IN THE
NEW JERSEY SUPREME COURT
No. 082209 (A-72-18)

STATE OF NEW JERSEY, *Plaintiff–Respondent,* v. ROBERT ANDREWS, *Defendant–Appellant.*	Criminal Action: On Appeal from an Interlocutory Order of the Superior Court of New Jersey Appellate Division, Docket No. A-0291-17T4 Sat below: Hon. Joseph L. Yannotti, P.J.A.D., Hon. Garry S. Rothstadt, J.A.D., and Hon. Arnold L. Natali, Jr., J.A.D, t/a

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION, AND AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY

Alexander Shalom (021162004)
Jeanne LoCicero
AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY FOUNDATION
Post Office Box 32159
Newark, New Jersey 07102
973.642.2084

Jennifer Granick (*pro hac vice* pending)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, California 94111
415.343.0758

Andrew Crocker (*pro hac vice* pending)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
415.436.9333

July 22, 2019

Attorneys for Amici *Electronic Frontier Foundation, American Civil Liberties Union, American Civil Liberties Union of New Jersey*

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

STATEMENT OF INTEREST

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that works to protect free speech and privacy in the digital world. Founded in 1990, EFF has over 30,000 active donors and dues-paying members across the United States. EFF represents the interests of technology users in court cases and broader policy debates surrounding the application of law to technology. EFF is particularly interested in ensuring that individuals, and their constitutional rights, are not placed at the mercy of advancements in technology.

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with more than two million members and supporters dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. Since its founding in 1920, the ACLU has appeared before the Supreme Court and other federal courts in numerous cases implicating Americans' right to privacy, including as counsel in *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

The ACLU of New Jersey ("ACLU-NJ") is the New Jersey affiliate of the ACLU. It frequently appears before this Court on issues implicating search and seizure, *see*, *e.g.*, *State v. Lunsford*, 226 N.J. 129 (2016), and self-incrimination, *see*, *e.g.*, *State v. Wint*, 236 N.J. 174 (2018).

SUMMARY OF ARGUMENT

This case presents a question of first impression in this Court: whether the right against self-incrimination in the Fifth Amendment to the U.S. Constitution and under New Jersey common and statutory law prevents the State from forcing a defendant to disclose the passcodes to his encrypted iPhones, thereby delivering the phones' contents to the State for use against him in a criminal proceeding. Centuries of precedent and practice support the conclusion that, in cases like this one, the State cannot compel a suspect to recall and use information that exists only in his mind—such as a memorized password—in order to aid its prosecution of him. *See Curcio v. United States*, 354 U.S. 118, 128 (1957). This is no technicality; it is a fundamental protection of human dignity, agency, and integrity that the Framers enshrined in the Fifth Amendment to the U.S. Constitution.

The Appellate Division erroneously ruled that Andrews may be compelled to recall from memory and then reproduce to law enforcement the passwords for decrypting his phones. It reasoned that disclosure of Andrews' passwords from memory would only convey testimony about the "ownership, control, use, and ability to access the phones," and that the State had already established that these facts were a "foregone conclusion." *State v. Andrews*, 457 N.J. Super. 14, 29 (App. Div. 2018).

This ruling improperly expands the foregone-conclusion exception—a limited exception to the Fifth Amendment privilege against self-incrimination—to compel disclosure of the contents of Andrews' mind. This was error because the State cannot require a defendant to remember, enter, use, or disclose the contents of his mind, such as a memorized passcode any more than it can compel incriminating oral testimony from a defendant it "knows" to be guilty.

The "foregone-conclusion exception" cannot justify a different result in this case. *See United States v. Hubbell*, 530 U.S. 27, 44 (2000) (citing *Fisher v. United States*, 425 U.S. 391, 411 (1976)); *Doe v. United States* (*Doe II*), 487 U.S. 201, 208 n. 6 (1988). The U.S. Supreme Court has applied this exception in a single case, to the mere act of producing subpoenaed business documents prepared by and in the possession of third parties. *See Fisher*, 425 U.S. 391. But the exception has no application in the context of an attempt to compel defendants to provide testimony against themselves by reciting, writing, typing, or otherwise reproducing the contents of their minds. And even if this Court chose to expand the foregone-conclusion exception far beyond the unique circumstances in *Fisher*, it could only apply if the State could establish that any and all testimonial aspects of the act of producing *those records* (not merely the passcodes) would be foregone conclusions. *See United States v. Doe* (*Doe I*), 465 U.S. 605, 614 n.13 (1984); *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335, 1346

(11th Cir. 2012). In other words, the State would have to describe with reasonable particularity the specific digital records it seeks to compel the defendant to produce. *In re Grand Jury Subpoena*, 670 F.3d at 1347 (citing *Hubbell*, 530 U.S. at 45). The Appellate Division's focus on the passcode was erroneous and, if upheld, would vitiate Fifth Amendment protection for all digital devices.

