



PHIL MURPHY
Governor

SHEILA OLIVER
Lt. Governor

State of New Jersey
OFFICE OF THE PUBLIC DEFENDER

Appellate Section

JOSEPH J. RUSSO
Deputy Public Defender

31 Clinton Street, 9th Floor, P.O. Box 46003
Newark, New Jersey 07101
Tel. 973-877-1200 · Fax 973-877-1239

JOSEPH E. KRAKORA
Public Defender

July 19, 2019

ELIZABETH C. JARIT
Deputy Public Defender II
Attorney ID No. 036452011
Of Counsel and
On the Letter-Brief

**LETTER-BRIEF ON BEHALF OF THE OFFICE OF THE PUBLIC DEFENDER AS
AMICUS CURIAE**

SUPREME COURT OF NEW JERSEY
DOCKET NO. 082209
IND. NO. 16-06-1781

STATE OF NEW JERSEY,

: CRIMINAL ACTION

Plaintiff-Respondent,

: On Motion for Leave to Appeal
from an Interlocutory Order

v.

: of the Superior Court of New
Jersey, Law Division, Essex

Robert Andrews,

: County.

Defendant-Appellant.

: Sat Below:

: Hon. Joseph L. Yannotti, P.J.A.D.,
Hon. Garry S. Rothstadt, J.A.D.,
: Arnold L. Hon. Natali, Jr., J.A.D.

Honorable Judges:

Pursuant to Rule 2:6-2(b), kindly accept this letter-
brief on behalf of the Office of the Public Defender as

Amicus Curiae.

TABLE OF CONTENTS

	<u>PAGE NO.</u>
<u>STATEMENT OF PROCEDURAL HISTORY AND STATEMENT OF FACTS</u>	1
<u>LEGAL ARGUMENT</u>	1
<u>POINT I</u>	1
THE GOVERNMENT CANNOT COMPEL A PERSON TO DISCLOSE THE PASSCODE FOR THEIR PHONE BECAUSE DOING SO VIOLATES THE FIFTH AMENDMENT AND NEW JERSEY'S COMMON-LAW PRIVILEGE AND STATUTORY RIGHT AGAINST SELF-INCRIMINATION.....	1
A. The purpose of the Fifth Amendment right against self-incrimination is to protect against the cruel trilemma, which is precisely the situation individuals face when asked to disclose their passcodes.....	1
B. New Jersey has never adopted the foregone conclusion doctrine as an exception to our common-law privilege, nor should this Court now depart from decades of settled law.....	7
C. The disclosure of cell phone passcodes is protected by our statutory right against self-incrimination.....	14
D. Recent out-of-state cases demonstrate a trend toward protecting against government compulsion to disclose a cell phone passcode.....	17
<u>CONCLUSION</u>	20

STATEMENT OF PROCEDURAL HISTORY AND STATEMENT OF FACTS

For the purposes of this brief, Amicus Curiae Office of the Public Defender adopts the Statement of Facts and Procedural History of the trial and appellate opinions. State v. Andrews, 457 N.J. Super. 14, 18-21 (App. Div. 2018); (Da 9-27)¹

LEGAL ARGUMENT

POINT I

THE GOVERNMENT CANNOT COMPEL A PERSON TO DISCLOSE THE PASSCODE FOR THEIR PHONE BECAUSE DOING SO VIOLATES THE FIFTH AMENDMENT AND NEW JERSEY'S COMMON-LAW PRIVILEGE AND STATUTORY RIGHT AGAINST SELF-INCRIMINATION.

Amicus curiae Office of the Public Defender agrees with the arguments contained in the briefs filed by the Association of Criminal Defense Lawyers of New Jersey and the American Civil Liberties Union/Electronic Frontier Foundation. The Office of the Public Defender incorporates their arguments and adds the following.

