence, and not merely one who testifies. *Hubbell*, 530 U.S. at 50 (Thomas, J., concurring).

This Court's decision in *Fisher* rejects this understanding and permits the government to force a person to furnish incriminating documents. And it does so by creating out of whole cloth a "foregone conclusion" exception that finds no support in the text, history or purpose of the Fifth Amendment. As noted above, if the government cannot compel an individual to answer "Did you enter the house?" even if she was arrested in the house and the state can prove burglary, it should not be able to compel *any* incriminating evidence, much less pure testimony, on the ground that it already knows the answer.

If necessary, therefore, this Court should revisit *Fisher* and reject the unfounded "foregone conclusion" exception altogether.

CONCLUSION

The petition for writ of certiorari should be granted.

Respectfully submitted,

Jennifer S. Granick
Counsel of Record
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94114
(415) 343-0758
jgranick@aclu.org

David D. Cole
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
915 15th Street, NW
Washington, D.C. 20005

Brett Max Kaufman
Jennesa Calvo-Friedman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004

Robert L. Tarver, Jr.
LAW OFFICES OF ROBERT L. TARVER, JR.
66 South Main Street
Toms River, NJ 08757

Jeanne LoCicero
Alexander Shalom
AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY FOUNDATION
Post Office Box 32159
Newark, NJ 07102

Mark Rumold
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Date: January 7, 2021

APPENDIX

APPENDIX A

SUPREME COURT OF NEW JERSEY
A-72 September Term 2018
082209

STATE OF NEW JERSEY,
Plaintiff-Respondent,
v.
ROBERT ANDREWS,
Defendant-Movant.

On appeal from the Superior Court,
Appellate Division, whose opinion is reported at
457 N.J. Super. 14 (App. Div. 2018).

[Filed August 10, 2020]

OPINION

JUSTICE SOLOMON delivered the opinion of the Court.

This appeal presents an issue of first impression to our Court—whether a court order requiring a criminal defendant to disclose the passcodes to his passcode-protected cellphones violates the Self-Incrimination Clause of the Fifth Amendment to the United States Constitution or New Jersey's common law or statutory protections against self-incrimination. We conclude that it does not and affirm the Appellate Division's judgment.

The target of a State narcotics investigation advised detectives that defendant, a law enforcement officer, had provided him with information about the investigation and advice to avoid criminal exposure.

The target gave statements to investigators, confirmed in part by his cellphone, about photographs, cellphone calls, text message exchanges, and conversations with defendant during which defendant recommended that the target remove a tracking device that may have been placed on his car by the police; recommended that the target discard cellphones he and his cohorts used; and revealed the identity of an undercover officer and an undercover police vehicle.

The State obtained an arrest warrant for defendant and search warrants for defendant's iPhones, which were seized. Because the contents of the iPhones were inaccessible to investigators without the iPhones' passcodes, the State moved for an order compelling defendant to disclose the passcodes.

Defendant claimed the United States Constitution and New Jersey's common law and statutory protections against compelled self-incrimination protected his disclosure of the passcodes. The motion court and Appellate Division concluded that defendant's disclosure of the passcodes could be compelled. We agree and affirm.

I.

The State claims that defendant Robert Andrews, a former Essex County Sheriff's Officer, revealed an undercover narcotics investigation to its target, Quincy Lowery.

The motion court and Appellate Division records disclose that Essex County Prosecutor's Office detectives went to the Essex County Sheriff's Office to interview Andrews, with his counsel present, about his association with Lowery. Andrews's attorney told the detectives that his client did "not wish to speak to

anyone" and would be invoking his Fifth Amendment privilege against self-incrimination. The attorney also requested the return of Andrews's two cellphones seized earlier that day. The detectives advised Andrews and his counsel that the cellphones were seized in connection with a criminal investigation and would not be immediately returned, but that Andrews was free to leave.

Later that day, detectives from the Essex County Prosecutor's Office interviewed Lowery, who detailed his relationship with Andrews. Lowery explained that they were members of the same motorcycle club and had known each other for about a year. During that time, Andrews registered a car and motorcycle in his name so that Lowery could use them. Lowery also told the detectives that he regularly communicated with Andrews using the FaceTime application on their cellphones.

Lowery claimed that during one of those communications, Andrews told him to "get rid of" his cellphones because law enforcement officials were "doing wire taps" following the federal arrests of Crips gang members.[1] According to Lowery, Andrews said that the State Police and the Sheriff's Office were "going to do a run" and Lowery should "just be careful."

Lowery also explained that he had suspected he was being followed by police officers after receiving a tip from a fellow drug dealer who observed a white van outside of Lowery's residence. Lowery relayed that suspicion to Andrews and texted him the license plate

[1] Lowery also informed the detectives that Andrews had self-identified as a member of the Grape Street Crips.

number of one of the vehicles Lowery believed was following him. According to Lowery, Andrews informed him that the license plate number belonged either to the Prosecutor's Office or the Sheriff's Department and advised him to put his car "on a lift to see if there is a [tracking] device under there."

Lowery reported that he "stopped hustling" and discarded one of his cellphones after realizing he was being followed. Lowery also described one occasion when he noticed a man enter a restaurant shortly after Lowery arrived. Lowery explained that he suspected the man was an undercover police officer after noticing a bulge, believed to be a gun, on his hip. Using his cellphone, Lowery surreptitiously photographed the man. Lowery claimed that later that day he showed the picture to Andrews who identified the individual as a member of the Prosecutor's Office.

Further investigation following Lowery's statements largely corroborated his allegations. Lowery's Samsung Galaxy S5 cellphone was sent to the Cyber Crimes Unit for data extraction. The extraction report revealed that Lowery changed his telephone number shortly after he claims Andrews informed him of a potential wiretap. The report also revealed that two days after changing his number, Lowery texted an unknown subscriber to "Go get new phones." Seven minutes later, he texted another number advising that "Everybody around u need to get new ones 2."

A month later, Lowery texted a number associated with Andrews and asked "Where you at[?]" Forty-four minutes after that message, Lowery texted Andrews the license plate number of the car he suspected of following him. Lowery received a text

message from one of Andrews's cellphone numbers two days later stating, "Bro call me we need to talk face to face when I get off."

Detectives later confirmed that the license plate number Lowery texted to Andrews was registered to a rental company and was being used by detectives on the Prosecutor's Office Narcotics Task Force. The extraction report also contained a photograph of a Narcotics Task Force detective matching the description of the undercover officer who followed Lowery into a restaurant. A review of State Motor Vehicle Commission records revealed that a 2002 Jeep Grand Cherokee Limited and 2007 Suzuki GSX motorcycle, which officers observed Lowery operating two weeks before his arrest, were registered to Andrews.

Following their second interview with Lowery, the State obtained Communication Data Warrants for cellphone numbers belonging to Andrews and Lowery. Over the next two weeks, the State sought and received additional search warrants for phones belonging to Lowery and Andrews, including a Communication Data Warrant for a second iPhone seized from Andrews. The warrants revealed 114 cellphone calls and text messages between Lowery and Andrews over a six-week period.

Andrews was indicted by an Essex County grand jury for (1) two counts of second-degree official misconduct (N.J.S.A. 2C:30-2); (2) two counts of third-degree hindering the apprehension or prosecution of another person (N.J.S.A. 2C:29-3(a)(2)); and (3) two counts of fourth-degree obstructing the administration of the law or other government function (N.J.S.A. 2C:29-1).

According to the State, its Telephone Intelligence Unit was unable to search Andrews's iPhones—an iPhone 6 Plus and an iPhone 5s—because they "had iOS systems greater [than] 8.1,[2] making them extremely difficult to access without the owner/subscriber's pass code." A State detective contacted and conferred with the New York Police Department's (NYPD) Technical Services unit, as well as a technology company called Cellebrite, both of which concluded that the cellphones' technology made them inaccessible to law enforcement agencies. The detective also consulted the Federal Bureau of Investigation's Regional Computer Forensics Laboratory, which advised that it employed "essentially the same equipment used by" the State and NYPD and would be unable to access the phones' contents. The State therefore moved to compel Andrews to disclose the passcodes to his two iPhones.

Andrews opposed the motion, claiming that compelled disclosure of his passcodes violates the protections against self-incrimination afforded by New Jersey's common law and statutes and the Fifth Amendment to the United States Constitution.

---

[2] "Apple manufactures smartphones, named iPhones, which run an operating system named iOS. Numerical names designate different versions of the operating system (e.g., iOS 8). Apple adopted full-disk encryption by default in September 2014 with iOS 8." Kristen M. Jacobsen, Note, *Game of Phones, Data Isn't Coming: Modern Mobile Operating System Encryption and its Chilling Effect on Law Enforcement*, 85 Geo. Wash. L. Rev. 566, 574 (2017) (footnotes omitted). "Full-disk encryption automatically converts everything on a hard drive, including the operating system, into an unreadable form until the proper key (i.e., passcode) is entered." *Id.* at 573 (internal quotation marks omitted).

The trial court rejected Andrews's arguments, ruling that "the act of providing a PIN, password, or passcode is not a testimonial act where the Fifth Amendment or New Jersey common and statutory law affords protection." The court reasoned that "[a]llowing the State to access the call logs and text messages on Andrews's iPhones will add little to nothing to the aggregate of the Government's information." The court added that "any testimonial act contained in the act of providing the PIN or passcode is a foregone conclusion because the State has established with reasonable particularity that it already knows that (1) the evidence sought exists, (2) the evidence was in the possession of the accused, and (3) the evidence is authentic."

Nevertheless, the trial court limited access to Andrews's cellphones "to that which is contained within (1) the 'Phone' icon and application on Andrews's two iPhones, and (2) the 'Messages' icon and/or text messaging applications used by Andrews during his communications with Lowery." The court also ordered that the search "be performed by the State, in camera, in the presence of Andrews's defense counsel and the [c]ourt," with the court "review[ing] the PIN or passcode prior to its disclosure to the State."

The Appellate Division denied Andrews's motion for leave to appeal from the trial court's order. We granted Andrews's motion for leave to appeal to this Court and summarily remanded to the Appellate Division to consider Andrews's arguments on the merits. *State v. Andrews*, 230 N.J. 553 (2017).

On remand, the Appellate Division affirmed the trial court's order requiring Andrews to disclose the passcodes to his two iPhones. *State v. Andrews*, 457 N.J. Super. 14, 18 (App. Div. 2018). The panel acknowledged Andrews's Fifth Amendment concerns but held that the only testimonial aspects of providing the passcodes "pertain to the ownership, control, use, and ability to access the phones," which were facts already known to the State. *Id.* at 29. Therefore, the "foregone conclusion" exception to the "act of production" doctrine applied because the State "establish[ed] with reasonable particularity (1) knowledge of the existence of the evidence demanded; (2) defendant's possession and control of that evidence; and (3) the authenticity of the evidence." *Id.* at 22-23. In the Appellate Division's view, the State satisfied all three requirements of the exception by describing "the specific evidence it seeks to compel, which is the passcodes to the phones" and establishing that Andrews "exercised possession, custody, or control over" the seized iPhones.[3] *Id.* at 24.

The Appellate Division similarly rejected Andrews's state common law claims, noting the State would likely be unable to decipher information stored on the iPhones without their passcodes and that, when "the State has established the elements for application of the 'foregone conclusion' doctrine, New Jersey's common law privilege against self-incrimination does not bar compelled disclosure of passcodes for defendant's phones." *Id.* at 32.

Finally, the Appellate Division rejected Andrews's contention that the information sought is

[3] The panel noted that the parties had not raised the issue of the authenticity of the electronically stored information. *Id.* at 30.

protected by N.J.S.A. 2A:84A-19 and N.J.R.E. 503, which provide protection from self-incrimination, subject to an exception for court orders compelling production of "a document, chattel or other thing" to which "some other person or a corporation or other association has a superior right." *See id.* at 32 (quoting N.J.S.A. 2A:84A-19(b); N.J.R.E. 503(b)). The panel concluded that the search warrants issued for Andrews's iPhones "give the State a superior right to possession of the passcodes." *Id.* at 33.

We granted Andrews's motion for leave to appeal. 237 N.J. 572 (2019). We also granted amicus curiae status to the Office of the Attorney General, the County Prosecutors Association of New Jersey, the New Jersey State Bar Association, the Association of Criminal Defense Lawyers of New Jersey (ACDL), the Office of the Public Defender, the Electronic Frontier Foundation, the American Civil Liberties Union, the American Civil Liberties Union of New Jersey, and the Electronic Privacy Information Center.

II.

Andrews contends that the Appellate Division subverted New Jersey's broader privilege against self-incrimination and employed a "simplistic mechanical approach" to the Fifth Amendment's foregone conclusion exception. According to Andrews, that exception should not apply to digital technology because it "is distinctly different than paper documents," and the State "does not know what the passwords are, if Andrews knew them, or what is on the phones." Andrews also accuses the Appellate Division of treating his state law right against self-incrimination as expendable and conflating the issuance of search warrants with ownership to

construe the State's search as consistent with the language of N.J.S.A. 2A:84A-19(b).

The State argues in response that Andrews's contention concerning the exposure of incriminating information is baseless because the trial court's order mandates disclosure of the passcodes in camera prior to their communication to the State. Similarly, the State claims that the passcodes are "merely a random sequence of numbers with no testimonial significance," placing their compelled disclosure beyond the reach of the Fifth Amendment's Self-Incrimination Clause.

In answer to Andrews's state law claims, the State argues that communication between co-conspirators has no special privacy status, that the State "has established . . . that it already knows what is on the phone[s]," and that the State has a superior right to the contents of the phones because of the unchallenged search warrant.

In support of the State, the County Prosecutors Association of New Jersey posits that the Fifth Amendment's privilege does not permit noncompliance with a search warrant valid under the Fourth Amendment. The Office of the Attorney General similarly warns that Andrews is attempting to use the Fifth Amendment to undermine the execution of a valid and enforceable search warrant. Additionally, the Attorney General argues that Andrews's constitutional, statutory, and common law rights against self-incrimination are not affected by the disclosure of his cellphone passcodes because compelled disclosure would communicate only his ability to unlock the phones.

The ACDL disagrees with the State and its supportive amici, contending that the Appellate Division's Fifth Amendment analysis was skewed by its focus on Andrews's ostensible knowledge of the phones' passcodes instead of the State's knowledge of the phones' contents. According to the ACDL, if we adopt the Appellate Division's reasoning with respect to mobile devices, self-incrimination protections will exist in name only.

The New Jersey State Bar Association, Electronic Frontier Foundation, American Civil Liberties Union, and American Civil Liberties Union of New Jersey echo the ACDL's arguments and claim that the Fifth Amendment shields information that exists only in a criminal defendant's mind from government compelled disclosure. They also assert that the State failed to satisfy the reasonable particularity requirement of the foregone conclusion exception because it cannot identify the digital records it wants Andrews to produce through disclosure of his passcodes.

III.

The question before the Court—whether defendant can be compelled to disclose the passcodes to his cellphones seized by law enforcement pursuant to a lawfully issued search warrant—is ultimately answered by analyzing federal and state protections against compelled self-incrimination. But because the State contends that those protections do not allow defendant to ignore a lawfully issued search warrant, we begin with a brief review of the applicable principles of our search and seizure jurisprudence.

A.

The Fourth Amendment to the United States Constitution and Article I, paragraph 7 of the New Jersey Constitution protect individuals' rights "to be secure in their persons, houses, papers, and effects" by requiring that search warrants be "supported by oath or affirmation" and describe with particularity the places subject to search and people or things subject to seizure. Searches executed pursuant to warrants compliant with those requirements are presumptively valid, *State v. Jones*, 179 N.J. 377, 388 (2004), and reviewing courts "should pay substantial deference" to judicial findings of probable cause in search warrant applications, *State v. Kasabucki*, 52 N.J. 110, 117 (1968).

Furthermore, the State has broad authority to effectuate searches permitted by valid search warrants. Pursuant to that authority, the State may destroy property, *United States v. Ramirez*, 523 U.S. 65, 69-71 (1998), forcibly enter a residence, *United States v. Banks*, 540 U.S. 31, 33, 40 (2003), and employ flash-bang devices, *State v. Rockford*, 213 N.J. 424, 431-32 (2013), all in the name of executing a warrant.

Andrews 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. Neither does defendant challenge the particularity with which the search warrants describe the "things subject to seizure." Thus, the State is permitted to access the phones' contents, as limited by the trial court's order, in the same way that the State may survey a home, vehicle, or other place that is the subject of a search

warrant.

But a lawful seizure does not allow compelled disclosure of facts otherwise protected by the Fifth Amendment. *In re Search of a Residence in Oakland*, 354 F. Supp. 3d 1010, 1014 (N.D. Cal. 2019); Michael S. Pardo, *Disentangling the Fourth Amendment and the Self-Incrimination Clause*, 90 Iowa L. Rev. 1857, 1860 (2005).

Andrews objects here to the means by which the State seeks to effectuate the searches authorized by the lawfully issued search warrants—compelled disclosure of his cellphones' passcodes—which Andrews claims violate federal and state protections against compelled self-incrimination. We therefore consider whether the Fifth Amendment protects Andrews from being compelled to disclose his passcodes.

B.

1.

The Fifth Amendment to the United States Constitution provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." U.S. Const. amend. V. That right against self-incrimination "applies only when the accused is compelled to make a testimonial communication that is incriminating." *Fisher v. United States*, 425 U.S. 391, 408 (1976).

Testimonial communications may take any form, *Schmerber v. California*, 384 U.S. 757, 763-64 (1966), but must "imply assertions of fact" for the Fifth Amendment privilege against self-incrimination to attach, *Doe v. United States* (*Doe II*), 487 U.S. 201, 209 (1988). Thus, actions that do not require an individual

"to disclose any knowledge he might have" or "to speak his guilt" are nontestimonial and therefore not protected by the Fifth Amendment. *Id.* at 211 (quoting *United States v. Wade*, 388 U.S. 218, 222-23 (1967)).

Accordingly, criminal defendants may lawfully be compelled to display their physical characteristics and commit physical acts because the display of physical characteristics is not coterminous with communications that relay facts. *United States v. Hubbell*, 530 U.S. 27, 35 (2000). Among those acts are creating handwriting samples, *Gilbert v. California*, 388 U.S. 263, 266 (1967), and voice samples, *United States v. Dionisio*, 410 U.S. 1, 7 (1973); providing blood, hair, and saliva samples, *State v. Burke*, 172 N.J. Super. 555, 557 (App. Div. 1980); standing in a lineup, *Wade*, 388 U.S. at 221; and donning particular articles of clothing, *Holt v. United States*, 218 U.S. 245, 252-53 (1910). Also, consistent with the Fifth Amendment, individuals may be compelled to execute an authorization directing a foreign bank to disclose account records "because neither the form, nor its execution, communicates any factual assertions, implicit or explicit, or conveys any information to the Government." *Doe II*, 487 U.S. at 215.