Additionally, even if the United States Constitution did not prohibit the compelled disclosure of Andrews' password, New Jersey common law and statutory protections against self-incrimination forbid the trial court's order. The Appellate Division panel below acknowledged the requirement that it address state protections against self-incrimination, but it failed to appreciate the extent to which state law provides more robust safeguards than the U.S. Constitution.

This Court should reverse the Appellate Division's order compelling Andrews to disclose his passwords and unlock his phones.

STATEMENT OF FACTS AND PROCEDURAL HISTORY

Amici accept the Statement of Facts and Procedural History contained in the Appellate Division opinion. *Andrews*, 457 N.J. Super. at 30–34.

ARGUMENT

I. COMPELLED DISCLOSURE OR ENTRY OF A PASSCODE BY THE TARGET OF A CRIMINAL INVESTIGATION IS TESTIMONY PRIVILEGED BY THE FIFTH AMENDMENT.

A. The Fifth Amendment Prohibits the Compelled Disclosure or Use of the Contents of a Suspect's Mind.

The Fifth Amendment guarantees that "[n]o person shall be . . . compelled in any criminal case to be a witness against himself." U.S. Const. amend. V. To come within the self-incrimination privilege, an individual must show three things: that the evidence is (1) compelled, (2) testimonial, and (3) self-incriminating. *Hubbell*, 530 U.S. at 34. Only the second factor is at issue here.

Privileged testimony includes communications or any information, direct or indirect, verbal or non-verbal, that require a person to use "the contents of his own mind" to truthfully relay facts. *Id.* at 43 (citing *Curcio*, 354 U.S. at 128); *see Pennsylvania v. Muniz*, 496 U.S. 582, 595 & n.9 (1990) (Fifth Amendment right spares an accused from "having to share his thoughts and beliefs with the Government"). The testimonial nature of a communication does not turn on whether it is spoken, but whether it requires, by "word or deed," *Doe II*, 487 U.S. at 219 (Stevens, J., dissenting), a truthful "expression of the contents of an individual's mind." *Curcio*, 354 U.S. at 128 (Fifth Amendment prohibits compelling individual to "testify orally as to the whereabouts of nonproduced

records because [because it] requires him to disclose the contents of his own mind"); *see also Doe II*, 487 U.S. at 219 & n.1.

B. The Fifth Amendment Prohibits Compelled Recollection and Disclosure or Entry of a Memorized Passcode.

The trial court ordered Andrews to disclose his passcodes—by typing the passcodes into his iPhones and unlocking them[1]—in violation of the Fifth Amendment. First, compelled entry of a password constitutes a modern form of written testimony, which is categorically protected from compulsion. Second, even if the Court views this order as a demand for action rather than for written testimony, it is impermissible because it would require Andrews to use the contents of his mind. *Curcio*, 354 U.S. at 128.

Reciting, writing, typing, entering, or otherwise reproducing a password from memory is testimony protected by the Fifth Amendment. The entry of a computer password to decrypt an electronic device is equivalent to "telling an inquisitor the combination to a wall safe," *Hubbell*, 530 U.S. at 43, because it requires the defendant to reveal information stored in his mind. The Eleventh Circuit applied this principle in a case remarkably similar to this one, holding that

[1] The trial court described the effect of its order in various terms, including forcing Andrews to "disclose," Da. 51, "produc[e]," or "enter[]" his "PINs or passwords." Da. 50. It also purported to limit the State's "access" to the unlocked phones to "that which is contained within (1) the 'Phone' icon and application on Andrews' two iPhones, and (2) the 'Messages' icon and/or text messaging applications." Da. 51.

"the decryption . . . of the hard drives would require the use of the contents of Doe's mind and could not be fairly characterized as a physical act that would be nontestimonial in nature." *In re Grand Jury Subpoena*, 670 F.3d at 1346. Many other courts agree: production of computer passwords requires the suspect "to divulge through his mental processes his password." *United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010); *see also, e.g., Commonwealth v. Baust*, No. CR14-1439, 2014 WL 10355635, at *4 (Va. Cir. Ct. Oct. 28, 2014); *SEC v. Huang*, No. 15-cv-269, 2015 WL 5611644, at *3 (E.D. Pa. Sept. 23, 2015); *G.A.Q.L. v. State*, 257 So.3d 1058, 1061–62 (Fla. Dist. Ct. App. 2018); *In re Boucher*, No. 2:06-MJ-91, 2007 WL 4246473, at *1 (D. Vt. Nov. 29, 2007).

Moreover, opening a lock with a memorized passcode is testimonial regardless of whether the State learns the combination. *See United States v. Green*, 272 F.3d 748, 753 (5th Cir. 2001). For example, there is "no serious question" that asking an arrestee to disclose the locations of and open the combination locks to cases containing firearms compels "testimonial and communicative" acts as to his "knowledge of the presence of firearms in these cases and of the means of opening these cases." *Id*.