- A. The purpose of the Fifth Amendment right against self-incrimination is to protect against the cruel trilemma, which is precisely the situation individuals face when asked to disclose their passcodes.**

The Fifth Amendment was drafted in response to "certain historical practices, such as ecclesiastical inquisitions and

¹ "Da" refers to the appendix of Defendant's Appellate Brief.
"Pmb" refers to the State's Brief in Opposition to the Defendant's Motion for Leave to Appeal
"1T" refers to the transcript dated April 21, 2017

the proceedings of the Star Chamber, which placed a premium on compelling subjects of the investigation to admit guilt from their own lips." Anderson v. Maryland, 427 U.S. 463, 470 (1976) (quotation omitted). At these proceedings, suspects were placed in the untenable position of being compelled to speak, and thus subjected to the "cruel trilemma of self-accusation, perjury or contempt[.]" Murphy v. Waterfront Comm'n of New York Harbor, 378 U.S. 52, 55 (1964). In protecting suspects from compulsion, the right against self-incrimination "registers an important advance in the development of our liberty." Ullmann v. United States, 350 U.S. 422, 427 (1956).

Based on the underlying purpose of the Fifth Amendment, a communication is considered testimonial "[w]henver a suspect is asked for a response requiring him to communicate an express or implied assertion of fact or belief," so that "the suspect confronts the 'trilemma' of truth, falsity, or silence[.]" Pennsylvania v. Muniz, 496 U.S. 582, 597 (1990). Unlike compelling a person to be the source of physical evidence by, for example, providing a blood sample or participating in a line-up, testimonial communications force a person to "choose between truthfully or falsely revealing" incriminating information within their own mind. Id. at 597-98.

The privilege "spare[s] the accused from having to reveal, directly or indirectly, his knowledge of facts relating him to

the offense or from having to share his thoughts and beliefs with the Government." Doe v. United States, 487 U.S. 201, 213 (1988). Thus, "[t]here are very few instances in which a verbal statement, either oral or written, will not convey information or assert facts" and "[t]he vast majority of verbal statements [] will be testimonial and, to that extent at least, will fall within the privilege." Id. at 213-14.

In Muniz, the United States Supreme Court found that simply asking the defendant for the date of his sixth birthday "required a testimonial response" because he was confronted by the cruel trilemma. 496 U.S. at 598 (where answer demonstrated his impairment and was therefore incriminating). Conversely, "compell[ing] writing and voice exemplars did not involve situations in which suspects were asked to communicate any personal belief or knowledge of facts, and therefore the suspects were not forced to choose between truthfully or falsely revealing their thoughts." Id. at 597-98.

When law enforcement asks a suspect to reveal the passcode to his phone, that person is placed in the situation of either 1) being compelled to use the contents of his own mind to incriminate himself by communicating information to the government; 2) lying to the police by providing an incorrect code or claiming that he does not know the passcode; or 3) remaining silent and risk being held in contempt or charged with

obstruction. This is precisely the cruel trilemma that the Fifth Amendment protects against. Compelling a person to disclose their passcode is therefore a protected testimonial communication. No further analysis is necessary.

Despite this protection, the Appellate Division and several other jurisdictions have applied the "foregone conclusion doctrine" as an exception to the Fifth Amendment right against self-incrimination when passcodes are concerned. As other parties have pointed out, however, the United States Supreme Court has only applied the foregone conclusion doctrine once, to the production of business records created by and in the possession of a third-party. Fisher v. United States, 425 U.S. 391 (1976).² The reasoning of the foregone conclusion doctrine, however, does not pertain to compelling the disclosure of passcodes.

The basis of the exception is that because the compelled speech does not add anything to the government's case, the suspect is not being forced to incriminate himself. Fisher, 425 U.S. at 411. The defendant is merely asked to "surrender" what

² Application of this doctrine beyond this type of evidence is uncertain. That the Court has required heightened constitutional protections for cell phone evidence suggests that this exception does not apply in this context. See Carpenter v. United States, ___ U.S. ___, 138 S.Ct. 2206, 2219-20 (2018) (holding that third-party doctrine does not apply to cell site location information); Riley v. California, 573 U.S. 373, 394 (2014) (holding that search incident to arrest exception does not apply to cell phones on arrestee's person).

is already known; because no additional information is provided to law enforcement, the defendant does nothing to assist in his own prosecution. Ibid. The cruel trilemma is not implicated. As a result, there is no "extortion of information from the accused himself that offends our sense of justice." Id. at 398.