A handful of courts have held that compelled State access to electronic devices through the use of biometric features does not violate the Fifth Amendment. *In re Search Warrant Application for Cellular Tel. in U.S. v. Barrera*, 415 F. Supp. 3d 832, 833 (N.D. Ill. 2019) ("[C]ompelling an individual to scan their biometrics, and in particular their fingerprints, to unlock a smartphone device neither violates the Fourth nor Fifth Amendment."); *State v. Diamond*, 905 N.W.2d 870, 878 (Minn. 2018) ("[P]roviding a fingerprint to the police to unlock a

cellphone was not a testimonial communication protected by the Fifth Amendment."). But see *In re Search of a Residence in Oakland*, 354 F. Supp. 3d at 1018 (denying a search warrant seeking use of biometrical features to unlock electronic devices).

As those examples suggest, the Fifth Amendment is not an absolute bar to a defendant's forced assistance of the defendant's own criminal prosecution. *Doe II*, 487 U.S. at 213. In contrast to physical communications, however, if an individual is compelled "to disclose the contents of his own mind," such disclosure implicates the Fifth Amendment privilege against self-incrimination. *Id.* at 211 (quoting *Curcio v. United States*, 354 U.S. 118, 128 (1957)). In a series of cases, the United States Supreme Court has considered when an act of production constitutes a protected testimonial communication rather than a non-testimonial and therefore unprotected communication. In advancing that distinction, the Court has also developed an exception to the Fifth Amendment privilege against self-incrimination for acts of production that are testimonial in nature but of minimal testimonial value because the information they convey is a "foregone conclusion." We turn now to those developments.

2.

In *Wilson v. United States*, the Supreme Court upheld a contempt finding against a corporate officer who failed to comply with a grand jury subpoena compelling disclosure of potentially incriminating corporate records in his possession. 221 U.S. 361, 386 (1911). The Court explained that "the physical custody of incriminating documents does not of itself protect the custodian against their compulsory production."

Id. at 380. Therefore "the fact of actual possession or of lawful custody would not justify the officer in resisting inspecting, even though the record was made by himself and would supply the evidence of his criminal dereliction." *Ibid.*

Sixty-five years later, the Fisher Court drew a distinction between the act of producing documents and the documents themselves in the context of subpoenaed tax records, finding that, even though the documents were not privileged,

> [t]he act of producing evidence in response to a subpoena nevertheless has communicative aspects of its own, wholly aside from the contents of the papers produced. Compliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer. It also would indicate the taxpayer's belief that the papers are those described in the subpoena.
>
> [425 U.S. at 409-10.]

After those observations, the Court found that "the elements of compulsion are clearly present" in the production, "but the more difficult issues are whether the tacit averments of the taxpayer are both 'testimonial' and 'incriminating' for purposes of applying the Fifth Amendment." *Ibid.* Ultimately, the Court declared itself "confident that however incriminating the contents of the accountant's workpapers might be, the act of producing them—the only thing which the taxpayer is compelled to do—would not itself involve testimonial self-incrimination." *Id.* at 410-11.

The reasoning with which the Court explained that conclusion ultimately gave rise to the foregone conclusion exception:

> It is doubtful that implicitly admitting the *existence* and *possession* of the papers rises to the level of testimony within the protection of the Fifth Amendment. . . . *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.* Under these circumstances by enforcement of the summons "no constitutional rights are touched. The question is not of testimony but of surrender." *In re Harris*, 221 U.S. 274, 279 (1911). . . . .
>
> Moreover, assuming that these aspects of producing the accountant's papers have some *minimal testimonial significance*, surely it is not illegal to seek accounting help in connection with one's tax returns or for the accountant to prepare workpapers and deliver them to the taxpayer. At this juncture, we are quite unprepared to hold that either the fact of existence of the papers or of their possession by the taxpayer poses any realistic threat of incrimination to the taxpayer.
>
> *As for the possibility that responding to the subpoena would authenticate the workpapers, production*

> *would express nothing more than the taxpayer's belief that the papers are those described in the subpoena*. . . . The documents would not be admissible in evidence against the taxpayer without authenticating testimony. Without more, responding to the subpoena in the circumstances before us would not appear to represent a substantial threat of self-incrimination.
>
> [*Id.* at 411-13 (emphases added; footnotes and citations omitted).]

In *United States v. Doe (Doe I)*, the Court applied the logic from *Fisher* in considering "whether, and to what extent, the Fifth Amendment privilege against compelled self-incrimination applies to the business records of a sole proprietorship," 465 U.S. 605, 606 (1984), particularly where the district court indicated that "the Government had conceded that the materials sought in the subpoena were or might be incriminating," *id.* at 608.

After "hold[ing] that the contents of those records are not privileged," the Court stressed, as did the *Fisher* Court, that even where "the contents of a document may not be privileged, the act of producing the document may be" because "[a] government subpoena compels the holder of the document to perform an act that may have testimonial aspects and an incriminating effect." *Id.* at 612. Stressing the district court's factfinding that the subject documents did contain incriminating information, the *Doe I* Court distinguished *Fisher*. *Id.* at 613-14.

The *Doe I* Court rejected the Government's argument "that any incrimination [flowing from the

compelled production in that case] would be so trivial that the Fifth Amendment is not implicated," relying instead on "the findings made" by the trial court in holding that "the risk of incrimination was 'substantial and real' and not 'trifling or imaginary.'" *Id.* at 614 n.13 (quoting *Marchetti v. United States*, 390 U.S. 39, 53 (1968)). The Court explained, "Respondent did not concede in the District Court that the records listed in the subpoena actually existed or were in his possession. Respondent argued that by producing the records, he would tacitly admit their existence and his possession." *Ibid.*

Although the Court reached its holding on that basis, it also noted the respondent's argument "that if the Government obtained the documents from another source, it would have to authenticate them before they would be admissible at trial. By producing the documents, respondent would relieve the Government of the need for authentication." *Ibid.* (citation omitted).

The Court stressed that a "valid claim of the privilege against self-incrimination" had been asserted, which the Government could then rebut "by producing evidence that *possession, existence, and authentication were a 'foregone conclusion*.'" *Ibid.* (emphasis added) (quoting *Fisher*, 425 U.S. at 411). In *Doe I*, "however, the Government failed to make such a showing." *Ibid*.

In *Hubbell*, the Court reiterated, with respect to "13,120 pages of documents and records" produced in response to a grand jury subpoena, 530 U.S. at 31, that "[t]he 'compelled testimony' that is relevant in this case is not to be found in the contents of the documents produced in response to the subpoena. It

is, rather, the testimony inherent in the act of producing those documents," *id.* at 40. Noting that the parties' dispute centered "on the significance of that testimonial aspect," the Court wrote, "The Government correctly emphasizes that the testimonial aspect of a response to a subpoena duces tecum does nothing more than establish the existence, authenticity, and custody of items that are produced." *Id.* at 40-41.

But to convey that information, the Court stressed, "[i]t was unquestionably necessary for respondent to make extensive use of 'the contents of his own mind' in identifying the hundreds of documents responsive to the requests in the subpoena," such that "[t]he assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox." *Id.* at 43 (quoting *Curcio*, 354 U.S. at 128). Indeed, the act of production at issue "was tantamount to answering a series of interrogatories asking a witness to disclose the existence and location of particular documents fitting certain broad descriptions." *Id.* at 41.

In finding the act of producing the documents fell within the ambit of the Fifth Amendment's protection against self-incrimination, *id.* at 45, the Court rejected the Government's argument that "the existence and possession of . . . records [like those sought through the subpoena] by any businessman is a 'foregone conclusion'" as a misreading of *Fisher* and an end run around *Doe I*. *Id.* at 44. The Court explained,

> Whatever the scope of this "foregone conclusion" rationale, the facts of this

> case plainly fall outside of it. While in *Fisher* the Government already knew that the documents were in the attorneys' possession and could independently confirm their existence and authenticity through the accountants who created them, here the Government has not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent. The Government cannot cure this deficiency through the overbroad argument that a businessman such as respondent will always possess general business and tax records that fall within the broad categories described in this subpoena.
>
> [*Id.* at 44-45.]

From those cases, which all addressed the compelled production of documents, the following principles can be inferred: For 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. And even production that is of a testimonial nature can be compelled if the Government can demonstrate it already knows the information that act will reveal—if, in other words, the existence of the requested documents, their authenticity, and the defendant's possession of and control over them—are a "foregone conclusion."

3.

Although the Supreme Court has considered the application of the foregone conclusion exception only in the context of document production, courts in other jurisdictions have grappled with the applicability of the exception beyond that context, and many have considered whether the exception applies to compelled decryption or to the compelled production of passcodes and passwords, reaching divergent results.

Among other causes for that divergence is a dispute over how to adapt the foregone conclusion analysis from the document-production context, which involves the act of producing the document and the contents of the document, to the context of passcode production, which involves the act of producing the passcode that protects the contents of the electronic device.

Some courts to consider the issue have focused on the production of the passcode as a means to access the contents of the electronic device, treating the contents of the devices as the functional equivalent of the contents of documents at issue in the United States Supreme Court cases. Most recently, the Supreme Court of Indiana considered a woman's challenge to the order that she unlock her iPhone for law enforcement after she had been arrested for stalking. *Seo v. State*, ___ N.E.3d ___, ___ (June 23, 2020) (slip op. at 2-3).

After reviewing *Fisher*, *Doe I*, and *Hubbell*, *id.* at 6-8, the court in *Seo* "dr[ew] two analogies" in extending its observations on those cases "to the act of producing an unlocked smartphone": "First, entering the password to unlock the device is analogous to the

physical act of handing over documents. And second, the files on the smartphone are analogous to the documents ultimately produced," *id.* at ___ (slip op. at 8-9) (citing Laurent Sacharoff, *What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr*, 97 Tex. L. Rev. Online 63, 68 (2019)). "Thus," the court reasoned,

> a suspect surrendering an unlocked smartphone implicitly communicates, at a minimum, three things: (1) the suspect knows the password; (2) the files on the device exist; and (3) the suspect possessed those files. And, unless the State can show it already knows this information, the communicative aspects of the production fall within the Fifth Amendment's protection.
>
> [*Id.* at ___ (slip op. at 9) (footnote omitted).]

The court noted that "[t]he majority of courts to address the scope of testimony implicated when a suspect is compelled to produce an unlocked smartphone have reached a similar conclusion." *Id.* at ___ n.3 (slip op. at 9) (collecting cases).

Applying that test, the court found in *Seo* the foregone conclusion exception inapplicable. *Id.* at ___ (slip op. at 10). "Even if we assume the State has shown that Seo knows the password to her smartphone," the court wrote, "the State has failed to demonstrate that any particular files on the device exist or that she possessed those files." *Id.* at ___ (slip op. at 9-10). Rather, if law enforcement were granted access to the phone, they "would be fishing for 'incriminating evidence' from the device," such that "Seo's act of producing her unlocked smartphone

would provide the State with information that it does not already know." *Id.* at ___ (slip op. at 10).

After finding that the foregone conclusion exception did not apply, the *Seo* court also noted that "[t]his case highlights concerns with extending the limited foregone conclusion exception to the compelled production of an unlocked smartphone." *Id.* at ___ (slip op. at 11); *see also id.* at ___ (slip op. at 11-17) (explaining those concerns).

A four-Justice majority of the Supreme Court of Pennsylvania likewise focused on the files stored on a computer in considering whether production of the computer's password could be compelled. *See Commonwealth v. Davis*, 220 A.3d 534, 537 (Pa. 2019). The majority noted, "The Commonwealth is seeking the password, not as an end, but as a pathway to the files being withheld." *Id.* at 548. Reasoning that "the compelled production of the computer's password demands the recall of the contents of Appellant's mind, and the act of production carries with it the implied factual assertions that will be used to incriminate him," the court determined "that compelling Appellant to reveal a password to a computer is testimonial in nature" and thus protected by the Fifth Amendment. *Id.* at 548, 551.

The *Davis* majority took note of the foregone conclusion exception but stressed the limited context—document production—in which it has been applied by the United States Supreme Court, as well as the Supreme Court's sharp distinction between the physical and the mental. *Id.* at 548-51. The majority determined that, "until the United States Supreme Court holds otherwise, we construe the foregone conclusion rationale to be one of limited application

and . . . believe the exception to be inapplicable to compel the disclosure of a defendant's password to assist the Commonwealth in gaining access to a computer." *Id.* at 551.

In a footnote, the majority explained, "Even if we were to find that the foregone conclusion exception could apply to the compulsion to reveal a computer password, we nevertheless would conclude that the Commonwealth has not satisfied the requirements of the exception in this matter." *Id.* at 551 n.9. Stressing that "[i]t is not merely access to the computer that the Commonwealth seeks to obtain through compelling Appellant to divulge his computer password, but all of the files on Appellant's computer," and that "[t]he password is merely a means to get to the computer's contents," the majority found that

> because the Commonwealth has failed to establish that its search is limited to the single previously identified file, and has not asserted that it is a foregone conclusion as to the existence of additional files that may be on the computer, which would be accessible to the Commonwealth upon Appellant's compelled disclosure of the password, . . . the Commonwealth has not satisfied the foregone conclusion exception.
>
> [*Ibid.*]

The three-Justice dissent in *Davis* took issue not only with the majority's determination that the foregone conclusion exception is inapplicable in the context of compelled password production, but also with its determination that the exception should not be applied in that case. *Id.* at 552-53 (Baer, J.,

dissenting).

In the dissent's view, "the compulsion of Appellant's password is an act of production, requiring him to produce a piece of evidence similar to the act of production requiring one to produce a business or financial document, as occurred in *Fisher*." *Id.* at 554. The dissent noted that "[a]n order compelling disclosure of the password . . . has testimonial attributes, not in the characters themselves, but in the conveyance of information establishing that the password exists, that Appellant has possession and control of the password, and that the password is authentic, as it will decrypt the encrypted computer files." *Id.* at 555.

Stressing that "[t]he Commonwealth is not seeking the 64-character password as an investigative tool, as occurred in *Hubbell*," but rather "already possesses evidence of Appellant's guilt, which it set forth in an affidavit of probable cause to obtain a warrant to search Appellant's computer," the dissent viewed "the compulsion order as requiring the 'surrender' of Appellant's password to decrypt his computer files"—an act to which "*Fisher's* act-of-production test" and the foregone conclusion rationale would apply. *Ibid.*

The *Davis* dissent then explained why the foregone conclusion exception would apply in that case, contrary to the majority's analysis. *Id.* at 556-58. Notably, the dissent disagreed with the majority's focus on the files that would be made accessible if the password were revealed, reasoning instead

> that the foregone conclusion exception as applied to the facts presented relates not to the computer files, but to the password

itself. Appellant's computer files were not the subject of the compulsion order, which instead involved only the password that would act to decrypt those files. This change of focus is subtle, but its effect is significant. While the government's knowledge of the specific files contained on Appellant's computer hard drive would be central to any claim asserted pursuant to the Fourth Amendment, the same is not dispositive of the instant claim based upon the Fifth Amendment right against self-incrimination, which focuses upon whether the evidence compelled, here, the password, requires the defendant to provide incriminating, testimonial evidence. . . . This Court should not alleviate concerns over the potential overbreadth of a digital search in violation of Fourth Amendment privacy concerns by invoking the Fifth Amendment privilege against self-incrimination, which offers no privacy protection. . . .

Accordingly, I would align myself with those jurisdictions that examine the requisites of the foregone conclusion exception by focusing only on the compelled evidence itself, i.e., the computer password, and not the decrypted files that the password would ultimately reveal.

[*Id.* at 557 (citations omitted) (collecting cases).]

The Florida District Courts of Appeals have similarly splintered when considering the focus of the foregone conclusion analysis and the scope of the exception. In *State v. Stahl*, the court opined that "[t]o know whether providing [a] passcode implies testimony that is a foregone conclusion, the relevant question is whether the State has established that it knows with reasonable particularity that the *passcode* exists, is within the accused's possession or control, and is authentic." 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016).

The court held that the exception applied under the circumstances before it. *Id.* at 136-37. First, the court found that "the State established that the phone could not be searched without entry of a passcode" and that "[a] passcode therefore must exist," as well as that "the phone was [the defendant's] and therefore the passcode would be in [the defendant's] possession." *Id.* at 136. And recognizing that, because "technology is self-authenticating [such that] no other means of authentication may exist," the court also found that "[i]f the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic." *Ibid.*

In *G.A.Q.L. v. State*, another Florida District Court of Appeals viewed the issue differently. 257 So. 3d 1058, 1062-63 (Fla. Dist. Ct. App. 2018). There, the State sought to compel a minor charged with drunk driving "to provide the passcode for [her] iPhone and the password for an iTunes account associated with it." *Id.* at 1060. The court reasoned that "the 'evidence sought' in a password production case such as this is not the password itself; rather it is the actual files or evidence on the locked phone." *Id.* at 1064. In declining to apply the foregone conclusion exception,

the court held that the State "must identify what evidence lies beyond the passcode wall with reasonable particularity" but "fail[ed] to identify any specific file locations or even name particular files that it [sought] from the encrypted, passcode-protected phone." *Id.* at 1064-65; *see also Pollard v. State*, 287 So. 3d 649, 651 (Fla. Dist. Ct. App. 2019) (holding that the "proper legal inquiry . . . is whether the state is seeking to compel a suspect to provide a password that would allow access to information the state knows is on the suspect's cellphone and has described with reasonable particularity").

In *Commonwealth v. Gelfgatt*, the Supreme Judicial Court of Massachusetts took a slightly different view of the authentication element of the foregone conclusion test: "Here, the defendant's decryption of his computers does not present an authentication issue analogous to that arising from a subpoena for specific documents because he is not selecting documents and producing them, but merely entering a password into encryption software." 11 N.E.3d 605, 615 n.14 (Mass. 2014).

The *Gelfgatt* court thus found authentication immaterial and applied the exception in the context of the issue before it: the prosecution's motion to compel a defendant charged with forgery and theft to enter an encryption key[4] in computers lawfully seized by law enforcement. *Id.* at 608, 614. The Supreme Judicial Court held that even though entering an encryption

[4] Encryption keys, like a PIN or passcode, are "essentially a string of numbers or characters" that are applied "to the encrypted data using the algorithm of the given encryption program. By funneling the encrypted data through the algorithm, the data is rendered 'readable' again." *Gelfgatt*, 11 N.E.3d at 610 n.9.

key would be a testimonial communication, "[t]he facts that would be conveyed by the defendant through his act of decryption—his ownership and control of the computers and their contents, knowledge of the fact of encryption, and knowledge of the encryption key—already are known to the government and, thus, are a 'foregone conclusion.'" *Id.* at 615.

