SYLLABUS

This syllabus is not part of the Court's opinion. It has been prepared by the Office of the Clerk for the convenience of the reader. It has been neither reviewed nor approved by the Court. In the interest of brevity, portions of an opinion may not have been summarized.

State v. Robert Andrews (A-72-18) (082209)

Argued January 21, 2020 -- Decided August 10, 2020

SOLOMON, J., writing for the Court.

The Court considers 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.

The target of a State narcotics investigation, Quincy Lowery, advised detectives that defendant Robert Andrews, a former Essex County Sheriff's Officer, had provided him with information about the investigation and advice to avoid criminal exposure. The State obtained an arrest warrant for defendant, who was later released, and search warrants for defendant's iPhones, which were seized.

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. Lowery relayed his suspicion that he was being followed by police officers to Andrews and texted him the license plate 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 claimed that he also showed Andrews a picture of a man Lowery suspected was following him and that Andrews identified the individual as a member of the Prosecutor's Office. Lowery's cellphone records largely corroborated his allegations. Following their second interview with Lowery, the State obtained Communication Data Warrants for cellphone numbers belonging to Andrews and Lowery. The warrants revealed 114 cellphone calls and text messages between Lowery and Andrews over a six-week period. Andrews was indicted for official misconduct, hindering, and obstruction.

According to the State, its Telephone Intelligence Unit was unable to search Andrews's iPhones. A State detective contacted and conferred with the New York Police Department's Technical Services unit, as well as a technology company, both of which concluded that the cellphones' technology made them inaccessible to law enforcement agencies. The Federal Bureau of Investigation's Regional Computer Forensics Laboratory advised that it likewise 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.

The trial court rejected Andrews's arguments but 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 affirmed. 457 N.J. Super. 14, 18 (App. Div. 2018). The Court granted leave to appeal. 237 N.J. 572 (2019).

HELD: Neither federal nor state protections against compelled disclosure shield Andrews's passcodes.

1. The Fourth Amendment to the United States Constitution and Article I, paragraph 7 of the New Jersey Constitution require 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. Andrews does not challenge the search warrants issued for his cellphones or 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. 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. (pp. 15-17)

2. The Fifth Amendment right against self-incrimination applies only when the accused is compelled to make a testimonial communication that is incriminating. 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. In contrast to physical communications, if an individual is compelled to disclose the contents of his own mind, such disclosure implicates the Fifth Amendment privilege against self-incrimination. (pp. 17-20)

3. The Court reviews the origin and development of the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination in Fisher v. United States, 425 U.S. 391 (1976), United States v. Doe, 465 U.S. 605 (1984), and United States v. Hubbell, 530 U.S. 27 (2000). 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. (pp. 20-26)

4. 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 device, treating the contents of the devices as the functional equivalent of the contents of the documents at issue in the Supreme Court cases. Other courts have focused on the passcodes themselves as that which is produced. The Court reviews case law expressing both views. (pp. 26-36)

5. Here, 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 -- nor the phones themselves -- which are physical objects, not testimonial communications -- are protected by the privilege against self-incrimination. Therefore, production of the cellphones and their contents is not barred. But access to the cellphones' contents depends here upon entry of their passcodes. Communicating or entering a passcode requires facts contained within the holder's mind. It is a testimonial act of production. (pp. 36-37)

6. 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, the Court first considers to what it might apply -- the act of producing the passcodes, or the act of producing the cellphones' contents through the passcodes. 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, an approach that imports Fourth Amendment privacy principles into a Fifth Amendment inquiry. The compelled act of production in this case is that of producing the passcodes. Although that act of production is testimonial, 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. 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. (pp. 37-40)

7. Based on the record in this case, compelled production of the passcodes falls within the foregone conclusion exception. 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 exception thus applies. Therefore, the Fifth Amendment does not protect Andrews from compelled disclosure of the passcodes to his cellphones. The Court would reach the same conclusion if it viewed the analysis to encompass the phones' contents. The search warrants and record evidence of the particular content that the State knew the phones contained provide ample support for that determination. This was no fishing expedition. (pp. 40-41)

8. Turning to state law, the relevant 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). 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) 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 . . . ." 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. Finding that the passcodes are therefore not protected by statute, the Court considers state common law protections. (pp. 42-44)

9. New Jersey's common law privilege against self-incrimination derives from the notion of personal privacy established by the United States Supreme Court in Boyd v. United States, 116 U.S. 616 (1886). The Fisher Court overturned Boyd's protection of private documents. See 425 U.S. at 407. In In re Grand Jury Proceedings of Guarino, the Court affirmed its "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.'" 104 N.J. 218, 231 (1986). Thus, despite the shift at the federal level, the New Jersey common law privilege continues to consider whether evidence requested is of an inherently private nature. Noting as much yields the 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. Whether the inquiry is limited here to the passcodes or extended to the phones' contents, the result is the same. (pp. 44-47)

AFFIRMED.