Because compelled disclosure or entry of Andrews' passcodes is testimonial and self-incriminating,[2] it is privileged by the Fifth Amendment. The analysis should end here.

II. *FISHER*'S LIMITED FOREGONE-CONCLUSION EXCEPTION HAS NO APPLICATION IN THIS CASE.

Even if the police know with reasonable certainty that someone committed a bank robbery, no one could credibly suggest that they could then be compelled to testify orally or in writing concerning a key fact because it was a "foregone conclusion." That is because the Fifth Amendment does not allow the government to compel suspects to speak, write, type, or otherwise reproduce the contents of their minds to aid in a prosecution. Some courts, however, including the Appellate Division below, have erroneously concluded that the foregone-conclusion exception permits the State to bypass this bedrock constitutional limitation and compel witnesses to disclose or enter their memorized passcodes into digital devices. This Court should reject that conclusion.

The U.S. Supreme Court applied a foregone-conclusion exception in a single unique case, *Fisher*, 425 U.S. 391, and has never again allowed the government to

[2] Importantly, the compelled testimony need not *itself* be incriminating to fall within the privilege, so long as the testimony provides a "link in the chain of evidence" needed to prosecute. *Hoffman v. United States*, 341 U.S. 479, 486 (1951); *Hubbell*, 530 U.S. at 38; *Doe II*, 487 U.S. at 208 n.6.

compel a testimonial act of production on those grounds. *See Hubbell*, 530 U.S. at 44; *Doe I*, 465 U.S. at 612–14.

In more than forty years since *Fisher*, lower courts, with few exceptions, have applied the foregone-conclusion exception only in the context of the production of specific, tangible business and financial records. The few courts that have found an order to recall or use a memorized password to be a foregone conclusion have erroneously stretched this rationale far beyond its limits.

Even if the foregone-conclusion exception could apply in cases involving passcodes, the State would have to show far more than the Appellate Division held to be required. Rather than simply demonstrating that an individual had *possession and control* over a device, the State would have to show with reasonable particularity that it has independent knowledge of *any and all information disclosed* by the compelled act of production—including that the specific, identifiable files it seeks are stored on that device. The State has not shown that here. Thus, even if this Court decides to expand a foregone-conclusion analysis to the compulsory entry of a memorized password to obtain private communications, that exception does not apply in this case.

A. The Foregone-Conclusion Exception Applies Only to the Production of Specified, Preexisting Business Records.

The facts in *Fisher* make clear just how limited any foregone-conclusion exception to the baseline Fifth Amendment rule against self-incrimination actually is. That case—unlike this one—did not involve compelled written or oral testimony. And law enforcement in that case—also unlike this one—did not seek private communication records. Rather, that case involved third-party subpoenas for business records.

In *Fisher*, the government sought the compelled production of documents created by accountants preparing the defendants' tax records and in possession of the defendants' attorneys. 425 U.S. at 412–13. The U.S. Supreme Court has long recognized that producing records in response to a subpoena or court order can have testimonial aspects protected by the Fifth Amendment—including implicit admissions concerning the existence, possession, and authenticity of the documents produced. *See id.* at 410. The *Fisher* Court nevertheless concluded that in the unique circumstances of the case, the Fifth Amendment did not immunize that act of producing those business documents. *Id*. at 411. That was because the government had independent knowledge of the existence and authenticity of documents created by accountants preparing the defendants' tax records and in possession of the defendants' attorneys. *Id.* at 412–13. But even as it ruled this way—creating a "foregone-conclusion" exception it had never applied before and

has never applied since—it made sure to warn of the limits of its decision. In particular, the Court called out the "[s]pecial problems of privacy" that might arise in the case of a subpoena seeking production of more sensitive documents like a personal diary, noting that such problems were not an obstacle to compelled production under *Fisher*'s facts. *Id.* at 401 n.7 (citing *United States v. Bennett*, 409 F.2d 888, 897 (2d Cir. 1969)); *see id.* at 394–95 nn.2–3.

Thus, *Fisher* stands for the proposition that if (1) the court order demands only an act of production and not disclosure of or reliance on the contents of one's mind, (2) the target neither created nor possesses the documents sought, and (3) the documents are not private in the way that a personal diary is, then the state may be able to compel the target's disclosure of those papers.

Unsurprisingly, given the highly specific factual circumstances in *Fisher*, in the nearly forty-three years since the case was decided, the Supreme Court has never again held that an act of disclosure is unprotected by the Fifth Amendment because the testimony it implies is a foregone conclusion. Indeed, the Court has only even considered foregone-conclusion arguments in two other cases, and it rejected them both times. Those cases involved the government seeking to compel the production of preexisting business or other financial records. *See Hubbell*, 530 U.S. at 44–45 (holding that the case "plainly [fell] outside of" the foregone-conclusion exception where the government sought "general business and tax

records that [fell] within the broad categories described in this subpoena" rather than specific, known files); *Doe I*, 465 U.S. at 612–14 (rejecting application of the foregone-conclusion exception where the subpoena sought several broad categories of general business records).