Likewise, in *United States v. Apple MacPro Computer*, the United States Court of Appeals for the Third Circuit relied on the district court's fact findings, and affirmed its determination that the compelled decryption of the defendant's devices was not testimonial within the meaning of the Fifth Amendment in light of what the police already knew would be found on those devices. 851 F.3d 238, 248 (3d Cir. 2017).

The Third Circuit pointedly added, however, that it was "not concluding that the Government's knowledge of the content of the devices is necessarily the correct focus of the 'foregone conclusion' inquiry in the context of a compelled decryption order." *Id.* at 248 n.7. "Instead," the court noted, "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." *Ibid.* And the court explained that, "[i]n this case, the fact known to the government that is implicit in the act of providing the password for the devices is 'I, John Doe, know the password for these devices.'" *Ibid.*

Those cases from jurisdictions that have considered the viability of the foregone conclusion exception in the context of compelled decryption or passcode disclosure provide helpful guidance as we

consider the issue before us, a matter of first impression for this Court.

C.

1.

Considering the foregoing in light of the facts of this case, we note first that the State correctly asserts that the lawfully issued search warrants—the sufficiency of which Andrews does not challenge—give it the right to the cellphones' purportedly incriminating contents as specified in the trial court's order. And neither those contents—which are voluntary, not compelled, communications, *see Oregon v. Elstad*, 470 U.S. 298, 306-07 (1985)—nor the 37 phones themselves—which are physical objects, not testimonial communications, *see Pennsylvania v. Muniz*, 496 U.S. 582, 589 (1990)—are protected by the Fifth Amendment privilege against self-incrimination. Therefore, production of Andrews's cellphones and their contents is not barred; indeed, had the State succeeded in its efforts to access the phones, this case would not be before us.

But access to the cellphones' contents depends here upon entry of their passcodes. A cellphone's passcode is analogous to the combination to a safe, not a key. Communicating or entering a passcode requires facts contained within the holder's mind—the numbers, letters, or symbols composing the passcode. It is a testimonial act of production.

2.

The inquiry does not end there, however, because, if the foregone conclusion exception applies, production of the passcodes may still be compelled. To determine the exception's applicability, we must first

determine to what it might apply—the act of producing the passcodes, or the act of producing the cellphones' contents through the passcodes. To be consistent with the Supreme Court case law that gave rise to the exception, we find that the foregone conclusion test applies to the production of the passcodes themselves, rather than to the phones' contents.

The relevant Supreme Court cases explicitly predicate the applicability of the foregone conclusion doctrine on the fundamental distinction between the act of production and the documents to be produced. The documents may be entitled to no Fifth Amendment protection at all—and, indeed, they were not so entitled in *Fisher*—but the act of producing them may nevertheless be protected.

In light of the stark distinction the Court has drawn between the evidentiary object and its production—a division reinforced even in those cases where the foregone conclusion exception was held not to apply—it is problematic to meld the production of passcodes with the act of producing the contents of the phones. As the *Davis* dissent observed, that approach imports Fourth Amendment privacy principles into a Fifth Amendment inquiry.

In *Fisher*, the Supreme Court rejected such importation when it rejected "the rule against compelling production of private papers" set forth in *Boyd v. United States*, 116 U.S. 616 (1886), to the extent the *Boyd* rule "rested on the proposition that seizures of or subpoenas for 'mere evidence,' including documents, violated the Fourth Amendment and therefore also transgressed the Fifth." 425 U.S. at 409. The *Fisher* Court noted that "the foundations for the

[*Boyd*] rule have been washed away" and that "the prohibition against forcing the production of private papers has long been a rule searching for a rationale *consistent with the proscriptions of the Fifth Amendment* against compelling a person to give 'testimony' that incriminates him." *Ibid.* (emphasis added); *see also* Pardo, 90 Iowa L. Rev. at 1882 ("Of the two Amendments, the Fifth Amendment plays the major role in subpoena doctrine. This is due, in part, to the absence of a significant role for the Fourth Amendment."). We agree with the *Davis* dissent that the proper focus here is on the Fifth Amendment and that the Fourth Amendment's privacy protections should not factor into analysis of the Fifth Amendment's applicability.

We also share the concerns voiced by other courts that holding passcodes exempt from production whereas biometric device locks may be subject to compulsion creates inconsistent approaches based on form rather than substance. The distinction becomes even more problematic when considering that, at least in some cases, a biometric device lock can be established only after a passcode is created, calling into question the testimonial/non-testimonial distinction in this context. *See* Kristen M. Jacobsen, Note, *Game of Phones, Data Isn't Coming: Modern Mobile Operating System Encryption and its Chilling Effect on Law Enforcement*, 85 Geo. Wash. L. Rev. 566, 582 (2017).

In sum, we view the compelled act of production in this case to be that of producing the passcodes. Although that act of production is testimonial, we note that passcodes are a series of characters without independent evidentiary significance and are therefore of "minimal testimonial value"—their value

is limited to communicating the knowledge of the passcodes. *See Apple MacPro*, 851 F.3d at 248 n.7. Thus, although the act of producing the passcodes is presumptively protected by the Fifth Amendment, its testimonial value and constitutional protection may be overcome if the passcodes' existence, possession, and authentication are foregone conclusions.

3.

Based on the record before us, we have little difficulty concluding that compelled production of the passcodes falls within the foregone conclusion exception. The 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 Andrews'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.[5] *See Gelfgatt*, 11 N.E.3d at 615. Finally, to the extent that authentication is an issue in this context, the passcodes self-authenticate by providing access to the cellphones' contents. *See Stahl*, 206 So. 3d at 136; *Gelfgatt*, 11 N.E.3d at 615 n.14.

The State's demonstration of the passcodes' existence, Andrews's previous possession and operation of the cellphones, and the passcodes' self-authenticating nature render the issue here one of surrender, not testimony, and the foregone conclusion exception to the Fifth Amendment privilege against

[5] We give deference to the trial court's factual findings and view them as binding upon appeal to the extent that they are "supported by adequate, substantial and credible evidence." *Rova Farms Resort, Inc. v. Inv'rs Ins. Co. of Am.*, 65 N.J. 474, 484 (1974).

self-incrimination thus applies. Therefore, the Fifth Amendment does not protect Andrews from compelled disclosure of the passcodes to his cellphones.

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. *Cf. Apple MacPro*, 851 F.3d at 248 & n.7. The search warrants and record evidence of the particular content that the State knew the phones contained provide ample support for that determination. In short, this was no "fishing expedition." *Cf. Hubbell*, 530 U.S. at 42; Seo, ___ N.E.3d at ___ (slip op. at 10).

Having concluded that the Fifth Amendment's Self-Incrimination Clause does not protect Andrews from government compelled disclosure of the cellphones' passcodes, we turn to state law.

IV.

New Jersey's privilege against compelled self-incrimination is not expressed in its constitution, but the privilege "is deeply rooted in this State's common law and codified in both statute and an evidence rule." *State v. Muhammad*, 182 N.J. 551, 567 (2005).

We begin with the relevant statutes and rules of evidence.

1.

In 1960, the Legislature codified the protection against compelled self-incrimination. *See* L. 1960, c. 152, §§ 18-19. "N.J.S.A. 2A:84A-18 and -19 define[] the right against self-incrimination," but also "set[] forth specific limitations on that right." *In re Grand Jury Proceedings of Guarino*, 104 N.J. 218, 229 n.6 (1986). The statute and corresponding rule of evidence

explicitly afford a suspect the "right to refuse to disclose . . . any matter *that will incriminate* him or expose him to a penalty or a forfeiture of his estate." N.J.S.A. 2A:84A-19; N.J.R.E. 503 (emphasis added).[6] For the right of refusal to apply, therefore, a matter must first be found to be incriminating.

N.J.S.A. 2A:84A-18 and N.J.R.E. 502, in turn, define the circumstances under which a matter will be deemed incriminating:

> [A] matter will incriminate (a) if it constitutes an element of a crime against this State, or another State or the United States, or (b) is a circumstance which with other circumstances would be a basis for a reasonable inference of the commission of such a crime, or (c) is a clue to the discovery of a matter which is within clauses (a) or (b) above . . . .

Applying that definition, we note first that the passcodes are obviously not an element of any crime charged against Andrews. They are only a method of production of or access to the contents of his cellphones. Although disclosure of a passcode is evidence of ownership and control of a cellphone and its contents, the State has already established both of those facts here. The passcodes then, as amalgamations of characters with minimal evidentiary significance,[7] do not themselves support

---

[6] In addition to providing four enumerated exceptions to the right to refuse disclosure, *see* N.J.S.A. 2A:84A-19(a) to (d); N.J.RE. 503(a) to (d), both the statute and the rule specify, through reference to "Rule 37" (renumbered in 1993 as N.J.R.E. 503), that the right may be waived.

[7] Defendant does not claim that the amalgamations of numbers,

an inference that a crime has been committed, nor do they constitute "clues."

Said another way, where ownership and control of an electronic device is not in dispute, its passcode is generally not substantive information, is not a clue to an element of or the commission of a crime, and does not reveal an inference that a crime has been committed. *Cf. State v. Fisher*, 395 N.J. Super. 533, 547-48 (App. Div. 2007) ("The disclosure of one's name and address does not entail a substantial risk of self-incrimination. 'It identifies but does not *by itself* implicate anyone in criminal conduct.'" (emphasis added) (quoting *California v. Byers*, 402 U.S. 424, 434 (1971))).

We turn, therefore, to New Jersey common law.

2.

New Jersey's common law privilege against self-incrimination "generally parallels federal constitutional doctrine," *State v. Chew*, 150 N.J. 30, 59 (1997), but also "offers broader protection than its federal counterpart under the Fifth Amendment," *Muhammad*, 182 N.J. at 568; *accord Guarino*, 104 N.J. at 229. Our privilege derives from the notion of personal privacy established by the United States Supreme Court in *Boyd*. *Guarino*, 104 N.J. at 230.

In *Boyd*, decided in 1886, the Court considered whether the production of private papers could be compelled and determined that "a compulsory production of the private books and papers of the

---

letters, or symbols constituting his passcodes have independent evidentiary significance. Such a claim would not, in any event, change the outcome here in light of the limitations set forth in the trial court's disclosure order.

owner of goods sought to be forfeited in such a suit is" not only "compelling him to be a witness against himself, within the meaning of the Fifth Amendment to the Constitution," but also "is the equivalent of a search and seizure—and an unreasonable search and seizure—within the meaning of the Fourth Amendment." 116 U.S. at 634-35.

As noted above, the *Fisher* Court overturned that rule in the context of federal constitutional analysis. *See* 425 U.S. at 407 (explaining that "[s]everal of Boyd's express or implicit declarations have not stood the test of time" and listing examples, including private documents); *see also Doe I*, 465 U.S. at 618 (O'Connor, J., concurring) ("[T]he Fifth Amendment provides absolutely no protection for the contents of private papers of any kind. The notion that the Fifth Amendment protects the privacy of papers originated in [*Boyd*], but our decision in [*Fisher*] sounded the death knell for *Boyd*."); Pardo, 90 Iowa L. Rev. at 1858 ("Subsequent doctrinal developments have torpedoed *Boyd's* view of the overlap [between the Fourth and Fifth Amendments] as the Court has systematically rejected and cabined *Boyd's* holding.").

In *Guarino*, this Court considered as a matter of first impression whether Fisher's overthrow of *Boyd's* private-papers rule would affect New Jersey law. 104 N.J. at 231. The *Guarino* Court "affirm[ed] our belief in the *Boyd* doctrine and [held] that the New Jersey common law privilege against self-incrimination protects the individual's right 'to a private enclave where he may lead a private life.'" *Ibid.* (quoting *Murphy v. Waterfront Comm'n*, 378 U.S. 52, 55 (1964)). Thus, despite the shift at the federal level, our common law privilege continues to consider whether evidence requested is of an inherently private

nature.

The *Guarino* Court articulated the relevant test as follows:

> To determine whether the evidence sought by the government lies within that sphere of personal privacy a court must look to the "nature of the evidence." *Couch v. United States*, 409 U.S. 322, 350 (1973) (Marshall, J., dissenting). In the case of documents, therefore, a court must look to their contents, not to the testimonial compulsion involved in the act of producing them, as the Supreme Court has done in *Fisher* and *Doe*. Neither *Fisher* nor *Doe* recognize the fundamental privacy principles underlying the New Jersey common-law privilege against self-incrimination. Thus, in defining the scope of our common-law privilege, we decline to follow the Court's rationale for its *Doe* decision.
>
> [*Id.* at 231-32.]

In other words, in contrast to federal law which distinguishes between Fourth and Fifth Amendment inquiries, New Jersey's common law views the privilege against self-incrimination as incorporating privacy considerations.

Noting as much gives us our answer here. The constitutional privacy considerations, *see* U.S. Const. amend. IV; N.J. Const. art. I, ¶ 7, that would apply to those portions of the cellphones' contents of which disclosure has been ordered have already been considered and overcome through the unchallenged

search warrants granted in this case. As we noted in the federal context, whether the inquiry is limited here to the passcodes or extended to the phones' contents, the result is the same.

We thus agree with the Appellate Division that New Jersey's common law and statutory protections against compelled self-incrimination do not apply here.

V.

For the reasons set forth above, neither federal nor state protections against compelled disclosure shield Andrews's passcodes. We therefore affirm the Order of the Appellate Division compelling Andrews's disclosure of the passcodes to his cellphones seized consistent with the trial court's order of production, and remand to the trial court for further proceeding

CHIEF JUSTICE RABNER and JUSTICES PATTERSON and FERNANDEZ-VINA join in JUSTICE SOLOMON's opinion. JUSTICE LaVECCHIA filed a dissent, in which JUSTICES ALBIN and TIMPONE join.

JUSTICE LaVECCHIA, dissenting.

In a world where the right to privacy is constantly shrinking, the Constitution provides shelter to our innermost thoughts—the contents of our minds—from the prying eyes of the government. The right of individuals to be free from the forced disclosure of the contents of their minds to assist law enforcement in a criminal investigation, until now, has been an inviolate principle of our law, protected by the Fifth Amendment and our state common law. No United States Supreme Court case presently

requires otherwise. No case from this Court has held otherwise. That protection deserves utmost respect and should not be lessened to authorize courts to compel a defendant to reveal the passcode to a smartphone so law enforcement can access its secured contents.

We are at a crossroads in our law. Will we allow law enforcement—and our courts as their collaborators—to compel a defendant to disgorge undisclosed private thoughts—presumably memorized numbers or letters—so that the government can obtain access to encrypted smartphones? In my view, compelling the disclosure of a person's mental thoughts is anathema to fundamental principles under our Constitution and state common law.

The Court's outcome deviates from steadfast past principles protective of a defendant's personal autonomy in the face of governmental compulsion in a criminal matter. Those same principles should apply even in the face of the latest challenge presented by new technology. Respectfully, I dissent from the course the Court now takes.

I.

The facts that set up the pivotal legal question in this matter are these. Defendant Robert Andrews, a former law enforcement officer in the Essex County Sheriff's Department, was suspected of helping a drug dealer named Quincy Lowery in Lowery's criminal scheme. Lowery knew Andrews through their joint interest in a motorcycle club. Lowery made the accusations that led to Andrews's investigation when Lowery began cooperating with police to gain benefit after being charged as part of a larger narcotics

investigation.

The State obtained Lowery's phone by consent. According to Lowery, although some messages were deleted, his phone showed telephone calls and messages between him and Andrews. In the course of its investigation, the State seized two phones from Andrews and obtained a warrant to search them after Andrews refused to consent to a search. One phone was listed as Andrews's personal cell phone and registered to his home address. The other phone was subscribed to by Kay Transportation, LLC, a business with which Andrews presumably was associated, although its address is not listed as Andrews's home. Both phones were on him when seized.

Although the scope of the warrant to search the two phones contains no substantive limit on its face, its scope was later narrowed to permit a search of the phone icon and the message icon. There was no restriction to control with whom a conversation took place or the time periods within which a message or phone call took place. The two aforementioned limitations were imposed by the court during proceedings on the State's motion to compel discovery of the passcodes to the phones.[1] According to the State, it could not then, or even by the time of argument before our Court, access the phones' contents, nor could Apple, the manufacturer of these iPhones, or the Federal Bureau of Investigation. The State also represents that no service company has been able to help it gain access.

Andrews resisted the State's motion, claiming a

[1] Hereinafter, we refer either to a passcode or personal identification number (PIN) as the means to unlock and decrypt these smartphones' security systems.

violation of the Fifth Amendment, as well as New Jersey common law and law governing privilege, to wit: N.J.S.A. 2A:84A-19 and Evidence Rules 501 and 503. Also, according to Andrews, the State waited two years to seek the passcodes; the State does not know what phone the sought-after information is on or where it is located; nor does it know with any particularity what information on the phones will provide evidence of criminality.

The motion court granted the motion to compel, and, on interlocutory review, the Appellate Division affirmed.

We are reviewing the Appellate Division's judgment, at which the court arrived by concluding that the forced disclosure of the passcode is a testimonial act for purposes of a Fifth Amendment analysis, but applying an exception (identified as "foregone conclusion") to avoid finding a constitutional violation. The Appellate Division also rejected all state law arguments that Andrews advanced.

This Court's majority opinion conveys the essence of the motion court and Appellate Division rulings, so, to avoid repetition, I turn directly to why I believe it to be error to sustain the compelled disclosure of presumably memorized passcodes to these smartphones under the Fifth Amendment or state law.

II.

A.

The Fifth Amendment of the United States Constitution provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." U.S. Const. amend. V. The privilege extends

beyond compelled incriminatory testimony given in court to include other forced testimony that "would furnish a link in the chain of evidence needed to prosecute the claimant." *United States v. Hubbell*, 530 U.S. 27, 38 (2000) (quoting *Hoffman v. United States*, 341 U.S. 479, 486 (1951)). In the Court's seminal decision of *Boyd v. United States*, it was recognized that "a compulsory production of the private books and papers of [an individual] is compelling him to be a witness against himself, within the meaning of the Fifth Amendment to the Constitution." 116 U.S. 616, 634-35 (1886).

Boyd was rooted in a privacy rationale that prevents "the invasion of [one's] indefeasible right of personal security, personal liberty and private property." *Id.* at 630. Its privacy principle was maintained for decades and reinforced in *Couch v. United States*. *See* 409 U.S. 322, 327 (1973) (explaining that the Fifth Amendment "respects a private inner sanctum of individual feeling and thought"—an inner sanctum that necessarily includes an individual's papers and effects to the extent that the privilege bars their compulsory production and authentication—and "proscribes state intrusion to extract self-condemnation").