While this analysis may work in the context of known business records created and possessed by third parties, it is not suited to assess passcodes protecting the contents of cell phones. As explained by the defendant and amici, the foregone conclusion doctrine must be assessed concerning the contents of the phone, not just the passcode itself. By disclosing a passcode, the suspect is providing all of the underlying contents to the government. Critically, without the compelled passcode, the government does not possess evidence to be used in the defendant's prosecution. Even in cases where the government has very good reason to believe a device contains evidence of criminality (because, for example, an officer observed this evidence on the device prior to it being locked), compelling a person to enter their passcode in order to access this evidence provides the State with, at the very least, corroborating evidence that bolsters its case and assists in the prosecution. Because the suspect remains faced with the cruel trilemma, disclosing a passcode is more than mere surrender.

Here, the State seeks to search two phones, relying on statements of a cooperating witness alleging defendant's criminal activity and the use of his cell phone to engage in this behavior. Notably, these statements were provided by a witness with the hope that doing so would keep his niece from being arrested and mitigate pending charges, undermining these statements' trustworthiness. (Da 28-66; Da 69-79) In addition, the State relies on call logs and two text messages from the witness to the defendant obtained from the witness's phone. (1T17-20; 11-3 to 12-18)

The State concedes that they do not know what is on the phone, maintaining: "At this point, it remains unknown for sure (though the State has its well-grounded suspicions) what the limited analysis of defendant's iPhones will unearth." (Pmb 7) The State does not know the length of the calls between the parties, the number of text messages, or the contents of either. The State does not know the passcode (otherwise it would not need to compel it). There is even a dispute as to whether the defendant is the actual owner of the phones and knows the passcode.³ Compelling the defendant to disclose the passcode

³ At the hearing, defense counsel noted that although the two phones were seized from the defendant's person, neither are in his name and they were turned over after defendant arrived directly from work. (1T41-25 to 43-4) Thus, even if the proper analysis for the foregone conclusion doctrine focuses solely on the passcode, only after its disclosure would the State know if

would provide the government with troves of new information beyond the State's "suspicions." Because this compelled communication is not one of mere surrender, the foregone conclusion doctrine cannot apply. To hold otherwise would gut the Fifth Amendment.

B. New Jersey has never adopted the foregone conclusion doctrine as an exception to our common-law privilege, nor should this Court now depart from decades of settled law.

New Jersey's "state-law privilege against self-incrimination offers broader protection than its federal counterpart under the Fifth Amendment." State v. Muhammad, 182 N.J. 551, 568 (2005). Like the Fifth Amendment, our common-law privilege against self-incrimination "rest[s] 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 Phillo, 11 N.J. 8, 15-16 (1952) (Brennan, J.) (quoting Boyd v. United States, 116 U.S. 616, 632 (1886)). But while federal jurisprudence departed from Boyd's privacy emphasis, "the notion of personal privacy first embodied" in Boyd remains

defendant has access to either of the phones and whether the passcode provided is authentic. The State cannot meet the foregone conclusion doctrine for even the passcode on its own.

"central to our state common-law conception of the privilege against self-incrimination." In re Grand Jury Proceedings (Guarino), 104 N.J. 218, 230 (1986). Consequently, unlike the federal right, the focus of the New Jersey privilege is not on compulsion but on whether the "contents of the evidence sought lies within that sphere of personal privacy" considered a "private enclave" of an individual's life. Id. at 231 (finding that business records are not within the "private enclave" protected by our state privilege).