That the Court has never considered the foregone-conclusion exception outside of cases involving specific, preexisting business and financial records is unsurprising. These types of records constitute a unique category of material that, to varying degrees, has been subject to compelled production and inspection by the government for over a century. *See, e.g.*, *Braswell v. United States*, 487 U.S. 99, 104 (1988); *Shapiro v. United States*, 335 U.S. 1, 33 (1948).

Lower courts, too, have overwhelmingly applied the exception only in cases concerning the compelled production of specific, preexisting business and financial records. *See, e.g., United States v. Sideman & Bancroft, LLP*, 704 F.3d 1197, 1200 (9th Cir. 2013) (business and tax records); *United States v. Bright*, 596 F.3d 683, 689 (9th Cir. 2010) (credit-card records); *United States v. Gippetti*, 153 F. App'x 865, 868–69 (3d Cir. 2005) (bank and credit-card account records); *United States v. Bell*, 217 F.R.D. 335, 341–42 (M.D. Pa. 2003) ("tax avoidance" materials advertised on defendant business's website); *In re Grand Jury Subpoenas Served Feb 27, 1984*, 599 F. Supp. 1006, 1012 (E.D. Wash. 1984) (business-partnership records); *cf. Burt Hill, Inc. v. Hassan*, No. CIV.A. 09-1285, 2010 WL 55715, at *2

(W.D. Pa. Jan. 4, 2010) (contents of electronic storage devices used by defendants while employed by plaintiff).

On the other hand, courts routinely decline to apply the foregone-conclusion exception to cases involving the compelled production of physical evidence, such as guns or drugs, because the act of production in such cases would constitute an implicit admission of guilty knowledge. *See, e.g.*, *Commonwealth v. Hughes*, 404 N.E.2d 1239, 1244 (Mass. 1980); *State v. Dennis*, 558 P.2d 297, 301 (Wash. 1976).

Here, the State did not seek an order compelling the production of specific, tangible business or financial records, but rather an order compelling Andrews to disclose his memorized passcode to aid law enforcement in a search of calls and text messages stored on his device. The Appellate Division's reliance on the foregone-conclusion exception was therefore in error, and, as explained below, application of a foregone-conclusion exception beyond its typical narrow confines risks a broad erosion of the privilege against self-incrimination.

B. Even If the Foregone-Conclusion Exception Could Apply in this Context, the State Must Describe with Reasonable Particularity the Incriminating Files It Seeks.

Even assuming the foregone-conclusion exception could ever be applied to an order compelling a defendant to disclose his password and decrypt a digital device, the State first must demonstrate knowledge of the existence, location, ownership, and authenticity of the device and also identify with reasonable

particularity what files it will find stored there. *In re Grand Jury Subpoena*, 670 F.3d at 1346. That is a far higher bar for the State to clear than the mere "possession and control" standard applied by the Appellate Division.

The foregone-conclusion exception only applies where the State can show with "reasonable particularity" that it "already [knows] of the materials, thereby making any testimonial aspect a 'foregone conclusion.'" *See id.* at 1345 (citing *Hubbell*, 530 U.S. at 36 n.19, 38). By contrast, where an act of production implies a statement of fact the State does not already know, compelling that act would violate the Fifth Amendment. *See Hubbell*, 530 U.S. at 45 (no foregone conclusion where government did not have "any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent").

The majority of courts that have considered application of the foregone-conclusion exception to password-protected digital devices have held that investigators must know and be able to describe with reasonable particularity the discrete, tangible contents of a device—not merely that the device belongs to the defendant. For example, in *In re Grand Jury Subpoena*, the Eleventh Circuit held that an order requiring the defendant to produce a decrypted hard drive would be "tantamount to testimony by [the defendant] of his knowledge of the existence and location of potentially incriminating files; of his possession, control, *and* access to

the encrypted portions of the drives; and of his capability to decrypt the files." 670 F.3d at 1346 (emphasis added). The government could not compel the defendant to produce the information under the foregone-conclusion exception unless it could show with "reasonable particularity" the "specific file names" of the records sought, or, at minimum, that the government seeks "a certain file," and can establish that "(1) the file exists in some specified location, (2) the file is possessed by the target of the subpoena, and (3) the file is authentic." *Id.* at 1347 n.28.[3] But in that case, the government did not know "the existence or the whereabouts" of the records it sought. *Id*.; *see also United States v. Apple MacPro Computer*, 851 F.3d 238, 248 (3d Cir. 2017) (finding the foregone-conclusion exception satisfied where the government had evidence *both* that contraband files existed on the devices and that the defendant could access them).