The precept that one's inner thoughts cannot be compelled to be disclosed because they are protected by the Fifth Amendment privilege against self-incrimination is still an accepted United States Supreme Court principle. The Supreme Court's continuous assertion of that principle about compelled production of information stored in the mind, even as recently as in its 2000 majority opinion in *Hubbell*, 530 U.S. at 43, provides the polestar in this matter. Although that polestar has apparently been not as

bright for some courts when addressing law enforcement efforts to force an individual to reveal passcodes for encrypted devices like the smartphones here, creating a divide in the jurisprudence in the federal and state courts, I see no basis to depart from that core Fifth Amendment principle.

The divide is rooted in applications of the altered analysis developed by the Supreme Court during the 1970s and 1980s, concerning the production of physical documents, leading to, among other things, a one-time application of an "exception" called "foregone conclusion." Although that exception has not been applied again by the Supreme Court, the aforementioned jurisprudential split exists because some courts have expansively, and in various ways, applied that concept to excuse alleged violations of the privilege against self-incrimination in applications of forced disclosure of mentally cached passcodes to bypass security for new technology. But, for me, there is no real difference between forcing one to divulge the mentally stored combination of a safe—the very example that the Supreme Court has used, more than once, as a step too far in ordering a defendant to assist in his or her own prosecution—and forcing one to divulge the passcode to a smartphone. A recitation of that relevant Supreme Court precedent follows.

B.

It is well established that to fall within the self-incrimination privilege, an individual must show that the evidence is compelled, testimonial, and self-incriminating. *Hubbell*, 530 U.S. at 34-35. An order to compel a defendant to produce documents implicates the Fifth Amendment and, originally, the Supreme Court interpreted the Fifth Amendment as protecting

all private papers. *Boyd*, 116 U.S. at 630-32. That was altered in *Fisher v. United States*, 425 U.S. 391 (1976).

With its decision in *Fisher*, the Court shifted from a blanket protection for private papers to a new paradigm for evaluating a self-incrimination claim involving the production of *existing* documents—documents which, because they already existed, were not themselves testimonial. *Id.* at 409-10. The analysis thus turned from the content of the document to an examination of the act of production of documents, hence becoming known as the act of production doctrine. The Court's *Fisher* decision held that the act of producing documents in response to a government subpoena could be testimonial if the act of production used the contents of the mind and revealed, either explicitly or implicitly, the existence, possession and control, or authenticity of the physical documents. *Id.* at 410-13. Thus, the facts in *Fisher* require attention.

Fisher involved consolidated cases in which the defendants, in each, were involved in an IRS investigation into possible civil or criminal federal tax liability. *Id.* at 393-94. The taxpayers retrieved documents from their accountants related to the accountants' preparation of their tax returns, which the taxpayers then shared with their lawyers. *Id.* at 394. When the lawyers were served with summonses from the IRS directing them to produce the accounting documents in question, they declined. *Id.* at 394-95. After differing results in the circuit courts, the Supreme Court granted certiorari.

Focusing on the act of "'physical or moral compulsion' exerted on the person asserting the privilege," the Court did not find the necessary

personal compulsion and declined to extend Fifth Amendment protection to the compelled production of the documents. *Id.* at 397 (quoting *Perlman v. United States*, 247 U.S. 7, 15 (1918); other citations omitted). The Court observed that the documents could be obtained without action from the accused, adding that the subpoena to the taxpayers' lawyer had no authority to compel the taxpayer to provide incriminating information against himself. *Id.* at 398 ("It is extortion of information from the accused himself that offends our sense of justice." (quoting *Couch*, 409 U.S. at 328)). The documents in question were not prepared by the taxpayers, did not contain testimonial declarations by the taxpayers, and were prepared in an entirely voluntary manner. *Id.* at 409. Because production of the documents would not "compel the taxpayer to restate, repeat, or affirm" the contents of those documents, the Court determined that compulsion to produce them was not testimonial. *Ibid.*

Importantly, the Court acknowledged that whether the Fifth Amendment lends its protection to the documents in question could not be answered without considering whether responding to a subpoena is itself communicative. *Id.* at 410. "Compliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer. It also would indicate the taxpayer's belief that the papers are those described in the subpoena." *Ibid.* However, that was not found to exist on the facts presented, as the subpoena was served on the lawyer. *Id.* at 410-11.

The Court's new framework and its application in *Fisher* led the Court to establish the foregone conclusion doctrine. That doctrine was described as

providing that if the government can demonstrate that the existence, possession or control, and authenticity of the identified documents or materials it seeks are a foregone conclusion, then the act of production itself "adds little or nothing to the sum total of the Government's information" because the government is not relying on the veracity of the statement implicit in the act of production to prove the existence, possession or control, or authenticity of the documents. *Ibid.* Ultimately, the Court stated, "[t]he question is not of testimony but surrender." *Id.* at 411 (quoting *In re Harris*, 221 U.S. 274, 279 (1911)).

The Court expanded on the notion that the response to a subpoena itself could be incriminating in *United States v. Doe (Doe I)*, 465 U.S. 605 (1984). There the Court had to determine whether bank statements, phone records, and other business records of a sole proprietor of a business could be compelled for production. *Id.* at 606-07. Doe was the owner of several sole proprietorships. *Id.* at 606. During the course of investigating "corruption in the awarding of county and municipal contracts," a grand jury issued subpoenas attempting to compel Doe to provide telephone, business, and bank records pertaining to his companies. *Id.* at 606-07. Doe filed a motion in the District Court of New Jersey requesting that the subpoenas be quashed, and the court granted the motion, stating that "the relevant inquiry is . . . whether the act of producing the documents has communicative aspects which warrant Fifth Amendment protection." *Id.* at 607-08 (quoting *In re Grand Jury Empanelled March 19, 1980*, 541 F. Supp. 1, 3 (D.N.J. 1981)). The United States Court of Appeals for the Third Circuit affirmed. *Id.* at 608.

The Supreme Court held that such production is protected by the Fifth Amendment because the government was not certain the defendant actually possessed and/or controlled those documents. The Court again noted that "[a]lthough the contents of a document may not be privileged, the act of producing the document may be." *Id.* at 612. Producing documents would indicate that the defendant possesses them, controls them, and believes them to be the documents requested. *Id.* at 613 & n.11. Relying on the Third Circuit's assessment that there was "nothing in the record that would indicate that the United States knows, as a certainty, that each of the myriad documents demanded by the five subpoenas in fact is in the [defendant's] possession or subject to his control," *id.* at 613 n.12 (quoting *In re Grand Jury Empanelled March 19, 1980*, 680 F.2d 327, 335 (3d Cir. 1982)), the Court upheld the determination that the act of producing the documents was testimonial, *id.* at 614. As the Court emphasized, "the Government, unable to prove that the subpoenaed documents exist—or that [Doe] even is somehow connected to the business entities under investigation—is attempting to compensate for its lack of knowledge by requiring [Doe] to become, in effect, the primary informant against himself." *Id.* at 613 n.12 (quoting *In re Grand Jury Empanelled March 19, 1980*, 680 F.2d at 335). Ultimately, the Court held that although the contents of the underlying documents were not privileged, the State could not compel defendant to provide them because "[t]he act of producing the documents at issue in this case is privileged and cannot be compelled without a statutory grant of use immunity pursuant to 18 U.S.C. §§ 6002 and 6003." *Id.* at 617.

Completing the trilogy of cases in this vein, four years later, the Court issued a decision in the case known colloquially as *Doe II*. *Doe v. United States*, 487 U.S. 201 (1988). There, the Court answered the question of "whether a court order compelling a target of a grand jury investigation to authorize foreign banks to disclose records of his accounts, without identifying those documents or acknowledging their existence, violates the target's Fifth Amendment privilege against self-incrimination." *Id.* at 202. Doe was the target of a federal grand jury investigation into suspected "fraudulent manipulation of oil cargoes and receipt of unreported income." *Ibid.* The grand jury issued a subpoena and Doe was directed to produce records of transactions at three specific banks in Bermuda and the Cayman Islands. *Ibid.* Doe produced some records, but when asked about whether there were other records and where they might be, he invoked his Fifth Amendment privilege against self-incrimination. *Id.* at 202-03. When Doe invoked his Fifth Amendment rights, the United States branches of the foreign banks were also served with subpoenas attempting to compel them to produce the responsive documents. *Id.* at 203. Because the banks were subject to their governments' privacy and secrecy laws and refused to comply with the subpoena, the government attempted to compel Doe to sign twelve forms that would permit release by the banks of any records relating to twelve foreign accounts the Government "knew or suspected" Doe controlled. *Ibid.*

The Supreme Court upheld the subpoena's enforcement, refining the issue to be whether compelling Doe to sign the form was a "testimonial communication." *Id.* at 207. The Court's analysis emphasized that "[i]t is consistent with the history of

and the policies underlying the Self- Incrimination Clause to hold that the privilege may be asserted only to resist compelled explicit or implicit disclosures of incriminating information." *Id.* at 212.

Scrutinizing the form the defendant was forced to sign, the Court noted that it was "carefully drafted not to make reference to a specific account," and did "not acknowledge that an account in a foreign financial institution is in existence or that it is controlled by petitioner," "indicate whether documents or any other information relating to petitioner are present at the foreign bank, assuming that such an account does exist," or "even identify the relevant bank." *Id.* at 215. The Court concluded that the act of signing the form was not testimonial. *Ibid.* The Court was untroubled by Doe being compelled to sign the form because "[b]y signing the form, Doe makes no statement, explicit or implicit, regarding the existence of a foreign bank account or his control over any such account." *Id.* at 215-16. The Court concluded that the form did not direct the government to evidence; rather, it simply provided access to evidence if the government could independently find it. *Id.* at 215.

In *Doe II*, there is passing reference to the foregone conclusion doctrine, but it is not used in the Court's analysis. *Ibid.* Indeed, it has never again been used by the Supreme Court, and was even questioned in a later case, as well as in separate opinions, making *Doe II* the end point of Supreme Court cases leaving the door open to the use—let alone expansion—of that doctrine. *See Hubbell*, 530 U.S. at 44, 49-50; *see also Seo v. State*, ___ N.E.3d ___, ___ (slip op. at 7) (Ind. 2020) (similarly observing that "*Fisher* was the first, and only, Supreme Court decision to find that the

testimony implicit in an act of production was a foregone conclusion. In contrast, the government failed to make that showing in the other two relevant decisions: [*Doe I* and *Hubbell*].").

Further—and, importantly, foreshadowing a seeming retrenchment of that troika of Fifth Amendment cases—Justice Stevens disagreed with the Court's decision in *Doe II*. 487 U.S. at 219-21 (Stevens, J., dissenting). He aptly noted:

> A defendant can be compelled to produce material evidence that is incriminating. Fingerprints, blood samples, voice exemplars, handwriting specimens, or other items of physical evidence may be extracted from a defendant against his will. But can he be compelled to use his mind to assist the prosecution in convicting him of a crime? I think not. He may in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe—by word or deed.
>
> [*Id.* at 219.]

Justice Stevens's analogy to disclosure of a memorized combination to a wall safe harkened back to the basic principle that the contents of one's mind are protected from compulsion under the Fifth Amendment.

Borrowing from the sound logic of that dissent in *Doe II*, the Court in *Hubbell* paused in continuing down this act-of-production line of cases. In *Hubbell*, the Court considered "whether the Fifth Amendment

privilege protects a witness from being compelled to disclose the existence of incriminating documents that the Government is unable to describe with reasonable particularity," and whether the produced documents can be used to "prepare criminal charges" "if the witness produces such documents pursuant to a grant of immunity." 530 U.S. at 29-30 (footnote omitted).

Hubbell, the witness in question, had pled guilty to mail fraud and tax evasion relating to his billing practices while at a law firm in Arkansas. *Id.* at 30. In his plea agreement, Hubbell agreed to cooperate in an investigation into claims of federal law violation relating to the Whitewater Development Corporation. *Ibid*. While serving the sentence imposed as a result of his plea agreement, Hubbell was served with a subpoena for several categories of documents. *Id.* at 31. He invoked his Fifth Amendment privilege and refused to comply. *Ibid*.

After he was offered immunity pursuant to 18 U.S.C. § 6003(a), Hubbell produced thousands of pages of requested documents and records. *Ibid*. Those documents led to incriminating information that spawned a second prosecution for unrelated wire fraud and other tax-related crimes. *Ibid*. The District Court dismissed the indictment, in part because the "use of the subpoenaed documents violated [18 U.S.C.] § 6002 because all of the evidence" that would be offered against Hubbell would be derived "from the testimonial aspects of respondent's immunized act of producing those documents." *Id.* at 31-32. The Court of Appeals for the District of Columbia vacated the judgment and remanded for further proceedings. *Id.* at 32.

In the Supreme Court's analysis, written by Justice Stevens, the question was framed as whether "incriminating information derived directly or indirectly from the compelled testimony" was protected by the Fifth Amendment. *Id.* at 38. In fact, more narrowly, the Government was not intending to use the act of producing the documents and records against defendant at trial, but rather the information the underlying documents conveyed. *Id.* at 41.

The Court concluded that the government had made "derivative use" of the material, and that "[i]t is apparent from the text of the subpoena itself that the prosecutor needed respondent's assistance both to identify potential sources of information and to produce those sources." *Ibid.* The Court distinguished its analysis from that used in *Fisher*, noting:

> *Whatever the scope of this "foregone conclusion" rationale*, the facts of this case plainly fall outside of it. While in *Fisher* the Government already knew that the documents were in the attorneys' possession and could independently confirm their existence and authenticity through the accountants who created them, here the Government has not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent. The Government cannot cure this deficiency through the overbroad argument that a businessman such as respondent will always possess general business and tax records that fall within the broad

categories described in this subpoena.

[*Id.* at 44-45 (emphasis added).]

The Court ultimately determined "that the constitutional privilege against self-incrimination protects the target of a grand jury investigation from being compelled to answer questions designed to elicit information about the existence of sources of potentially incriminating evidence." Id. at 43. Given the breadth and depth of the requested documents, the Court concluded that the defendant's response was the "functional equivalent of the preparation of an answer to either a detailed written interrogatory or a series of oral questions at a discovery deposition," id. at 41-42, and it was "abundantly clear" to the Court that ubbell's compelled production of the documents was the catalyst to his eventual second prosecution, id. at 42. Notably, the Court stated that the government's "fishing expedition," id. at 42, was more akin to compelling someone to provide the combination to a safe than the key to a lockbox, id. at 43. Thus, the Court resorted once again to the invariable Fifth Amendment protection that must shield inquisitions into mentally cached information or thought processes. *Ibid.*[2]

---

[2] In a separate opinion, Justice Thomas questioned whether the act-of-production doctrine originating in *Fisher* is itself consistent with the original meaning of the self-incrimination protection enshrined in the Fifth Amendment. *Hubbell*, 530 U.S. at 49 (Thomas, J., concurring). He expressed, joined by the late Justice Scalia, a willingness to reconsider that decision's narrowing of the protection against compelled evidence in light of the Fifth Amendment's historical meaning and scope. *Ibid.* However, because the issue was not raised by the parties, the concurring Justices declined to address at that time whether the Fifth Amendment has "a broader reach than *Fisher* holds,"

C.

From those Supreme Court decisions involving production of physical documents, state courts and the federal circuits differ in their efforts to apply the act-of-production doctrine to the forced disclosure of a PIN or password to bypass security and obtain access to the contents of an encrypted device.

There appears near unanimity in recognizing that in compelling disclosure of a passcode the compelled individual must use his or her mind and, further, that the act provides at least inferences about the existence, possession or control, and authenticity of the material or documents sought by the government. *Seo*, ___ N.E.3d at ___, ___ n.3 (slip op. at 8-9, 9 n.3). Thus, the cases agree that an act of production is involved in compelling disclosure of a passcode.

The decisions splinter, however, over what the compelled act produces, and that decision relatedly affects what those courts hold the government must establish in order for the foregone conclusion exception to apply. Some courts hold that the order for decryption seeks only the password. *See, e.g., State v. Stahl*, 206 So. 3d 124, 133 (Fla. Dist. Ct. App. 2016); *Commonwealth v. Jones*, 117 N.E.3d 702, 714 (Mass. 2019); *see also United States v. Apple MacPro Comput.*, 851 F.3d 238, 248 n.7 (3d Cir. 2017) (suggesting without deciding that the password is the proper focus). Other courts find such orders indistinguishable from compelling production of the documents and materials housed on the encrypted device. *See, e.g., United States v. Doe (In re Grand*

---

although suggesting that it may. *Id.* at 56.

Jury Subpoena Duces Tecum dated March 25, 2011), 670 F.3d 1335, 1346 (11th Cir. 2012) (analogizing decryption to the production of a combination to a safe because it uses the contents of the defendant's mind and implies factual statements about the defendant's connection to the contents on encrypted devices); *G.A.Q.L. v. State*, 257 So. 3d 1058, 1062 (Fla. Dist. Ct. App. 2018); *Seo*, ___ N.E.3d at ___ (slip op. at 8) (describing the act of production as continuing to link the means of production to the documents ultimately produced).

In *Seo v. State*, the Indiana Supreme Court recently addressed the constitutional implications of compelling an individual to produce the passcode to his or her locked smartphone, holding such compulsion would violate one's Fifth Amendment privilege against self-incrimination. ___ N.E.3d at ___ (slip op. at 2). While *Seo* addressed the Fifth Amendment question with respect to a subpoena that would have allowed an unlimited search of the contents of a woman's phone, the court in *Seo* highlighted the inapplicability of the foregone conclusion doctrine in the context of smartphones generally. *Id.* at ___ (slip op. at 9-17).

The *Seo* opinion astutely observed that "production of an unlocked smartphone is unlike the compelled production of specific business documents." Id. at ___ (slip op. at 11). The *Seo* court noted that even the Supreme Court in Fisher recognized the difference between subpoenas that sought business "documents of unquestionable relevance to the tax investigation," and subpoenas of more personal documents, which might present "[s]pecial problems of privacy." *Id.* at ___ (slip op. at 11) (alteration in original) (quoting *Fisher*, 425 U.S. at 401 n.7). Importantly, the *Seo*

decision conveys the Indiana Supreme Court's reasons for being wary of employing the foregone conclusion exception, citing among those reasons both its questionable viability and that it was crafted for a different context. *Id.* at ___ (slip op. at 11-17). The *Seo* court ultimately found that it would be "imprudent" to adopt the foregone conclusion exception to permit the State to compel a defendant to disclose a smartphone's passcode. *Id.* at ___ (slip op. at 14). It is not the only recent case to have not walked down the "foregone conclusion" path. *See id.* at ___ n.7 (slip op. at 16 n.7).