JUSTICE LaVECCHIA, dissenting, is of the view that 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 law, protected by the Fifth Amendment and New Jersey common law. Justice LaVecchia explains that no United States Supreme Court case presently requires otherwise, no case from the Supreme Court of New Jersey has held otherwise, and that protection deserves utmost respect. In Justice LaVecchia's view, 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. Modern technology continues to evolve, bringing new problems; but it also may bring new solutions, and, Justice LaVecchia writes, 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, to date, its case law on accessing physical documents does not support the steps being taken here.

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.

SUPREME COURT OF NEW JERSEY

A-72 September Term 2018

082209

State of New Jersey,

Plaintiff-Respondent,

v.

Robert Andrews,

Defendant-Appellant.

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

Argued	Decided
January 21, 2020	August 10, 2020

Charles J. Sciarra argued the cause for appellant (Sciarra & Catrambone, attorneys; Charles J. Sciarra, of counsel, and Deborah Masker Edwards, on the briefs).

Frank J. Ducoat, Special Deputy Attorney General/Acting Assistant Prosecutor, argued the cause for respondent (Theodore N. Stephens, II, Acting Essex County Prosecutor, attorney; Frank J. Ducoat, of counsel and on the briefs, and Caroline C. Galda, Special Deputy Attorney General/Acting Assistant Prosecutor, on the briefs).

Elizabeth C. Jarit, Deputy Public Defender, argued the cause for amicus curiae Public Defender of New Jersey (Joseph E. Krakora, Public Defender, attorney; Elizabeth C. Jarit, of counsel and on the brief).

Andrew Crocker (Electronic Frontier Foundation) of the California bar, admitted pro hac vice, argued the cause for amici curiae Electronic Frontier Foundation, American Civil Liberties Union, and American Civil Liberties Union of New Jersey (Electronic Frontier Foundation, American Civil Liberties Union Foundation, and American Civil Liberties Union of New Jersey Foundation, attorneys; Andrew Crocker, Jennifer Granick (American Civil Liberties Union Foundation) of the California bar, admitted pro hac vice, Alexander Shalom, and Jeanne LoCicero, on the brief).

Christopher J. Keating argued the cause for amicus curiae New Jersey State Bar Association (New Jersey State Bar Association, attorneys; Evelyn Padin, President, of counsel, and Christopher J. Keating, Richard F. Klineburger, Brandon D. Minde, and Matheu D. Nunn, on the brief).

Megan Iorio (Electronic Privacy Information Center) of the District of Columbia bar, admitted pro hac vice, argued the cause for amicus curiae Electronic Privacy Information Center (Barry, Corrado, Grassi & Gillin-Schwartz and Electronic Privacy Information Center, attorneys; Megan Iorio, Alan Butler (Electronic Privacy Information Center) of the District of Columbia bar, admitted pro hac vice, Marc Rotenberg (Electronic Privacy Information Center) of the District of Columbia bar, admitted pro hac vice, and Frank L. Corrado, on the brief).

Matthew S. Adams argued the cause for amicus curiae Association of Criminal Defense Lawyers of New Jersey (Fox Rothschild, attorneys; Matthew S. Adams, Jordan B. Kaplan, Marissa Koblitz Kingman, and Victoria Salami, on the brief).

Lila B. Leonard, Deputy Attorney General, argued the cause for amicus curiae Attorney General of New Jersey (Gurbir S. Grewal, Attorney General, attorney; Lila B. Leonard, of counsel and on the brief).

Gregory R. Mueller, First Assistant Sussex County Prosecutor, argued the cause for amicus curiae County Prosecutors Association of New Jersey (Francis A. Koch, Sussex County Prosecutor, President, attorney; Gregory R. Mueller, of counsel and on the brief).

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."

---

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

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 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

---

[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

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.

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

---

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).

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.

---

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

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

---

[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.

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

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

[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).

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 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.

---

[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.

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 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

---

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

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 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 proceedings.

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.

State of New Jersey,

Plaintiff-Respondent,

v.

Robert Andrews,

Defendant-Appellant.

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.

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

Andrews resisted the State's motion, claiming a 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 Hubbell'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

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

---

time whether the Fifth Amendment has "a broader reach than Fisher holds," although suggesting that it may. Id. at 56.

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 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]

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

---

[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).

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. 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

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.

> 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).]

See, e.g., Commonwealth v. Davis, 220 A.3d 534, 550 (Pa. 2019) and other cases cited in Seo, ___ 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.

---

[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).

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.

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

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.

> 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 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.]

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 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]

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

[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 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))).

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. 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.