A number of other courts have similarly held that law enforcement must know with reasonable particularity what information is on an encrypted device—not merely that the suspect knows the passcode. As the Florida Court of Appeals

[3] The Eleventh Circuit rejected the government's assertion that the use of encryption on the device in that case alone demonstrated that the suspect "was trying to hide something." *In re Grand Jury Subpoena*, 670 F.3d at 1347. Rather, it explained, "[j]ust as a vault is capable of storing mountains of incriminating documents, that alone does not mean that it contains incriminating documents, or anything at all." *Id*. Indeed, encryption is designed to protect the owner from thieves, fraud, hackers, and abusive spouses. Far from creating a "zone of lawlessness," encryption *prevents* crime.

explained, "when it comes to data locked behind a passcode wall, the object of the foregone conclusion exception is not the password itself, but the data the state seeks behind the passcode wall." *G.A.Q.L.*, 257 So. 3d at 1063. It is thus "not enough to know that a passcode wall exists, but rather, the state must demonstrate with reasonable particularity that what it is looking for is in fact located behind that wall." *Id*. at 1063–64; *see Huang*, 2015 WL 5611644, at *3 (State must know what "if anything, [is] hidden behind the encrypted wall"); *see also Doe I*, 465 U.S. at 613 n.12.

There is an immense difference between a foregone-conclusion exception for devices that focuses on mere possession and control of a device, and an exception that requires knowledge of the information to be uncovered through compelled provision of a password.

In the digital era, more and more evidence resides on personal digital devices, which contain "a digital record of nearly every aspect of [users'] lives." *Riley v. California*, 573 U.S. 373, 375 (2014). In this context, an "exception" to self-incrimination protections that allows law enforcement to force a suspect to reveal the contents of their device simply because they know the device belongs to the suspect would render protections for the "privacies of life" hollow by effectively "expand[ing] the contours of the foregone conclusion exception so as to swallow the protections of the Fifth Amendment." *G.A.Q.L.*, 257 So. 3d at 1063.

Every password-protected device "would be subject to compelled unlocking since it would be a foregone conclusion that any password-protected [device] would have a passcode." *Id*. Under this reasoning, the State could, as investigators unsuccessfully sought to do in *Matter of Residence in Oakland, California*, overcome a roomful of individuals' Fifth Amendment rights without any basis. 354 F. Supp. 3d 1010, 1017 (N.D. Cal. 2019) (request to compel every person present at residence to potentially unlock unspecified digital devices was overbroad).

By contrast, the reasonable-particularity requirement ensures that Fifth Amendment rights cannot be overcome merely by "categorical requests for documents the Government anticipates are likely to exist." *Huang*, 2015 WL 5611644, at *3. "Without reasonable particularity as to the documents sought behind the passcode wall, the facts of th[e] case 'plainly fall outside' of the foregone-conclusion exception and amount to a mere fishing expedition." *G.A.Q.L.*, 257 So. 3d at 1064 (quoting *Hubbell*, 530 U.S. at 44); *see also Huang*, 2015 WL 5611644, at *3 (SEC could not establish with "reasonable particularity" that any documents sought resided in the locked phones); *Boucher*, 2009 WL 424718, at *2 (subpoena for unencrypted hard drive enforceable where defendant admitted illegal downloads and agents observed thousands of file names reflecting apparent child pornography); *Matter of Residence in Oakland*, 354 F. Supp. 3d at 1017 (government lacks requisite prior knowledge of files on digital devices it

anticipates seizing because "smartphones contain large amounts of data, including GPS location data and sensitive records, the full contents of which cannot be anticipated by law enforcement").

A few courts, including the Appellate Division below, have in recent years misconstrued which standard should apply to the foregone-conclusion exception in the context of compelled decryption orders. These courts have accepted the argument that the foregone-conclusion exception is satisfied where investigators can show knowledge of the existence, location, and authenticity of a device and that the suspect knows the password to unlock it—rather than making the same showing regarding the evidence the State actually seeks. *See, e.g.*, *State v. Stahl*, 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016); *United States v. Spencer*, No. 17-CR-00259-CRB-1, 2018 WL 1964588, at *3 (N.D. Cal. Apr. 26, 2018); *Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 622 (Mass. 2014) (Lenk, J., dissenting) (majority compelled defendant to enter encryption key even though "the government has not shown that it has any knowledge as to the existence or content of any particular files or documents on any particular computer").[4]

[4] The Third Circuit's *MacPro* decision does not support the Appellate Division's conclusion that the State need only show that the ownership of the device is a foregone conclusion. *Andrews*, 457 N.J. Super. at 27. In *MacPro*, the Third Circuit did not hold that "possession and control" was the proper focus of the test, because it had no need to do so. Instead, its holding was based on the fact that the government provided evidence not only that the defendant owned the device and knew the password, but also that there were contraband files on the computer. *See*

Focusing only on the passcode misses the point. In all of these cases, including this one, law enforcement is seeking both the passcode *and* the underlying data. The Fifth Amendment prevents the State from acting as if the underlying data appears like "manna from heaven," divorced from the compelled disclosure of the password that protects this data. *In re Grand Jury Subpoena*, 670 F.3d at 1352 (quoting *Hubbell*, 530 U.S. at 33, 42). Moreover, the State's position in this case would impermissibly leave individuals "at the mercy of advancing technology." *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018). The Constitution, however, demands more. The State cannot compel Andrews to recall and enter his passcodes.