The United States Supreme Court has not addressed the differences that have developed from courts applying the act-of-production analytic framework—developed in the context of the compelled production of books, records, and physical documents—to encrypted devices.[3]

---

[3] Decisions splintering over the testimonial nature of the compelled disclosure of passcodes have fostered further splits concerning compelled use of biometrics to decrypt devices, with courts' views about the testimonial nature of compelled disclosure of a passcode informing the analysis regarding biometrics. *Compare In re Search of a Residence in Oakland, Cal.*, 354 F. Supp. 3d 1010, 1015-16 (N.D. Cal. 2019) (finding that compelled production of biometric data was testimonial for Fifth Amendment purposes in the context of a warrant application seeking permission to compel fingerprint or facial recognition device unlocking), and *In re Application for a Search Warrant*, 236 F. Supp. 3d 1066, 1073-74 (N.D. Ill. 2017) (same as to forced fingerprint device unlocking), with *In re the Search of: A White Google Pixel 3 XL Cellphone in a Black Incipio Case*, 398 F. Supp. 3d 785, 793-94 (D. Idaho 2019) (finding that a forced application of a fingerprint to unlock a device was not testimonial for Fifth Amendment purposes), and *In re Search of [Redacted] Washington, D.C.*, 317 F. Supp. 3d 523, 539 (D.D.C. 2018) (same).

D.

Until the Court clarifies its intentions about application of the act of production doctrine in this setting, I would follow the only sure directional signs the Court has given—the same themes I introduced at the outset of this analytic section.

First, the forced disclosure of mentally cached information that represents the contents of one's mind is violative of the Fifth Amendment's protections. The Court's recurring metaphor of the combination to a safe, unmistakably included in the majority opinion in *Hubbell*, harkens back to the classic notion, first expressed in *Boyd*, that the Fifth Amendment has roots in protection of personal autonomy from government compulsion. It signals, for me, the Court's unwillingness to hold that the Fifth Amendment permits the government to compel one's inner held thoughts in order to assist in one's own prosecution. The memorized passcode is classic contents-of-mind material. *See Seo*, ___ N.E.3d ___ (slip op. at 9). It is simply off limits under the Fifth Amendment.

To the extent that *Fisher* created an act-of-production analysis for use in considering, from a Fifth Amendment perspective, the government's efforts to obtain already existing physical documents, I would not expansively apply that precedent to permit it to force disclosure of the contents of one's mind, as is required in the application involved in this matter. The government should not be permitted to force defendant to cooperate in his own prosecution by obtaining, through his entry of passcodes, access to information the government believes will be incriminating. The government may have a search warrant for the phones' contents, and it may

physically have the phones. But, like the wall safe, the government has to obtain access in a way other than compelling defendant into providing the PIN or passcode to obtain access. That testimonial act—an act of compelled cooperation in his own prosecution—is a step beyond what *Hubbell* says is required. *See Hubbell*, 530 U.S. at 43-44.

Second, I would not adopt and apply the foregone conclusion exception, which, at last word, the Court has declined to use and has questioned what it even means. *See id.* at 44, 49-50. In my judgment, the single use of the descriptor "foregone conclusion" in reference to the documents the Supreme Court found unprotected by the self-incrimination privilege in *Fisher* does not merit its current status as a "doctrine" deserving of expansive use outside of the original tax document setting in which it was first mentioned. *Cf. Seo*, ___ N.E.3d ___ (slip op. at 15-16) (questioning the exception's viability outside of its original context).[4]

---

[4] The Indiana Supreme Court gave sound reasons for being wary about the exception's viability, let alone expanding it.

> The limited, and questionable, application of the foregone conclusion exception also cautions against extending it further. Indeed, *Fisher* was decided over forty-four years ago, and it remains the lone U.S. Supreme Court decision to find that the exception applied. In the intervening years, the Court has discussed it twice and in only one context: in grand jury proceedings when a subpoena compelled the production of business and financial records. During this same time period, legal scholars—including three current members of the Supreme Court—have wondered whether *Fisher* interpreted the Fifth Amendment too narrowly, calling into question the viability of the foregone conclusion exception itself. *See Hubbell*, 530 U.S.

The exception's only use by the Court in *Fisher* does not resemble its application to information on an encrypted device. *Id.* at ___ (slip op. at 11- 12). The exception originated in the setting of the government ferreting out already existing, physical documents held by another person. It requires expansion to be used here. Its lineage does not merit its use in the present context of overriding the privilege to keep one's thoughts and recollections to one's self and not turn that over to the government for use in easing its investigatory efforts. Other courts also have recently declined to apply it or have not even acknowledged it when addressing how the Fifth Amendment applies to compelled disclosure of the passcode to an encrypted smartphone. *See, e.g., Commonwealth v. Davis*, 220 A.3d 534, 550 (Pa. 2019) and other cases cited in *Seo*,

---

at 49-56 (Thomas, J., concurring); *Carpenter v. United States*, 585 U.S. ___, 138 S. Ct. 2206, 2271 (2018) (Gorsuch, J., dissenting); Samuel A. Alito, Jr., *Documents and the Privilege Against Self-Incrimination*, 48 U. Pitt. L. Rev. 27, 45- 51 (1986); *see also*, e.g., Bryan H. Choi, *The Privilege Against Cellphone Incrimination*, 97 Tex. L. Rev. Online 73, 74 n.6 (2019); Richard A. Nagareda, *Compulsion "To Be a Witness" and the Resurrection of* Boyd, 74 N.Y.U. L. Rev. 1575, 1606 & nn.124-25 (1999); Robert Heidt, *The Fifth Amendment Privilege and Documents—Cutting Fisher's Tangled Line*, 49 Mo. L. Rev. 439, 443 (1984). Regardless of the foregone conclusion exception's viability, it seems imprudent to extend it beyond its one-time application. *Cf. Silverman v. United States*, 365 U.S. 505, 510, 512 (1961) (deciding not to extend the rationale of a factually distinct case "by even a fraction of an inch").

[*Seo*, ___ N.E.3d at ___ (slip op. at 15-16).]

___ N.E.3d at ___ (slip op. at 16 n.7).[5]

Rather, I would adhere to the Court's bright line: the contents of one's mind are not available for use by the government in its effort to prosecute an individual. The private thoughts, ideas, and information retained in one's mind are not subject to compelled recollection and disgorgement for use in a person's own prosecution. That practice, reminiscent of an inquisition, was abolished by the Fifth Amendment's inclusion in the Constitution and was as certainly forbidden through the common law of this state from its earliest times.

In sum, I would hold that the Fifth Amendment was properly invoked by defendant when resisting the State's motion to compel the passcodes. In my view, it is error to affirm the Appellate Division judgment. Further, I would not rest that determination on the application of federal constitutional principles alone.

Defendant also claims he is protected under State law from being compelled by judicial order to disclose the passcode to decrypt the secured contents of phones seized in the government's investigation of him. In my view, his claim is right.

---

[5] *See, e.g., United States v. Jimenez*, 419 F. Supp. 3d 232, 233 (D. Mass. 2020) (denying the government's motion to compel the defendant to disclose his smartphone passcode because it "would force defendant to 'disclose the contents of his own mind'"); *In re Search of a Residence in Oakland, Cal.*, 354 F. Supp. 3d at 1016-18 (relying on the Supreme Court's proposition in Riley v. California, 573 U.S. 373, 393-97 (2014), that phones are entitled to greater privacy protection in concluding that the foregone conclusion doctrine should not be applied in the context of mobile phones).

III.

A.

New Jersey has historically provided broad protection against self-incrimination through our common law, rules of evidence, and statutes. This expansive protection has been recognized as exceeding that which is provided under federal law. *See State v. Hartley*, 103 N.J. 252, 286 (1986). And we have never suggested any malleability in the steadfastly rigorous protection of the privilege because it is not codified in the State Constitution—an act viewed as unnecessary in light of the revered status of the privilege from the earliest of days in New Jersey. *State v. Fary*, 19 N.J. 431, 434-35 (1955); *see also State v. Zdanowicz*, 69 N.J.L. 619, 622 (E. & A. 1903).[6]

---

[6] In making an observation about the uncertainty of the Fifth Amendment's reach, our predecessor Court observed:

> It is not deemed necessary to consider whether this [Fifth Amendment] constitutional provision will operate to prevent any state, if it is conceivable that any state should desire to do so, from enacting laws establishing a practice in criminal cases such as is in vogue in countries not following the course of the common law, or permitting an accused person to be subject to such compulsion as may be exerted by harassing examination or other means, forcible or practically forcible, compelling him to testify against himself, or to prevent the adoption by any state of a practice which might produce that effect.
>
> Although we have not deemed it necessary to insert in our constitution this prohibitive provision, the common law doctrine, unaltered by legislation or by lax practice, is by us deemed to

Under our present Rules of Evidence and their counterparts codified in law, the protection against self-incrimination provides: "Every person has in any criminal action in which he is an accused a right not to be called as a witness and not to testify." N.J.S.A. 2A:84A-17(1); N.J.R.E. 501. New Jersey's privilege applies "in any . . . proceeding . . . where the answers might tend to [be] incriminat[ing]." *State v. P.Z*, 152 N.J. 86, 101 (1997) (quoting *Minnesota v. Murphy*, 465 U.S. 420, 426 (1984)). Under N.J.S.A 2A:84A-18, "a matter will incriminate," if, in relevant part,

> (a) . . . it constitutes an element of a crime . . . , or (b) is a circumstance which with other circumstances would be a basis for a reasonable inference of the commission of such a crime, or (c) is a clue to the discovery of a matter which is within clauses (a) or (b) above; provided, a matter will not be held to incriminate if it clearly appears that the witness has no reasonable cause to apprehend a criminal prosecution.

The history of New Jersey's common law protection against self-incrimination dates back to colonial times, as has been summarized by this Court before.

> The privilege of a witness against being compelled to incriminate himself, of ancient origin, is precious to free men as a restraint against high-handed and

---

> have its full force. In New Jersey, no person can be compelled to be a witness against himself.
>
> [*Zdanowicz*, 69 N.J.L. at 622.]

arrogant inquisitorial practices. 8 Wigmore, Evidence 276 et seq. (3d ed. 1940); Edwin S. Corwin, *The Supreme Court's Construction of the Self-Incrimination Clause*, 29 Mich. L. Rev. 1, 3-9 (1930). It has survived centuries of hot controversy periodically rekindled when there is popular impatience that its protection sometimes allows the guilty to escape. It has endured as a wise and necessary protection of the individual against arbitrary power; the price of occasional failures of justice under its protection is paid in the larger interest of the general personal security. "The wisdom of the exemption has never been universally assented to since the days of Bentham, many doubt it today, and it is best defended not as an unchangeable principle of universal justice, but a law proved by experience to be expedient." *Twining v. New Jersey*, 211 U.S. 78, 113 (1908). Although not written into our State Constitution (as it is in the Fifth Amendment to the Federal Constitution and in the constitutions of all our sister states except Iowa), and not given even statutory expression until it appeared as section 4 of the Evidence Act of 1855, L. 1855, c. 136, § 4, ¶ 668, now N.J.S.[A.] 2A:81-5, the privilege has been firmly established in New Jersey since our beginnings as a State. *Zdanowicz*, 69 N.J.L. 619; *State v. Miller*, 71 N.J.L. 527 (E. & A. 1905); *Fries v. Brugler*, 12 N.J.L. 79 (Sup. Ct. 1830); *In re Vince*, 2 N.J. 443

(1949); *In re Pillo*, 11 N.J. 8 (1952).

[*Fary*, 19 N.J. at 434-35.]

The right has always been regarded as critical. *State v. Vincenty*, 237 N.J. 122, 132 (2019) ("The importance of the common law right 'is not diminished by the lack of specific constitutional articulation.'" (quoting *P.Z.*, 152 N.J. at 101)). Our State's broad embrace of providing robust protection against self-incrimination traces back to the early founders' repugnance to any practice that compelled an individual to cooperate with the authorities in securing his or her own conviction. In an oft-quoted passage from an opinion Justice Brennan wrote for this Court, he explained the underlying rationale for the common law privilege developed in New Jersey:

> In modern concept its wide acceptance and broad interpretation rest on the view that compelling a person to convict himself of crime is "contrary to the principles of a free government" and "abhorrent to the instincts of an American," that while such a coercive practice "may suit the purposes of despotic power, . . . it cannot abide the pure atmosphere of political liberty and personal freedom."

[*In re Pillo*, 11 N.J. 8, 15-16 (1952) (quoting *Boyd*, 116 U.S. at 632).]

Tellingly, Justice Brennan's *Pillo* opinion incorporated *Boyd's* themes in the fulsome enforcement of the right against self-incrimination. That emphasis on the importance of the privacy themes of the privilege was repeated by Justice Brennan while a member of the United States

Supreme Court. When the Supreme Court's majority opinion in *Fisher*, written by Justice White, distanced itself from *Boyd* and moved to its act-of-production analysis, Justice Brennan voiced concern about the new direction, specifically his worry that the approach would not do justice to privacy. 425 U.S. at 416-17 (Brennan, J., concurring) (emphasizing that "precedent[] and history teach" that personal privacy is "a factor controlling in part . . . the scope of the privilege," not a "byproduct," and that "the scope of the privilege . . . [must have] the reach necessary to protect the cherished value of privacy which it safeguards").

That backdrop is important to how I believe this Court should consider *Boyd's* significance in this matter. According to our last word on the subject, this Court never let loose its embrace of *Boyd*, which I believe should continue to guide us in the present matter.

B.

In *In re Grand Jury Proceedings of Guarino*, 104 N.J. 218 (1986), this Court surveyed the Supreme Court's newly developed act-of-production case law in *Fisher* and *Doe I* and, although our Court's outcome in that matter was split, this Court's view of the new case law was not. Both the majority and dissenting opinions said that the common law of New Jersey embraced *Boyd's* approach and declared that *Boyd* was most in keeping with the underlying rationale for our state's common law privilege against self-incrimination. In fact, both specifically said that *Fisher* and *Doe I* were not consistent with our jurisprudence that provided a higher protection against government compelled self-incrimination and

would not be adopted for use in this State. Then, as noted, the two opinions differed in their outcomes.

The majority stated that it was hewing to an assessment of the privacy interest in the ultimate contents of the produced documents, reinforcing its commitment to *Boyd's* protection of private documents. *Id.* at 231. Focusing on the contents of the documents sought by the government, the majority opinion concluded that the business records of a sole proprietor were not in a specific zone of privacy that deserved protection. *Id.* at 232. The Court noted that the documents had been disclosed to third parties and were not an extension of private or intimate aspects of one's life, which were, in the majority's view, the type of document that the privilege protected. *Id.* at 232-33.

The dissent disagreed with the majority's analysis as not properly adhering to *Boyd's* principles, which the majority was expressly reinforcing as the doctrine of this State. And, importantly, the dissent took the occasion to deconstruct the analytic structure of the new federal paradigm, criticizing it for ignoring the privacy roots of *Boyd* that had been "sedulously adhered to" for decades and factored into the "determin[ation] whether individuals could withhold the production, as well as the contents, of incriminating personal documents." *Id.* at 239-40 (Handler, J., dissenting). For the dissent, the federal law's turn was out of sync with the history and import of the Fifth Amendment's protection against compelled incrimination, and the dissent explained in detail why adherence to our common law's approach required adherence to *Boyd's* recognition of privacy and personal autonomy. *Id.* at 243.

In sum, both opinions in *Guarino* espoused fidelity to *Boyd's* acknowledgment that the privilege against self-incrimination must protect the integrity and privacy of the individual. Yet, I believe that my colleagues in the majority misconstrue *Guarino's* import when concluding that the Court's holding today stays true to its principles.

In continuing New Jersey's steadfast protection of personal privacy and autonomy, *Guarino* stands for the proposition that *Boyd* remains valid in that respect in our jurisdiction. Indeed, it is one of many proud decisions in New Jersey that have adhered to our belief, in self-incrimination settings, that New Jersey provides enhanced protections for personal privacy and autonomy. *See, e.g., State v. Muhammad*, 182 N.J. 551, 568-69 (2005) (holding that a suspect's silence, while in custody, at or near time of arrest, cannot be used against him); *State v. Strong*, 110 N.J. 583, 593-595 (1988) (concluding that New Jersey law not only protects against improper conduct to obtain compelled testimony, but also protects against its improper use because such use "is the difference between the constitutional right in not being compelled to incriminate oneself and the right in not having one's privacy unreasonably invaded"); *Hartley*, 103 N.J. at 285-86 (recognizing that the state law privilege against self-incrimination exceeds the protections provided under the Fifth Amendment); *State v. Deatore*, 70 N.J. 100, 112-14 (1976) (same).[7]

---

[7] Similarly, State law exceeds federal protections for privacy in Fourth Amendment searches and seizures as well. *See, e.g., State v. Earls*, 214 N.J. 564, 584-89 (2013) (finding a reasonable expectation of privacy in a person's cell phone location information prior to later federal court case development); *State v. Reid*, 194 N.J. 386, 396-99 (2008) (holding that, regardless of

To the extent that the *Guarino* Court split on the application of those personal privacy principles when it came to documents already in the possession of third parties, that does not support the invasion of private thoughts, as we have here. Defendant is being compelled to disgorge a memorized passcode to allow access to other information on his secure smartphone. In other words, he is being forced to disclose inner thoughts so as to assist law enforcement in his own prosecution. That is contrary to *Boyd's* tenets about personal freedom and privacy. And it is contrary to all previous decisions from this Court with respect to our state recognized law on the privilege against self-incrimination.

This Court has never before permitted law enforcement to compel from a defendant's lips inner thoughts to assist in his own prosecution. I cannot join in taking our state law in that direction. Therefore, for the same reasons that I would not extend federal law to require what the Supreme Court has not expressly held, so too I would not turn our jurisprudence from the guiding principles it has followed to date.

This intrusive use of compelled cooperation forcing self-incrimination through disclosure of the contents of one's mind is not consistent with our law.

---

the federal government's failure to find an expectation of privacy, under New Jersey's heightened protections there is a reasonable expectation of privacy in Internet subscriber information, which can reveal intimate details about a person's life); *State v. McAllister*, 184 N.J. 17, 26-33 (2005) (holding that, although the federal government does not recognize an expectation of privacy in bank records, New Jersey recognizes that expectation because the revealing information contained in a bank record "provides a virtual current biography" (quoting *Burrows v. Superior Court*, 529 P.2d 590, 596 (Cal. 1974))).

It should be rejected as a step backwards from the storied history in this State of protective law concerning personal autonomy and the privacy of one's inner thoughts with respect to the privilege against self-incrimination.

C.

Finally, for completeness, I note that the Appellate Division erred in reading a basis for foregone conclusion into our statute governing what is an incriminating statement. The majority's reasons for similarly adopting that approach are not persuasive and take our law in a direction that is a mistake, in my view. To be clear, I believe that foregone conclusion, as a notion in federal law, has shaky lineage. We should not perpetuate a questionable doctrine.

Further, examination of our statutory provision yields no fertile ground for finding the concept consistent with state law.

New Jersey has enacted statutory protections and an evidentiary rule against self-incrimination, both of which use identical language. See N.J.S.A. 2A:84A-17(1); N.J.R.E. 501. Under both N.J.S.A. 2A:84A-17(1) and N.J.R.E. 501, "[e]very person has in any criminal action in which he is an accused a right not to be called as a witness and not to testify." Further, "every natural person has a right to refuse to disclose in an action or to a police officer or other official any matter that will incriminate him or expose him to a penalty." N.J.S.A. 2A:84A-19; N.J.R.E. 503. There are four applicable exceptions to this rule. Most relevant is N.J.S.A. 2A:84A-19(b), which provides that

> no person has the privilege to refuse to obey an order made by a court to produce

> for use as evidence or otherwise a document, chattel or other thing under his control if some other person or a corporation or other association has a superior right to the possession of the thing ordered to be produced.

In this part of its analysis, the majority views narrowly what is turned over: only the passcodes, which the majority opinion describes as having "minimal evidentiary significance, do not themselves support an inference that a crime has been committed, nor do they constitute 'clues'" because the passcode is "not substantive information, is not a clue to an element of or the commission of a crime, and does not reveal an inference that a crime has been committed." *Ante* at ___ (slip op. at 43). The majority sees no privacy interest being violated because the State has a search warrant for the physical phone. In essence the majority adheres to the Appellate Division's conclusion that

> defendant is not conveying any important facts that the State does not already possess, he is not being required to disclose any 'matter' that would incriminate him or expose him to a penalty. Furthermore, the State has a "superior right of possession" to defendant's passcodes because the trial court has issued two search warrants for defendant's iPhones, which allow the State to obtain the passcodes that may be necessary to access information on the phones.
>
> [*State v. Andrews*, 457 N.J. Super. 14,

32-33 (App. Div. 2018).]

In so concluding, the Appellate Division first, and now the majority, improperly, in my view, read the foregone conclusion doctrine into New Jersey jurisprudence in a manner that is both inconsistent with the spirit of our law and not grounded in precedent.

First, the State cannot claim a superior right of access to the passcodes. While the State can claim a legal right to review internal information on the phone pursuant to a warrant, the State cannot have a superior right to the contents of one's mind—which here, is the passcode. Both the Appellate Division and the majority's opinion conflate the State's Fourth Amendment right to obtain a valid warrant based on probable cause with defendant's Fifth Amendment right not to be compelled to assist in his own prosecution by being ordered to provide information contained in his mind that can be used to obtain undetermined and unspecified information in the hope it will incriminate him.

Second, the Appellate Division did not properly consider the State's long-codified protections that uphold a person's refusal to disclose incriminating information. Pursuant to N.J.S.A. 2A:84A-18's clear definition of incrimination, something is incriminating

> (a) if it constitutes an element of a crime against this State, or another State or the United States, or (b) is a circumstance which with other circumstances would be a basis for a reasonable inference of the commission of such a crime, or (c) *is a clue to the*

> *discovery of a matter which is within clauses (a) or (b) above*; provided, a matter will not be held to incriminate if it clearly appears that the witness has no reasonable cause to apprehend a criminal prosecution. In determining whether a matter is incriminating under clauses (a), (b) or (c) and whether a criminal prosecution is to be apprehended, other matters in evidence, or disclosed in argument, the implications of the question, the setting in which it is asked, the applicable statute of limitations and all other factors, shall be taken into consideration.
>
> [N.J.S.A. 2A:84A-18 (emphasis added).]

The majority cannot support the claim that the State has a superior right of access to the phone's passcode. And the majority does not properly consider what the passcode would reveal. The majority opinion at times focuses on the passcode, and at others equates the passcode with the evidentiary information the government hopes to find somewhere in the encrypted device's phone and message icons. For this part of its analysis, the majority chooses to isolate the passcode from the hopefully incriminating contents the government wants.

The majority cannot have it both ways—focusing solely on the passcode sometimes and on the phones and their contents at other times. In my view, the Appellate Division and the majority fail to acknowledge that compelling defendant's participation in obtaining passcodes giving access to the phone would certainly provide more than just a

clue to an underlying crime: defendant is being compelled to essentially turn over what is presumed to be incriminating information, in direct violation of his right not to testify against himself.

IV.

For the foregoing reasons, I respectfully dissent from the judgment of the Court. I would hold that the judicial order compelling defendant to disclose the passcode to his smartphone by requiring him to reveal the contents of his mind is a violation of the Fifth Amendment protection against self-incrimination and a violation of our state law protecting the same.

Law enforcement must find another means of obtaining access to the encrypted substantive information on two cell phones whose contents it wishes to search and for which the government has a search warrant. Technological barriers must be overcome without sacrificing constitutional, deep-seated historical protections against governmental intrusions forcing individuals to become assistants in their own prosecutions. Modern technology continues to evolve, bringing new problems; but it also may bring new solutions. The resolution to the present problem must be found in those new technological solutions—at least until the Supreme Court addresses whether it is now willing to permit forced disclosure of mental thoughts because, in my view, to date, its case law on accessing physical documents, respectfully, does not support the steps being taken here.

APPENDIX B

SUPREME COURT OF NEW JERSEY
M-960 September Term
082209

———

STATE OF NEW JERSEY,
Plaintiff-Respondent,

v.

ROBERT ANDREWS,
Defendant-Movant.

———

On appeal from the Superior Court,
Appellate Division, whose opinion is reported at
457 N.J. Super. 14 (App. Div. 2018).

[FILED: May 3, 2019]

ORDER

It is **ORDERED** that the motion for leave to appeal is granted;

and it is further

ORDERED that the appellant may serve and file a supplemental brief on or before July 2, 2019, and respondent may serve and file a supplemental brief forty-five (45) days after the filing of appellant's supplemental submission, or, if appellant declines to file such a submission, on or before August 16, 2019.

APPENDIX C

SUPERIOR COURT OF NEW JERSEY
APPELLATE DIVISION
DOCKET NO. A-0291-17T4

———

STATE OF NEW JERSEY,
Plaintiff-Respondent,

v.

ROBERT ANDREWS,
Defendant-Appellant.

———

On appeal from an interlocutory order of Superior Court of New
Jersey, Law Division, Essex County,
Indictment No. 16-06-1781.

[FILED: November 15, 2018]

Before Judges Yannotti, Rothstadt and Natali.

OPINION

The opinion of the court was delivered by YANNOTTI, P.J.A.D.

Defendant appeals, on leave granted, from an order of the Law Division, which required defendant to disclose the personal identification numbers and passwords (the passcodes) for his lawfully-seized iPhones. Defendant argues that the compelled disclosure of this information violates his right against self-incrimination under the Fifth Amendment to the United States Constitution, and the protections against self-incrimination afforded

under New Jersey law. We reject defendant's arguments and affirm the trial court's order.

I.

We briefly summarize the pertinent facts and procedural history. In May and June 2015, a task force of the Essex County Prosecutor's Office (ECPO) was investigating a suspected narcotics-trafficking network in Newark. During surveillance, law enforcement officers observed Quincy Lowery (Lowery), the target of the investigation, operating a motorcycle and a Jeep, even though his driver's license was suspended at the time. Both vehicles were registered in defendant's name.

In June 2015, the task force obtained a court order, which authorized a wiretap of Lowery's phone and placement of a global positioning system (GPS) device on the Jeep. On June 30, 2015, Lowery was arrested on suspicion of drug trafficking. On the night of his arrest, Lowery gave a formal statement, alleging that an officer in the Essex County Sheriff's Office (ECSO), whom Lowery knew only as "Bolo," had helped him conceal his drug-trafficking activities. Lowery said he had known "Bolo" for about a year through a motorcycle club in which both men were members. From a photograph, Lowery identified defendant as the person named "Bolo."

Lowery claimed defendant assisted him by registering the Jeep and motorcycle in his own name because defendant knew Lowery's license had been suspended. Lowery said defendant warned him about the wiretap and urged him and his co-conspirators to get rid of their phones. According to Lowery, defendant checked the license plate of a vehicle Lowery had suspected of following him and confirmed

it was a county-issued vehicle. Defendant also confirmed Lowery's suspicion that a man Lowery saw at a bar was an undercover officer. In addition, defendant suggested that Lowery put his motor vehicle on a lift to check it for a GPS device, and to discard any such device.

Lowery consented to an electronic search of his phone and showed the police a picture of a license plate he had texted to defendant. The investigators later confirmed the license plate belonged to a vehicle the task force had used in a surveillance operation. The cell phone number associated with the name "Bolo" on Lowery's phone corresponds to the number for one of defendant's iPhones. Lowery suggested to investigators that defendant generally offered this assistance either in person or by using the video app FaceTime, and that the text messages the two exchanged were mostly limited to arranging meetings.

On the night Lowery was arrested, the Internal Affairs Department of the ECSO confronted defendant and asked him to surrender his two phones: an iPhone 5s and an iPhone 6 Plus. Defendant turned in the phones but refused to consent to a search of either phone or give a statement. Defendant later requested that the phones be returned to him. The officers denied the request and held the phones pending an application for a search warrant.

In June 2016, an Essex County grand jury returned a six-count indictment charging defendant with second-degree official misconduct, contrary to N.J.S.A. 2C:30-2 (counts one and two); third-degree hindering the apprehension or prosecution of another person, contrary to N.J.S.A. 2C:29-3(a)(2) (counts three and four); and fourth-degree obstruction of the

administration of the law or government function, contrary to N.J.S.A. 2C:29-1 (counts five and six).

In January 2017, the State filed a motion to compel defendant to disclose the passcodes required to unlock defendant's iPhones. In support of its motion, the State submitted call records it had obtained regarding Lowery's phone, which showed that in the thirty days before Lowery's arrest, 187 phone calls had been exchanged between defendant's iPhones and Lowery's mobile devices. However, these records reflected only the number of calls exchanged, and they provided no information about the duration of the calls.

Lowery's phone and call records also revealed a series of text messages with defendant. However, Lowery told investigators that on defendant's advice, he reset his phone about thirty days before his arrest. Therefore, the State could not access any of that data. Because defendant's iPhones were locked, the State could not determine whether defendant's devices contained any of the missing texts between Lowery and defendant or any information about the duration of their calls. The State asserted that the only way to obtain records as to the duration of the calls was through defendant's iPhones since Apple is a "closed end to end system," and defendant's service providers do not have access to Apple's "system."

Defendant opposed the motion, arguing that compelled disclosure of the passcodes would violate his Fifth Amendment right against self-incrimination. He argued that the State was seeking to compel disclosure of statements that are testimonial and potentially incriminating. He further argued that any compelled disclosure would be inconsistent with the

privilege against self-incrimination under New Jersey law.

The trial court heard oral argument on the motion, and on May 22, 2017, filed a written opinion in which it concluded that the State's motion should be granted. The court found that the compelled disclosure of the passcodes was not a violation of defendant's constitutional right against self-incrimination. The court also decided that the privilege against self-incrimination under New Jersey's common law, N.J.S.A. 2A:84A-19(b), and N.J.R.E. 503 did not preclude the court from requiring defendant to disclose the information.

The court memorialized its opinion in an order dated May 22, 2017. The order requires defendant to disclose the passcodes, but limited the State's access "to that which is contained within (1) the 'Phone' icon[s] and application[s] on [defendant's] two iPhones and (2) the 'Messages' icon[s] and/or text messaging applications." The order also requires defendant to disclose the passcodes in camera before any disclosure to the State, and directed the State to perform the actual search "in camera, in the presence of . . . defense counsel and the [c]ourt."

In June 2017, defendant filed a motion seeking leave to appeal the trial court's May 22, 2017 order. In July 2017, we denied the motion. Defendant then filed a motion in the Supreme Court for leave to appeal. The Supreme Court granted the motion and summarily remanded the appeal to this court for consideration on the merits. We later permitted the Association of Criminal Defense Lawyers of New Jersey (ACDL-NJ) to appear as amicus curiae.

II.

Defendant argues that the trial court's order compelling him to disclose the passcodes for the seized phones violates his right against self-incrimination, as provided in the Fifth Amendment to the United States Constitution. We conclude, however, that under the circumstances presented here, the compelled disclosure of the passcodes is not barred by the Fifth Amendment.

The Fifth Amendment to the United States Constitution, which is made applicable to the states through the Fourteenth Amendment, *Malloy v. Hogan*, 378 U.S. 1, 6 (1964), provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself[.]" U.S. Const. amend. V. "The word 'witness' in the constitutional text limits the relevant category of compelled incriminating communications to those that are 'testimonial' in character." *United States v. Hubbell*, 530 U.S. 27, 34 (2000).

"[T]o be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information," such as an admission that the revealed evidence "exist[s]," is "in [defendant's] possession or control," and is "authentic." *Doe v. United States*, 487 U.S. 201, 209-10 (1988) (citing *United States v. Doe*, 465 U.S. 605, 613 & n.11 (1984); *Fisher v. United States*, 425 U.S. 391-409-10 (1976)). "Only then is a person compelled to be a 'witness' against himself." *Id.* at 210.

The Fifth Amendment privilege against self-incrimination applies not only to verbal and written communications but also to the production of documents because "[t]he act of produc[tion]" itself

may communicate incriminatory statements. *Fisher*, 425 U.S. at 410. Nevertheless, the "foregone conclusion" principle is an exception to the "act of production" doctrine. *See id.* at 411.

For the "foregone conclusion" exception to apply, the State must establish with reasonable particularity: (1) knowledge of the existence of the evidence demanded; (2) defendant's possession and control of that evidence; and (3) the authenticity of the evidence. *See Hubbell*, 530 U.S. at 30, 40-41; *Fisher*, 425 U.S. at 410-13. Therefore, when an accused implicitly admits the existence and possession of evidence, the accused has "add[ed] little or nothing to the sum total" of the information the government has, and the information provided is a "foregone conclusion." *Fisher*, 425 U.S. at 411.

In *Doe*, the Court held that an order requiring the target of a grand jury investigation "to authorize foreign banks to disclose records of his accounts, without identifying those documents or acknowledging their existence," did not compel a testimonial act for purposes of the Fifth Amendment. *Doe*, 487 U.S. at 202, 219. The Court found that the defendant's execution of the disclosure form did not convey anything about the existence of any foreign bank account, the defendant's control over any such account, or the authenticity of any records the banks may produce. *Id.* at 215-16.

Here, as in *Doe*, the act of disclosing the passcodes to defendant's phones does not convey any implicit factual assertions about the "existence," or "authenticity" of the data on the device. *See ibid.* Moreover, in its order, the trial court required defendant to disclose the passcodes in camera before

they are communicated to the State. The order thus ensures that any incriminating information would not be disclosed. The order also ensures that by providing the passcodes, defendant will not be compelled "to restate, repeat, or affirm the truth of the contents of the" devices. *See Fisher*, 425 U.S. at 409.

However, by producing the passcode, defendant is making an implicit statement of fact that the iPhone passcodes are within his "possession or control." *See Doe*, 487 U.S. at 209 (citing *Doe*, 465 U.S. at 613 & n.11; *Fisher*, 425 U.S. at 409-10). Defendant is acknowledging he has accessed the phone before, set up password capabilities, and exercised some measure of control over the phone and its contents.

Nevertheless, these testimonial aspects of the passcodes are a "foregone conclusion" because the State has established and defendant has not disputed that he exercised possession, custody, or control over these devices. *See Fisher*, 425 U.S. at 411. Therefore, the fact that defendant knows the passcodes to these devices "adds little or nothing to the sum total of the Government's information." *See ibid.*

Furthermore, the State has described with "reasonable particularity" the specific evidence it seeks to compel, which is the passcodes to the phones. Defendant argues the State is unaware of all of the possible contents of defendant's devices. This is immaterial because the order requires defendant to disclose the passcodes, not the contents of the phones unlocked by those passcodes. *See Fisher*, 425 U.S. at 409.

Our conclusion that the Fifth Amendment privilege does not bar the court from requiring defendant to disclose the passcodes is supported by

United States v. Apple MacPro Computer, 851 F.3d 238 (3d Cir. 2017). In that case, as part of an investigation of the defendant's access to child pornography over the internet, authorities executed a search warrant and seized an Apple iPhone 5s and an Apple Mac Pro computer with two attached external hard drives, which were protected with encryption software. Id. at 242. The police later seized an Apple iPhone 6 Plus, which also was password-protected. *Ibid.*

The defendant voluntarily provided the authorities the password for the iPhone 5s, but refused to provide passwords that would allow access to the computer or the external hard drives. Ibid. Forensic analysis of the computer revealed that it had been used to visit sites known for child exploitation, and that thousands of files associated with child pornography had been downloaded. *Ibid.* The downloaded files were not on the computer, but stored on the external hard drives, which were encrypted. *Ibid.*

The defendant's sister informed the authorities that the defendant had shown her hundreds of images of child pornography on the external hard drives. *Id.* at 242-43. The defendant provided the password for the iPhone 6 Plus; however, he "did not grant access to an application on the phone which contained additional encrypted information." *Id.* at 243. The forensic analysis indicated that the phone's encrypted database contained more than 2000 images and video files. *Ibid.*

On an application by the federal authorities, the federal district court ordered the defendant to produce his iPhone 6 Plus, Mac Pro computer, and two

external hard drives "in a fully unencrypted state." *Ibid.* The defendant then filed a motion to quash the government's request, arguing that the act of decrypting would violate his Fifth Amendment privilege against self-incrimination. *Ibid.* A magistrate judge denied the motion. *Ibid.*

Later, the defendant appeared at the local police department for a forensic examination of the devices. *Ibid.* He provided the iPhone 6 Plus and the files on the application in a fully unencrypted state. *Ibid.* He claimed, however, that he could not recall the passwords required to decrypt the hard drives, and he entered several incorrect passwords during the examination. *Ibid.* Consequently, the federal authorities were unable to view the decrypted contents of the hard drives. *Ibid.*

On the government's motion, the federal district court held the defendant in contempt, and ordered his incarceration until he complied with the decryption order. *Id.* at 243-44. Defendant appealed and argued the order violated his right against self-incrimination. *Id.* at 244. The Third Circuit held that although the Fifth Amendment may be implicated by the compelled decryption of the devices, "any testimonial aspects of that production were a foregone conclusion." *Id.* at 248.