Assuming the Court believes that a foregone-conclusion exception could apply, the State nevertheless cannot compel Andrews to produce the decrypted contents of his iPhones without first demonstrating with reasonable particularity that it knows what documents it will find there. If a foregone-conclusion exception does apply, it must only be satisfied by a demonstration of "reasonable particularity" that the *existence* of these records is truly a foregone conclusion.

Apple MacPro, 851 F.3d at 248 ("Unlike *In re Grand Jury Subpoena*, the Government has provided evidence to show both that files exist on the encrypted portions of the devices and that Doe can access them.").

III. THE PROTECTIONS AGAINST SELF-INCRIMINATION CONTAINED IN NEW JERSEY COMMON LAW AND STATUTES INDEPENDENTLY SHIELD ANDREWS FROM COMPELLED DISCLOSURE OF THE PASSWORDS FOR HIS ENCRYPTED IPHONES.

The Appellate Division also made three critical errors in its analysis of state law. First, it understated the extent to which state law provides greater protection than the Federal Constitution. *Andrews*, 457 N.J. Super. at 30–34. Second, it undervalued the zone of privacy that surrounds cellphones. *Id.* at 31–32. And third, it improperly held that the existence of a warrant provided the government with a "superior right" of access to Andrews' cellphone. *Id.* at 32–34.

A. The State Provides Broad Protections Against Self-Incrimination.

New Jersey provides greater protections against self-incrimination—through the common law, rules, and statutes—than are provided by the United States Constitution. *In re Grand Jury Proceedings of Guarino* (*Guarino*), 104 N.J. 218, 229 (1986). The right against self-incrimination has enjoyed common law protection in New Jersey since colonial times, and the New Jersey Supreme Court recently reiterated that "[t]he importance of the common law right 'is not diminished by the lack of specific constitutional articulation.'" *State v. Vincenty*, 237 N.J. 122, 132 (2019) (quoting *State v. P.Z.*, 152 N.J. 86, 101 (1997)). The right against self-incrimination is "an integral thread in the fabric of New Jersey common law." *State v. Hartley*, 103 N.J. 252, 286 (1986). Moreover, this Court has

acknowledged that "[t]he privilege against self-incrimination . . . is one of the most important protections of the criminal law." *State v. Presha*, 163 N.J. 304, 312 (2000). The wide acceptance of this privilege and its broad interpretation "rest[s] on the view that compelling a person to convict himself of [a] crime is 'contrary to the principles of a free government' and 'abhorrent to the instincts of an American', that while [compelling self-incrimination] '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 v. United States*, 116 U.S. 616, 632 (1886)).[5]

New Jersey's tradition of providing protections against self-incrimination has deep roots. The privilege against self-incrimination was first codified as early as 1855, and was later incorporated into the New Jersey Rules of Evidence. *State v. A.G.D.*, 178 N.J. 56, 66–67 (2003). The current version of New Jersey's statutory protection against self-incrimination provides that "[e]very person has in any criminal action . . . a right not to be called as a witness and not to testify." N.J.S.A. 2A:84A-17(1). Another portion of the statute defines matters that will incriminate,

[5] While some U.S. Supreme Court cases have suggested that Boyd's underpinnings are no longer controlling in the Fifth Amendment context, this Court has never suggested any such change. *See, e.g.*, *Guarino*, 104 N.J. at 232 (acknowledging that the U.S. Supreme Court had departed from *Boyd*'s rationale, but finding that diversion inconsistent with "fundamental privacy principles underlying the New Jersey common-law privilege against self-incrimination" and therefore declining to follow that rationale).

explaining that a matter will incriminate "(a) if it constitutes an element of a crime"; "(b) is a circumstance which . . . 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)." N.J.S.A. 2A:84A-18. Finally, a third part of the statute, echoed by the New Jersey Rules of Evidence, sets forth four narrow exceptions to this privilege against self-incrimination, including an exception if "some other person or a corporation or other association has a superior right to the possession of the thing ordered to be produced." N.J.S.A 2A:84A-19(b); N.J.R.E. 503(b).

The language of N.J.S.A. 2A:84A-17 closely parallels the language of the Fifth Amendment of the United States Constitution. *See* U.S. Const. amend. V ("No person shall be . . . compelled in any criminal case to be a witness against himself."). And this Court has affirmed that "[i]n New Jersey, no person can be compelled to be a witness against himself." *Hartley*, 103 N.J. at 286 (quoting *State v. Zdanowicz*, 69 N.J.L. 619, 622 (1903)). Crucially, the Court found that the crux of the common law conception of the privilege against self-incrimination is the nature and content of the evidence, not "the testimonial compulsion involved in the act of producing them[.]" *Guarino*, 104 N.J. at 232. Therefore, the determination of whether an individual is being compelled to serve as a witness against himself

turns on the "notion of personal privacy," not whether the information sought is itself testimonial. *See id.* at 230, 232.

B. The Appellate Division Failed to Appreciate the Private Nature of Cellphones and Other Encrypted Devices.

In the case at bar, the panel below based its conclusion, in part, on the finding that the act of producing a phone passcode is testimonial with respect to "ownership, control, use, and ability to access the phones." *Andrews*, 457 N.J. Super. at 29. It held that such testimonial information is subject to the "foregone conclusion" exception to the Fifth Amendment, and the court saw "no basis for affording . . . greater protections against self-incrimination than those provided by the Fifth Amendment." *Id.* at 32. Moreover, the court below focused on whether the passcode itself was testimonial evidence rather than engaging with whether a phone passcode falls within the "special zone of privacy," which is protected by both the Fifth Amendment and this Court's precedent. *Compare id.* at 33 (concluding that "disclosure of cell phone passcodes does not involve the production of testimonial evidence"), *with Guarino*, 104 N.J. at 231 (affirming 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'" (quoting *Doe II*, 487 U.S. at 212–13)). This Court has held that the central inquiry with respect to whether or not the information sought is privileged against self-incrimination is whether it violates notions of personal privacy. *See Guarino*, 104

N.J. at 230. Therefore, the Appellate Division's failure to engage in this central inquiry, and instead to respond with a public policy argument, is a significant departure from the Court's precedent.

Even if the question of whether a phone passcode constitutes testimonial evidence is relevant to the inquiry, the panel below erred in its conclusion that the "forgone-conclusion" exception to the Fifth Amendment precludes New Jersey statutory protections. N.J.S.A. 2A:84A-17–18 protects individuals from self-incrimination, and elaborates that a matter is incriminating if it constitutes "a clue to the discovery" of incriminating evidence. N.J.S.A. 2A:84A-18.

In this case, a phone passcode is not only a clue, but the Rosetta Stone that would unlock Andrews' most private digital "papers," including those privileged records for which Andrews asserted his right against self-incrimination. This is no small thing. As the U.S. Supreme Court held in *Riley*, cell phones implicate significant privacy interests: "[m]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life[.]' The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." 573 U.S. at 403. Because compulsion here would violate Andrews' privacy in his iPhones, which

contain information far more revealing than any business papers, the state statutory privilege against self-incrimination applies.

C. The State Does Not Have a Superior Right of Access that Overcomes the Statutory Protection Against Self-Incrimination.

The Appellate Division found that Andrews' phone passcodes fall under an exception to the statutory protections against self-incrimination, asserting that "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[.]" *Andrews*, 457 N.J. Super. at 32–33 (quoting N.J.S.A. 2A:84A-19(b)). The statute provides that there is an exception to the statutory protection against self-incrimination "if some other person or a corporation or other association has a superior right to the possession of the thing ordered to be produced." N.J.S.A 2A:84A-19(b).

However, this is a misinterpretation of the statute. Including the government within the meaning of "association"—as the Appellate Division did, *Andrews*, 457 N.J. Super. at 32–33—requires the Court to ignore principles of statutory interpretation and vitiate statutory protections against self-incrimination *whenever* the State obtains a search warrant. Had the Legislature intended to include the government as "some other person or a corporation or other association," it could have done so explicitly. Some representative examples of the Legislature's use of the word 'association' are instructive here. The word "association" frequently appears in statutes alongside the words "foundation," "corporation," and

"individual." Under the maxim of *noscitur a sociis*—it is known by its neighbors—the meaning of words in a statute can be derived from the other words with which they are associated. *See*, *e.g.*, *State v. Watkins*, 193 N.J. 507, 525 (2008) (utilizing that principle of statutory construction). "Association" is repeatedly used in statutes in a list among other non-governmental entities. Therefore, it is best interpreted as a similar non-state entity. Further, many statutes mention "the State" or "government" in the same sentence or subsection as "association," which strongly indicates that the Legislature was consciously distinguishing between a government entity and an "association." *See, e.g.*, N.J.S.A. 40:33A-6(a) ("[a] county cultural and heritage commission . . . [may] apply for and accept any gifts, grants or bequests, including any grants from (1) the Federal Government or any agency thereof or (2) the government of this State or any of its agencies, instrumentalities or political subdivisions or (3) any foundation, corporation, association or individual"); *see also* N.J.S.A. 27:1A-7; N.J.S.A. 39:3-12.5(b); N.J.S.A. 40:33B-8(a); N.J.S.A. 52:27D-10.