The court found that the record supported the conclusion that the production of the decrypted devices "added little or nothing to the information" the government already had obtained. *Ibid.* The court noted that: the government had custody of the devices; the government knew the defendant owned, possessed, and had accessed the devices before they were seized; and the government had established that

the devices had images that met the definition of child pornography. *Ibid.*

A similar conclusion was reached in *Commonwealth v. Gelfgatt*, 11 N.E.3d. 605 (Mass. 2014). In that case, the defendant was charged with various offenses, which were allegedly part of a mortgage-fraud scheme. *Id.* at 608. The trial court denied the government's motion to compel the defendant to enter his password for encryption software he had placed on various digital media storage devices, which the government had seized as part of its investigation, finding that compelled disclosure of the information would violate the defendant's right against self-incrimination. *Id.* at 611-12. The Supreme Judicial Court of Massachusetts reversed. *Id.* at 617.

The court stated that although the Fifth Amendment typically applies to oral and written testimonial statements, "the act of producing evidence . . . may have communicative aspects." *Id.* at 613 (quoting *Fisher*, 425 U.S. at 410). Whether an act of producing evidence is testimonial for Fifth Amendment purposes "depend[s] on the fact and circumstances of [each] particular case[]." *Ibid.* (alterations in original) (quoting *Fisher*, 425 U.S. at 410).

The court stated that defendant's act of entering the encryption key "would appear, at first blush, to be a testimonial communication that triggers Fifth Amendment protection." *Id.* at 614. The defendant "would be acknowledging that he ha[d] ownership and control of the computers and their contents." *Ibid.* The court held, however, that the Fifth Amendment did not bar the government from compelling the defendant to produce the information

because the "foregone conclusion" exception applied. *Id.* at 615.

The court observed that by entering the encryption key, the defendant would be conveying facts as to "his ownership and control of the computers and their contents, knowledge of the fact of encryption, and knowledge of the encryption key." *Ibid.* Because the government already knew these facts, their disclosure was a "foregone conclusion." *Ibid.* The court held that the defendant's rights under the Fifth Amendment were not violated "because the defendant is only telling the government what it already knows." *Id.* at 615-16.

We are convinced that the decisions in *Apple MacPro Computer* and *Gelfgatt* provide persuasive authority for the conclusion that defendant's Fifth Amendment right against self-incrimination is not violated by requiring him to disclose the passcodes for his iPhones, which the State lawfully possessed. The act of producing the passcodes has testimonial aspects because defendant is acknowledging ownership, possession, and control of the devices. He is also acknowledging he has the ability to access the contents of the phone. However, by producing the passcodes, defendant is not implicitly conveying any information the State does not already possess. Defendant is not telling the government something it does not already know. Therefore, the implicit facts conveyed by the act of producing the passcodes is a "foregone conclusion" and compelled disclosure of the passcodes does not violate defendant's Fifth Amendment right against self-incrimination.[1]

---

[1] Other courts have reached similar conclusions and also support our decision. *See, e.g., United States v. Fricosu*, 841 F. Supp. 2d

We recognize that the contents of the phone may contain evidence that ties defendant to the offenses for which he has been charged. However, "[i]f a compelled statement is 'not testimonial and for that reason not protected by the privilege, it cannot become so because it will lead to incriminating evidence.'" *Doe*, 487 U.S. at 208-09 n.6 (quoting *In re Grand Jury Subpoena*, 826 F.2d 1166, 1172 n.2 (2d Cir. 1987) (Newman, J., concurring)).

In arguing that compelled disclosure of the passcodes violates his Fifth Amendment right against self-incrimination, defendant relies on *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (11th Cir. 2012). In that case, the defendant was ordered to appear before a federal grand jury and produce unencrypted contents of hard drives on his computers, as well as external hard drives. *Id.* at 1337.

1232, 1236-37 (E.D. Mich. 2010) (holding that the Fifth Amendment did not bar the subpoenaed decryption of the defendant's laptop where the defendant admitted to possession of the computer and federal agents were also aware "of the existence and location of the computer's files"); *State v. Stahl*, 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016) (concluding that defendant's act of providing the password to his iPhone pursuant to a search warrant was not testimonial where the State knew there was a password and that the defendant possessed the password); *Commonwealth v. Davis*, 176 A.3d 869, 876 (Pa. Super. Ct. 2017) (holding that the defendant's act of providing the password to his computer was not testimonial where the Commonwealth had already established the computer was password-protected, the defendant was the only user who knew the password, the "technology is self-authenticating," and there was a "high probability" that incriminating material would be discovered on the defendant's device).

The defendant refused to comply, relying upon his Fifth Amendment right against self-incrimination. *Ibid.* The government agreed to provide the defendant with immunity for the act of production of the unencrypted drives, but not for the derivative use of their contents. *Id.* at 1337-38. The defendant refused to decrypt the hard drives, and the federal district court held him in contempt. *Id.* at 1338. The defendant appealed and the Eleventh Circuit reversed. *Id.* at 1338-39.

The court noted that in *Hubbell*, a federal grand jury had issued a subpoena, which required the defendant "to produce eleven categories of documents." *Id.* at 1344 (citing *Hubbell*, 530 U.S. at 30-31). The court stated that in *Hubbell*, the Court had determined that the act of production was sufficiently testimonial to trigger the Fifth Amendment protection against self-incrimination, and the facts implicitly conveyed by the act of production were not a "foregone conclusion." *Ibid.* (citing *Hubbell*, 530 U.S. at 44-45). The court stated that, "The touchtone of whether an act of production is testimonial is whether the government compels the individual to use 'the contents of his own mind' to explicitly or implicitly communicate some statement of fact." *Id.* at 1345 (quoting *Curcio v. United States*, 354 U.S. 118, 128 (1957)).

The court determined that "the decryption and production of the hard drives would require the" defendant to use the contents of his mind. *Id.* at 1346. This "would be tantamount to testimony by [the defendant] of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; and his capability to decrypt the

files." *Ibid.* The court also rejected the contention that the facts conveyed by the production were a "foregone conclusion." *Id.* at 1346-47. The court stated the government did not know whether there was data on the decrypted records. *Id.* at 1347. The drives could contain as many as twenty million files and the government had not shown that these files could be useful. *Ibid.*

Here, defendant's reliance upon *In re Grand Jury Subpoena* is misplaced. In that case, the court found that requiring the defendant to provide the decrypted records was testimonial and the government had not shown that the facts conveyed by the act of production were a "foregone conclusion." *Id.* at 1346-47. In this case, however, defendant has been ordered to produce the passcodes and the testimonial aspects of that act pertain to the ownership, control, use, and ability to access the phones. The State has shown it has prior knowledge of those facts, and their disclosure is a "foregone conclusion."

Defendant also relies upon *United States v. Kirschner*, 823 F. Supp. 2d 665 (E.D. Mich. 2010). In that case, the defendant was charged with receiving child pornography by computer. *Id.* at 666. The government issued a subpoena to the defendant, which required that he appear before the grand jury and provide all passwords used or associated with the subject computer and any files. *Ibid.* The court found that the production of the computer passwords was testimonial because the government was "seeking testimony from the [d]efendant" which required "him to divulge through his mental processes his password[.]" *Id.* at 669. The court stated that the matter did not involve the production of specific

documents, but rather the production of "specific testimony asserting a fact." *Ibid.*

However, defendant's reliance upon Kirschner is unavailing. In that case, the court did not address the question of whether the government already was in possession of the facts implicitly conveyed by the act of producing the passwords. As we have explained, in this case, the State has established all of the elements required for application of the "foregone conclusion" principle.[2]

We note that in its brief, amicus curiae argues that electronically-stored information should be subjected to an enhanced degree of scrutiny because such data raises issues of authenticity. The parties to this appeal have not raised this issue. Therefore, we will not address it. *See State v. J.R.*, 227 N.J. 393, 421 (2017) (declining to "consider arguments that have not been asserted by a party, and are raised for the first time by an amicus curiae").

We therefore conclude that the trial court correctly found that compelled disclosure of defendant's passcodes does not violate defendant's Fifth Amendment privilege against self-incrimination.

---

[2] Defendant also relies on *In re Search Warrant Application*, 279 F. Supp. 3d 800, 806 (N.D. Ill. 2017), where the court held that disclosure of a passcode was testimonial; however, the court did not address the "foregone conclusion" principle. In addition, in *Commonwealth v. Baust*, 89 Va. Cir. 267, 271 (Cir. Ct. 2014), the court held that a "password is not a foregone conclusion because it is not known outside of [the defendant's] mind." The reasoning of the courts in *Apple MacPro Computer*, *Gelfgatt*, and the cases discussed previously is more persuasive.

III.

Defendant also argues that compelled disclosure of the passcodes would violate the privilege against self-incrimination under New Jersey law. He cites the common law, as well as N.J.S.A. 2A:84A-19 and N.J.R.E. 503.

A. Common-law Privilege

The New Jersey Constitution does not contain a privilege against self-incrimination. Even so, New Jersey has long recognized the privilege under the common law. *See, e.g., Fries v. Brugler*, 12 N.J.L. 79, 81 (Sup. Ct. 1830) (noting that "the general rule is, that a witness cannot be called upon to impute to himself a crime or to bring a reproach upon himself[.]"). Our Supreme Court has held that, in general, the "state-law privilege against self-incrimination offers broader protection than its federal counterpart." *State v. Muhammad*, 182 N.J. 551, 568 (2005) (citing *State v. Strong*, 110 N.J. 583, 595 (1988)).

"Central to our state common-law conception of the privilege against self-incrimination is the notion of personal privacy. . . ." *In re Grand Jury Proceedings of Guarino*, 104 N.J. 218, 230 (1986). In *Guarino*, the Court equated the personal privacy doctrine with a "respect for the inviolability of the human personality and of the right of each individual 'to a private enclave where he may lead a private life.'" *Id.* at 231 (quoting *Murphy v. Waterfront Comm'n of N.Y. Harbor*, 378 U.S. 52, 55 (1964)).

"To determine whether the evidence sought by the government lies within that sphere of personal privacy a court must look to the 'nature of the evidence.'" *Id.* at 231-32 (citing *Couch v. United States*,

409 U.S. 322, 350 (1973) (Marshall, J., dissenting)). The court must decide whether the "contents" of the compelled disclosures "contain the requisite element of privacy or confidentiality" such that they fall within a "special zone of privacy." *See id.* at 232 (quoting *Bellis v. United States*, 417 U.S. 85, 92 (1974)).

In this case, defendant argues that cell phones are "known to contain extremely personal information," and can be "used as a personal diary, recorder of personal images and videos, personal address book, and research device." Defendant therefore argues that cell phone passcodes should be deemed to fall within a "special zone of privacy" or confidentiality. We cannot agree.

Applying the privilege against self-incrimination to cell phone passcodes would essentially preclude the State from obtaining the contents of any passcode-restricted device as part of a criminal investigation. This would be so even when the State has obtained a warrant, issued on a showing of probable cause, for the contents of the device, and the State has established, as it has in this case, the basis for applying the "foregone conclusion" doctrine.

We see no basis for affording, in the particular circumstances presented by this case, greater protections against self-incrimination than those provided by the Fifth Amendment. We therefore hold that where, as here, the State has established the elements for application of the "foregone conclusion" doctrine, New Jersey's common law privilege against self-incrimination does not bar compelled disclosure of passcodes for defendant's phones.

B. Statutory and Evidentiary Privilege

New Jersey also has enacted a statute and evidence rule that, in identical language, provide that "every natural person has a right to refuse to disclose in an action or to a police officer or other official any matter that will incriminate him or expose him to a penalty," unless one of four exceptions applies. N.J.S.A. 2A:84A-19; N.J.R.E. 503. Under one of the exceptions to the privilege:

> (b) [N]o person has the privilege to refuse to obey an order made by a court to produce for use as evidence or otherwise a document, chattel or other thing under his control if some other person or a corporation or other association has a superior right to the possession of the thing ordered to be produced[.]
>
> [N.J.S.A. 2A:84A-19(b); N.J.R.E. 503(b).]

As we have determined, compelled disclosure of defendant's passcodes is not a violation of his right against self-incrimination under the Fifth Amendment or our common law. Because defendant is not conveying any important facts that the State does not already possess, he is not being required to disclose any "matter" that would incriminate him or expose him to a penalty. Furthermore, the State has a "superior right of possession" to defendant's passcodes because the trial court has issued two search warrants for defendant's iPhones, which allow the State to obtain the passcodes that may be necessary to access information on the phones.

Defendant has not argued that the warrants are unlawful. He argues, however, that under New Jersey law, he cannot be required to produce any

evidence that may be used against him. In support of this argument, he relies on *In re Addonizio*, 53 N.J. 107 (1968), and *State v. Kelsey*, 429 N.J. Super. 449 (App. Div. 2013). Both cases are distinguishable.

In *Addonizio*, the defendant was appealing the denial of a motion to set aside subpoenas that, similar to those in *Hubbell*, 530 U.S. at 31, had directed him to produce ten categories of financial documents. *See Addonizio*, 53 N.J. at 113. *Addonizio* involved no warrant of any kind, and would have required defendant to make extensive use of the contents of his mind in order to comply. *See Hubbell*, 530 U.S. at 43. As we have determined, however, disclosure of cell phone passcodes does not involve the production of testimonial evidence, and the act of producing the passcodes only coveys implicit facts that the government already knows.

Moreover, in *Kelsey*, the defendant challenged an order compelling him to produce a flashlight that he allegedly used as a weapon in a brawl. *Kelsey*, 429 N.J. Super. at 450. The police had obtained a warrant to search defendant's vehicle, but when they did not find what they were searching for, they sought an order for defendant to produce the item, which "may or may not" have been in defendant's possession. *Id.* at 450, 452 (emphasis added).

Here, the State has evidence indicating that defendant used the iPhones before surrendering them. The State knows defendant possesses the passcodes, and has obtained search warrants issued upon a showing of probable cause that the devices contain evidence of criminality. We therefore conclude the search warrants give the State a superior right to

possession of the passcodes; therefore, the exception in N.J.S.A. 2A:84A-19(b) and N.J.R.E. 503(b) applies.

Affirmed.

APPENDIX D

SUPREME COURT OF NEW JERSEY

STATE OF NEW JERSEY,
Plaintiff-Respondent,

v.

ROBERT ANDREWS,
Defendant-Movant.

On appeal from an interlocutory order of Superior Court of New
Jersey, Law Division, Essex County,
Indictment No. 16-06-1781.

[FILED: September 11, 2017]

ORDER

It is **ORDERED** that the motion for leave to appeal is granted and the matter is summarily remanded to the Superior Court, Appellate Division, to consider on the merits.

APPENDIX E

SUPERIOR COURT OF NEW JERSEY
LAW DIVISION - CRIMINAL PART
COUNTY OF ESSEX
Indictment No. 16-06-0178 1-1

———

STATE OF NEW JERSEY,
Plaintiff-Respondent,

v.

ROBERT ANDREWS,
Defendant-Appellant.

———

[FILED: May 22, 2017]

OPINION

HONORABLE ARTHUR J. BATISTA, J.S.C.

In this case, the issue presented is whether the United States Constitution's Fifth Amendment privilege against self- incrimination and/or New Jersey common law or statutory rights protect a defendant from the compelled disclosure of his iPhone PINs or passwords.

The State of New Jersey ("State") requests that the court compel the Defendant, Robert Andrews ("Andrews" or "Defendant"), to disclose his PINs or passwords to two of his lawfully-seized iPhones. Andrews objects to the State's request on constitutional grounds, asserting his Fifth Amendment privilege against self-incrimination as well as protections afforded by New Jersey common law, statutory law, and the New Jersey Rules of

Evidence. Andrews contends the requested compulsion is testimonial and incriminating and therefore violative of his constitutional rights.

This court finds that the act of providing a PIN, password, or passcode is not a testimonial act where the Fifth Amendment or New Jersey common and statutory law affords protection. Moreover, the State has sufficiently demonstrated that any testimonial act contained in the act of Andrews providing the PIN or passcode is a foregone conclusion pursuant to *Fisher v. U.S.*, 425 U.S. 391, 96 S. Ct. 1569, 48 L. Ed. 2d 39 (1976) and its progeny.

I.

We begin with an overview of a defendant's protections against self-incrimination to offer context for the discussion that follows.

The protection against self-incrimination is preserved in federal law in the Fifth Amendment to the United States Constitution, which provides that "[n]o person ... shall be compelled in any criminal case to be a witness against himself [.]" U.S. Const., amend. V. The privilege is at the fundamental core of our way of life, our "political liberty and personal freedom." *In re Pillo*, 11 N.J. 8, 16 (1952) (quoting *Boyd v. U.S.*, 116 U.S. 616, 632, 6 S. Ct. 524, 29 L. Ed. 746 (1886)). The privilege is applied to the states through operation of the Fourteenth Amendment. *Lefkowitz v. Turley*, 414 U.S. 70, 77, 94 S. Ct. 316, 38 L. Ed. 2d 274 (1973).

New Jersey's state constitution contains no similar provision. Instead, New Jersey's privilege against self-incrimination is found in the common law, statute, and the New Jersey Rules of Evidence. The New Jersey Supreme Court has recognized that

our common-law privilege against self-incrimination, "as codified both in N.J.S.A. 2A:84A-19 and N.J.R.E. 503 'offers broader protection than its federal counterpart.'" *State v. Brown*, 190 N.J. 144, 166-67 (2007) (citing *State v. Muhammad*, 182 N.J. 551 (2005)). Subject to enumerated limitations, "every natural person has a right to refuse to disclose in an action or to a police officer or other official any matter that will incriminate him or expose him to a penalty or a forfeiture of his estate[.]" N.J.R.E. 503.; see also N.J.S.A. 2A:84A-19. Our body of common law has thus diverged from Fifth Amendment case law.

In *Fisher v. U.S.*, *supra* 425 U.S. 391, and *U.S. v. Doe*, 465 U.S. 605, 104 S. Ct. 1237, 79 L. Ed. 2d 552 (1984), the United States Supreme Court limited its interpretation of the Fifth Amendment's protection against self-incrimination. "In effect, the focus of the Court shifted from privacy to the process of compulsion." *In re Grand Jury Proceedings (Guarino)*, 104 N.J. 218, 225 (1986). Under this interpretation, it is the act of testifying that cannot be compelled, not the substance of the information to be disclosed. *Fisher* did recognize that the act of producing a document could have "communicative aspects of its own, wholly aside from the contents of the papers produced" when the production served to confirm the existence of the documents or else to "authenticate" them. *Fisher*, *supra* 425 U.S. at 410. This communicative aspect, however, can be overcome if the revelation is a "foregone conclusion and ... adds little or nothing to the sum total of the Government's information[.]" *Id.* at 411.