Generally, "[w]hen [a legislature] provides exceptions in a statute, it does not follow that courts have authority to create others. The proper inference . . . is that [the legislature] considered the issue of exceptions and, in the end, limited the statute to the ones set forth." *United States v. Johnson*, 529 U.S. 53, 58 (2000); *see also Gangemi v. Berry*, 25 N.J. 1, 10 (1957) ("the limitation upon the general

legislative power is to be 'established and defined by words that are found written in that instrument,' and not by reference to 'some spirit that is supposed to pervade it or to underlie it'" (quoting *State v. Murzda*, 116 N.J.L. 219, 223 (1936))). And, more simply, had the Legislature intended to eliminate statutory self-incrimination protections whenever the State obtained a search warrant, it could have done so directly rather than through a contortion of the "superior right" analysis. But, of course, while both the Fourth Amendment's warrant requirement and the state protections against self-incrimination address privacy, their protections are not coextensive. Warrants alone cannot resolve the question of whether people are compelled to provide private information to convict themselves.

Even if the State did have a superior right to the contents of Andrews' phone, it cannot have a superior right to the contents of his mind. The exception built into the statute contemplates a situation where a person is asked to provide a business record of some sort, but where the government could obtain it through a third party who has a superior right to the document. *See*, *e.g.*, *United States v. Egenberg*, 443 F.2d 512, 517–18 (3d Cir. 1971) (holding that an accountant, as an agent for a client, must turn over incriminating tax returns because a third-party, the client, had a superior right to them). Thus, for example, a person could not rely on the statutory protection against self-incrimination to prevent the disclosure of a phone bill, if the State could also obtain it from the target's phone provider. In this

case, there is no third party with a superior right of access—or any access—to the contents of Andrews' mind.

IV. THE VALUES ANIMATING THE PRIVILEGE AGAINST SELF-INCRIMINATION REINFORCE THE CONCLUSION THAT THE STATE MAY NOT COMPEL PRODUCTION OR USE OF ENCRYPTION PASSWORDS.

The Supreme Court has explained that the self-incrimination privilege is rooted in our nation's "unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt[,]" "our respect for the inviolability of the human personality and of the right of each individual to a private enclave where he may lead a private life[,]" and "our realization that the privilege, while sometimes a shelter to the guilty, is often a protection to the innocent." *Doe II*, 487 U.S. at 212–13 (quotation marks omitted) (quoting *Murphy v. Waterfront Comm'n of N.Y. Harbor*, 378 U.S. 52, 55 (1964)).

Each element of the "cruel trilemma" is at work in cases of compelled disclosure or use of decryption passwords. The government gives those using encryption a choice: either provide the allegedly incriminating information you possess, lie about your inability to do so, or fail to cooperate and be held in contempt.[6] The privilege was designed to prevent suspects from facing this "trilemma" in the first instance. *See id*. at 212 (quoting *Murphy*, 378 U.S. at 55).

[6] A person who does not know or cannot remember the password to a device may be unable, not merely unwilling, to comply with a court's order. The self-

Forced disclosure or entry of a decryption key also encroaches on "the right of each individual to a private enclave where he may lead a private life." *Id.* (quoting *Murphy*, 378 U.S. at 55) (quotation marks omitted); *see also supra* Section III.C. Participating in modern society requires that one expose private information to communications providers—and from there potentially to advertisers, marketers, identity thieves, blackmailers, stalkers, spies, and more. Encryption is designed to protect individuals from these threats.

Encryption may impose obstacles to law enforcement in particular cases. So do window shades. It is sometimes true that constitutional protections interfere with law enforcement investigations. Nevertheless, law enforcement can pursue other means of building its case, as the State did here in reliance on incriminating statements by witnesses and evidence from third parties like telecommunications providers. Our Bill of Rights accepts that otherwise relevant evidence will sometimes be placed off-limits in order to strike a necessary balance between individual civil liberties and government power. Indeed, that is one of the Constitution's principal functions. Constitutional protections must be maintained, if not strengthened, in the digital age.

---

incrimination privilege ensures that an innocent person cannot be imprisoned for failing to comply with an impossible order.

CONCLUSION

Because the disclosure of Mr. Andrews' passcodes is inherently testimonial and because the foregone-conclusion exception cannot be expanded to allow the government to compel disclosure of the contents of a defendant's mind, this Court should reverse the trial court's order.

Dated: July 22 2019

_____

Alexander Shalom (021162004)
Jeanne LoCicero
AMERICAN CIVIL LIBERTIES
UNION OF NEW JERSEY
FOUNDATION
Post Office Box 32159
Newark, New Jersey 07102
Tel.: (973) 642-2084

Andrew Crocker (*pro hac vice* pending)
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, California 94109
Tel: (415) 436-9333

Jennifer Granick (*pro hac vice* pending)
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
39 Drumm Street
San Francisco, California 94111
Tel: (415) 343-0758

Attorneys for Electronic Frontier Foundation, American Civil Liberties Union, and American Civil Liberties Union of New Jersey