The New Jersey Supreme Court, by contrast, has found that the analysis should focus on the content of documents, not merely the act of producing

them. The Court found that the privilege against self-incrimination should be based on protecting an individual's right "to a private enclave where he may lead a private life." *In re Grand Jury Proceedings (Guarino)*, 104 N.J. at 231 (quoting *Murphy v. Waterfront Comm'n*, 378 U.S. 52, 55, 84 S. Ct. 1594, 12 L. Ed. 2d 678 (1964)).

While there is no precedent in New Jersey dealing with the compulsion of defendants to provide their cell phone PINs or passwords, other jurisdictions throughout the United States have commenced grappling with the competing interests at issue. A review of those decisions provides this court with essential guidance.

II.

In 2009, the United States District Court for the District of Vermont decided *In re Boucher*, 2009 U.S. Dist. LEXIS 13006, *1, 2009 WL 424718 (D. Vt. Feb. 19, 2009). The defendant Boucher was stopped at the United States border as he crossed into Vermont from Canada. A Customs and Border Protection inspector flagged his vehicle for secondary inspection. Boucher's laptop computer was consensually inspected and revealed certain files on the "Z" drive that appeared to include child pornography. The agent seized the device and shut it down. After obtaining a warrant to search the laptop, agents discovered that the contents of the "Z" drive were not able to be viewed because it was encrypted with password protection. As a result, a grand jury subsequently issued a subpoena compelling Boucher to produce any passwords associated with the laptop. Boucher then sought to quash the subpoena.

A U.S. Magistrate judge granted Boucher's motion to quash that subpoena on Fifth Amendment grounds. The government filed an appeal to the District Court, which heard the case on de nova review. The District court denied the motion, holding that allowing a second look at the files on the laptop added "little or nothing to the sum total of the Government's information." *Id.* at *9 (quoting *Fisher v. U.S.*, *supra* 425 U.S. at 411 (1976)). Citing *U.S. v. Fox*, 721 F.2d 32, 36 (2d Cir. 1983), the court treated the files contained on the laptop in the manner previous cases treated actual paper documents. If a disclosure would implicitly authenticate the documents, they cannot be compelled. However, when the existence and location of the documents are known to the government, no constitutional rights are touched, because these matters are a foregone conclusion. *Id.* at *8 (quoting *Fisher* at 411). The government knew what information was present on the laptop and where it was located because the files had already been observed by the inspecting agents. Thus, while the court found that providing the password to the encrypted laptop would be testimonial, it fell under the "foregone conclusion" exception to Fifth Amendment protection.

In 2010, the Eastern District of Michigan looked at a very similar case in *U.S. v. Kirschner*, 823 F. Supp. 2d 665 (E.D. Michigan, Southern Division 2010). There, the district court granted the defendant's motion to quash a subpoena directing him to turn over passwords to his encrypted laptop. The Michigan court followed the same analysis as in *Boucher*, but reached a contrary result because the government sought the subpoena for the purpose of discovering additional evidence of child pornography

that it suspected—but did not know—would be present on the defendant's laptop. The subpoena was "being utilized post-indictment to investigate additional charges," which the district court found impermissible. *Kirschner*, supra 823 F. Supp. 2d at 666. The case, moreover, was "not about producing specific documents—it [was] about producing specific testimony asserting a fact." *Id.* at 669. By producing the passwords, the defendant would communicate "information that may 'lead to incriminating evidence'" which "is privileged even if the information itself is not inculpatory." *Id.* (quoting *U.S. v. Hubbell*, 530 U.S. 27, 37, 120 S. Ct. 2037, 147 L. Ed. 2d 24 (2000) and *Doe v. U.S.*, *supra* 487 U.S. at 208 (1988) I.

In *U.S. v. Doe* (In re Grand Jury Subpoena Duces Tecum), 670 F.3d 1335 (11th Cir. Fla. 2012), government examiners similarly sought access to encrypted hard drives in order to search for child pornography files that they believed, but did not know, would be found therein. The hard drives were partitioned, and examiners could scrutinize unencrypted portions of the drives, on which they found no files. In testimony, a forensic examiner conceded that the encrypted portions of the hard drives might contain no data at all, and that the scope of his examination did not indicate a basis for the government agents' belief that data would be found in the encrypted portions. *Id.* at 1340. The Eleventh Circuit concluded that compelling Doe to decrypt and produce the contents of these drives would be testimonial on the part of Doe and that it would communicate information that was not a "foregone conclusion." *Id.* at 1346. It would communicate Doe's "knowledge of the existence and location of potentially incriminating files; of his possession, control, and

access to the encrypted portions of the drives; and of his capability to decrypt the files." *Id.* The court stressed that whether the actual content of the drives was testimonial was separate from whether the act of producing that content was testimonial, and the court did not address the former. *Id.* at 1342.

The issue of password protection was first examined at the state level by Massachusetts in *Com. v. Gelfgatt*, 11 N.E.3d 512 (Mass. 2014). In that case, Defendant Gelgatt was alleged to have improperly diverted funds received from his business dealings to himself for his personal use. In a lawful search of the defendant's home, law enforcement officers observed several computers that were powered on. The officers took photographs of the monitors, which displayed desktops with visible filenames or opened files. *Id.* at 516 n.6. The officers then seized the computers as evidence. They later discovered that they could not access the files on the seized computers because they were encrypted. The Massachusetts court concluded that, while decryption "would appear, at first blush, to be a testimonial communication," any information communicated would be a foregone conclusion that would not add to the government's sum total of information. *Id.* at 522. The court compelled the disclosure. Here, as in *Boucher*, the government sought access to documents that were previously viewed on the device itself, but were subsequently obscured by encryption. However, the court also maintained the distinction asserted in *Doe*, holding that the decryption of the devices was separate from their content, and this was the court's basis for allowing the decryption. As the officers were only asking that Doe enter the decryption key, he would not be disclosing any additional information to them.

Notably in dissent, Judge Lenk argued that the "artificial distinction between the act of entering the decryption key and the inevitable result of decrypting the devices obfuscates the realityof what the defendant is being compelled to disclose." *Id.* at 528-29.

In *Com. v. Baust*, 89 Va. Cir. 267 (Va. Cir. Ct. 2014), the city Circuit Court of Virginia Beach provided our first examination of the issue of password protection in the context of smartphones. The court found that requiring Baust to disclose the passcode to his encrypted smartphone would be testimonial and therefore he could not be compelled to do it. An assault victim in the case, the defendant's girlfriend, informed police that a video from a surveillance recording system capturing the assault had been transmitted to the defendant's phone. The victim was able to show police prior video that had been transmitted from the recording system to the defendant's phone which the defendant then texted to the victim. Here, the Virginia court addressed the testimonial nature of both the disclosure of the passcode and the underlying evidence the disclosure would reveal. Citing *Kirschner*, the court concluded that the passcode was a testimonial communication that the defendant could not be compelled to produce. As to the evidence that would be disclosed, both the victim and the defendant acknowledged that the "cell phone 'could have possibly' recorded the assault and the recording 'may exist' on the phone." *Id.* at 268. For the Virginia court, this was not sufficient to show that information received from the phone would be a foregone conclusion. *Id.* at 271.

In 2015, the United States District Court for the Eastern District of Pennsylvania found that an

employee could not be compelled to disclose his smartphone passcode even to his employer who owned the phone. *SEC Civil Action v. Huang*, 2015 U.S. Dist. LEXIS 127853, *1 (E.D. Pa. Sept. 23, 2015). In this case, the defendant's employer had issued the defendant and other employees smartphones for business use but allowed each employee to set their own secret passcode. Upon termination for alleged misconduct, the defendant relinquished his phone to his employer, who demanded the passcode to access its files. While the employer argued that the contents of the phone were its own business records, the court followed *U.S. v. Doe* and concluded that the passcode to the phone was separate from the phone's contents and, as it was wholly a product of the defendant's mind that had been shared with no one else, it was entitled to Fifth Amendment protection. *Id.* at *6.

In 2016, the Second District Florida Court of Appeals addressed this issue in *State v. Stahl*, 206 So. 3d 124 (Fla. Dist. Ct. App. 2d Dist. 2016). Defendant Stahl was caught in an act of voyeurism by the victim, who noticed him crouching under her skirt with an illuminated iPhone. Video surveillance from the store where the incident took place captured Stahl's actions. Law enforcement officers identified Stahl from the video and arrested him at his home. The State obtained a warrant to search the defendant's phone after confirming with the victim that it was the device used in the incident. However, the iPhone's encryption impeded access to its contents without the passcode. The trial court denied the State's motion to compel the passcode on the basis that it was testimonial and no foregone conclusion exception existed as "the State did not know 'for sure' whether a photo or video was on the phone." *Id.* at 130.

The Appellate Court disagreed and asserted that providing a passcode was not a testimonial act. Relying on *Doe v. U.S.*, *supra* 487 U.S. 201 and *U.S. v. Hubbell*, *supra* 530 U.S. 27, the court determined that, while the disclosure of a passcode may be communicative, it had no "testimonial significance." *Id.* at 134. Moreover, the court found that any testimony contained in the act of providing the passcode was a foregone conclusion if the State could show "with reasonable particularity" that "it already knew the evidence sought existed, the evidence was in the possession of the accused, and the evidence was authentic." *Id.* at 135 (citing *U.S. v. Doe*, *supra* 670 F.3d at 1344). The "evidence," the Florida court maintained, referred to the passcode, not the evidence to be found on the device. In so doing, the court agreed with the State's argument that it was seeking only the passcode and not any information it might find because of having that passcode. Limiting itself to certainty about the existence of the passcode itself, the Florida court's decision did not touch upon whether the State could show with reasonable particularity that the information sought from the encrypted iPhone was, in fact, contained on that iPhone.

In reviewing other jurisdictions' decisions on the issue currently before this court and reconciling them with New Jersey common law, statute, and our rules of evidence, this court must decide the following: (1) Whether the act of producing a cell phone PIN or password is testimonial and, if so, (2) Whether the "foregone conclusion" exception to the Fifth Amendment applies.

Using this framework, we turn to the facts of this case and the parties' arguments.

III.

At the time of the alleged offenses, Andrews was an Essex County Sheriff's Officer. The State charges that beginning in May 2015, Andrews exposed an undercover narcotics investigation to a known drug dealer, Quincy Lowery ("Lowery"), who was also the target of surveillance and a wiretap at the time of the alleged disclosures. The State specifically claims: (l) that Andrews told Lowery that he and his co-conspirators should discard their cell phones; (2) that Andrews told Lowery to examine his car and remove GPS tracking hardware that had been installed by the police; (3) that Andrews disclosed the identity of an undercover officer to Lowery; and (4) that Andrews identified an undercover police vehicle monitoring Lowery. The State contends that Andrews provided this information to help Lowery avoid law enforcement detection of his criminal activities and that these disclosures obstructed their criminal investigation and risked the lives of undercover officers.

On June 30, 2015, Lowery was arrested as part of a larger narcotics investigation known as "Operation TIDE." Following his arrest, Lowery gave two statements to detectives from the Essex County Prosecutor's Office, Professional Standards Bureau, detailing his relationship with Andrews and alleging that the officer assisted him in his drug dealing enterprise. This assistance came in the form of Andrews's purported willingness to share sensitive police information as opposed to selling drugs himself. Lowery testified before the Grand Jury consistent with his statements.

In addition, Lowery consented to data

extractions from his cell phone. Andrews's two cell phones with numbers (732) 318-7367 and (973) 342-9755 were also seized pursuant to a valid search warrant. Andrews did not consent to a search of his phones. Data extractions were unsuccessfully attempted by the State on Andrews's phones. However, Lowery's phones provided the State with physical evidence they allege is corroborative of his sworn statements to the police and the Grand Jury. Specifically, Lowery's cell phone and phone records contained 187 phone calls and numerous texts between Lowery and Andrews from May 18 through June 30, 2015 at all hours of the day and night. Lowery texted the license plate number H25-EKK to Andrews on June 20, 2015. This license plate was associated with a vehicle being used to surveil Lowery by the Essex County Prosecutor's Office as part of Operation TIDE. On June 22nd, a text from one of Andrews' phones to Lowery responded that they needed to meet and talk in person. Lowery's phone also contained the photo that Andrews purportedly used to identify the undercover police officer, text messages to and from Andrews about setting up in-person meetings and getting rid of cell phones, and the call history between them.

On June 2, 2016, Robert Andrews was indicted on six counts of criminal activity as follows: Two second-degree counts of Official Misconduct pursuant to N.J.S.A. 2C:30-2, by violating the laws of the State of New Jersey and multiple policies, procedures, rules and regulations of the Essex County Sheriff's Office ("ECSO"); Two third-degree counts of Hindering Apprehension or Prosecution pursuant to N.J.S.A. 2C:29-(3) (a) (2), by disclosing the identity of an undercover law enforcement officer

to a target of an active investigation; and Two fourth-degree counts of Obstructing the Administration of Law pursuant to N.J.S.A. 2C:29-1, by allegedly warning a target of a narcotics investigation of a wiretap and a GPS tracker on his vehicle and advising the target to dispose of his phones and how to remove the tracking device.

IV.

In this case, the court finds that the act of providing Defendant's PIN or passcode is not a testimonial act where the Fifth Amendment or New Jersey common and statutory law affords protection. As noted in *Doe v. U.S.*, *supra* 487 U.S. 201 and *U.S. v. Hubbell*, *supra* 530 U.S. 27, the disclosure of Defendant's PIN or passcode herein may be communicative, but it has no testimonial significance.[1] Allowing the State to access the call logs and text messages on Andrews's iPhones will add little to nothing to the aggregate of the Government's information. Moreover, the State of New Jersey has sufficiently demonstrated that any testimonial act contained in the act of providing the PIN or passcode is a foregone conclusion because the State has established with reasonable particularity that it already knows that (1) the evidence sought exists, (2) the evidence was in the possession of the accused, and (3) the evidence is authentic. In reconciling our New Jersey Supreme Court's direction in *In re Grand Jury Proceedings (Guarino)*, *supra* 104 N.J. 218, to focus on the contents of the cell phones, specifically the call logs and text messages, this court finds that the "foregone

[1] To ensure this, the court will review in camera the PIN or passcode prior to its disclosure to the state.

conclusion" exception and analysis provides Andrews with sufficient and adequate protections to ensure that his privilege against self-incrimination is not being violated herein.

First, the State provided evidence that there were 187 phone calls between Lowery and Andrews from May 18 through June 30, 2015 at all hours of the day and night. The State also established proof of text messages between the two including one from Lowery to Andrews with the license plate of the undercover vehicle purportedly exposed by Andrews. The text messages detail conversations setting up meetings between the two as well as statements regarding discarding cell phones. This is known from Lowery's sworn statements, his testimony at Grand Jury, the data extractions from Lowery's phone and phone records. The State knows what exists in Andrews's phone log and his texting application.

This case is similar to *State v. Stahl*, *supra* 206 So. 3d 124, where law enforcement knew exactly what it was looking for on the defendant's phone. In fact, the State in this case presented significantly more particularity than was offered in *Com. v. Gelfgatt*, *supra* 11 N.E.3d 512, *In re Boucher*, *supra* 2009 U.S. Dist. LEXIS 13006, *U.S. v. Doe*, *supra* 670 F.3d 1335, *U.S. v. Kirschner*, *supra* 823 F. Supp. 2d 665, *Com. v. Baust*, *supra* 89 Va. Cir. 267, or *SEC Civil Action v. Huang*, *supra* 2015 U.S. Dist. LEXIS 127853. There is an abundance of independent evidence showing that Andrews's phones contain the evidence sought. This is not merely a "fishing expedition" where the State does not know what it is looking for.

Next, Andrews's possession and ownership of

the phones has been definitively established. Andrews was in possession of the two iPhones when they were seized from him during the execution of a lawfully obtained warrant. As noted by the State in its moving papers and supporting documentation, Andrews specifically requested that the phones be returned to him. Lowery confirmed that Andrews was the person communicating with him via these cell phones.

Third, for the same reasons noted above, the proofs provided by the State in this case remove any doubt about the authenticity of Andrews's iPhones and their contents.

In this case, the State has established that the "foregone conclusion" exception to the Fifth Amendment privilege applies. The act of producing the PINs or passwords to his phones will not force Defendant to be a witness against himself. The declarations conveyed by the act of entering the PINs or passwords, including ownership and control of the iPhone, the content of the call logs, and the text messages sought are all "foregone conclusions" and not testimonial. The information contained in them is already known.

However, this decision does not give the State complete and unfettered access to Andrews's iPhones. The access allowed is specifically limited in scope to that which is contained within (1) the "Phone" icon and application on Andrews's two iPhones, and (2) the "Messages" icon and/or text messaging applications used by Andrews during his communications with Lowery as noted in the evidence attached to the State's moving papers. In no way shall the State be allowed to search through

any other icons, data, or applications for any additional evidence because the State has not produced any proofs that such other evidence already exists. Given the possibility that unfettered access to Andrews's iPhones could lead to the discovery of additional, now unknown evidence to be used against this Defendant, the review of the iPhones shall be performed by the State, in camera, in the presence of Andrews's defense counsel and the Court.

CONCLUSION

Therefore, the State's Motion compel Andrews to disclose his PINs or passwords to his two lawfully-seized iPhones is GRANTED subject to the limitations noted herein. An Order consistent with this decision is attached.

APPENDIX F

SUPERIOR COURT OF NEW JERSEY
LAW DIVISION - CRIMINAL PART
COUNTY OF ESSEX
Indictment No. 16-06-0178 1-1

———

STATE OF NEW JERSEY,
Plaintiff-Respondent,

v.

ROBERT ANDREWS,
Defendant-Appellant.

———

[FILED: May 22, 2017]

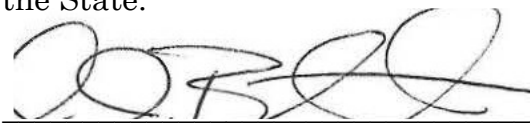
ORDER

THIS MATTER having been brought before the Court on motion of Alexander Albu, Assistant Prosecutor for Essex County appearing for the State, to compel discovery of iPhone PINs and passcodes, with notice to Charles J. Sciarra, Esq., attorney for the defendant ROBERT ANDREWS, and the Court having considered the moving papers and the oral arguments of counsel, and for good cause;

IT IS on this 22nd day of May, 2017;

ORDERED that the Plaintiffs Motion to Compel Discovery is hereby **GRANTED** for the reasons set out in the decision attached hereto. The access allowed is specifically limited in scope to that which is contained within (1) the "Phone" icon and application on Andrews's two iPhones, and (2) the "Messages" icon and/or text messaging applications used by Andrews during his communications with

Lowery as noted in the evidence attached to the State's moving papers. The search of the iPhones shall be performed by the State, in camera, in the presence of Andrews's defense counsel and the Court. The court will review in camera the PIN or passcode prior to its disclosure to the State.



HON. ARTHUR J. BATISTA, J.S.C.