A person's passcode to their phone -- and the information hidden as a result of that passcode -- is evidence that lies squarely within the sphere of personal privacy protected by our common-law privilege. New Jersey has consistently held that people have an expectation of privacy concerning the contents and data of their phones. See, e.g., State v. Earls, 214 N.J. 564, 569 (2013). The United States Supreme Court too recognizes the great intrusion of privacy caused by the search of a cell phone, noting that its vast contents can reconstruct "the sum of an individual's private life." Riley, 573 U.S. at 394. Cell phones are a ubiquitous part of each of our daily lives, containing volumes of personal information. Their contents reveal the owner's innermost thoughts, as well as reams of data about the owner's past whereabouts and personal associations. That a phone is protected by a password is itself evidence that

the contents are within an individual's "sphere of personal privacy."

The Appellate Division opinion recited this law but never engaged in any analysis about whether the information sought is part of the "private enclave" protected by our common-law right. Andrews, 457 N.J. Super. at 30-31. Instead, it summarily determined that because the state privilege "would essentially preclude the State from obtaining the contents of any passcode-restricted device as part of a criminal investigation," the communication of disclosing a passcode should not be protected. Id. at 32. The panel held that as long as the State has established the elements of the foregone conclusion doctrine, the government may compel disclosure. Ibid. This conclusion is fundamentally flawed for two reasons: 1) law enforcement demands cannot trump constitutional rights; and 2) New Jersey has never before, and should not now, adopted the foregone conclusion doctrine.

Preliminarily, the appellate panel's conclusion about law enforcement need is factually incorrect. The right against self-incrimination only protects a person from being forced to assist in his own prosecution. This does not mean that the government is precluded from seizing and searching a phone for which it has a warrant. It only means that the government cannot force an individual to assist in making that search easier or more

efficient. Without assistance from the cell phone owner, the government is still permitted to hack into the phone (just as the government could break down the door to a home). Law enforcement agencies nationwide are doing just that.

At least one company, Cellebrite, has the ability to hack into any locked phone. Andy Greenberg, [Cellebrite Says It Can Unlock Any iPhone for Cops](https://www.wired.com/story/cellebrite-ufed-ios-12-iphone-hack-android/), Wired (June 14, 2019), <https://www.wired.com/story/cellebrite-ufed-ios-12-iphone-hack-android/>. Another product, Graykey, has been used by law enforcement agencies nationwide to hack into most⁴ iPhone models. Thomas Brewster, [New York Cops Are Hacking iPhones with Secretive \\$15,000 Graykey](https://www.forbes.com/sites/thomasbrewster/2018/07/03/apple-iphones-hacked-by-grayshift-graykey-in-new-york/), Forbes (July 3, 2018) <https://www.forbes.com/sites/thomasbrewster/2018/07/03/apple-iphones-hacked-by-grayshift-graykey-in-new-york/>. There are thus other means at the government's disposal to obtain access to cellphones without compelling a person to assist the government in his own prosecution.

⁴ In October of 2018, it was revealed that Apple had changed its security features so that Graykey may not be able to hack into iPhones running iOS 12 or above. Thomas Brewster, [Apple Just Killed the 'Graykey' iPhone Passcode Hack](https://www.forbes.com/sites/thomasbrewster/2018/10/24/apple-just-killed-the-graykey-iphone-passcode-hack/), Forbes (Oct. 24, 2018), <https://www.forbes.com/sites/thomasbrewster/2018/10/24/apple-just-killed-the-graykey-iphone-passcode-hack/>. One police captain commented, however: "Give it time and I am sure a 'workaround' will be developed ... and then the cycle will repeat. Someone is always building a better mousetrap, whether it's Apple or someone trying to defeat device security." Ibid.

More fundamentally, whenever this Court is asked to decide whether a law enforcement tactic abides by the Constitution, the government maintains that without this practice it will be impossible to police criminality. Yet each time constitutional rights are reaffirmed, history demonstrates that placing limits on police power does not hamper the ability of law enforcement to protect the public. See, e.g., Fact Sheet: Stop and Frisks's Effect on Crime in New York City (Oct. 7, 2016), <https://www.brennancenter.org/analysis/fact-sheet-stop-and-frisks-effect-crime-new-york-city> (finding that after "stop-and-frisk" policy ended, crime rates fell despite claims that "stop-and-frisk was essential for fighting crime").

Regardless, constitutional rights cannot bend for the demands of law enforcement. Because the "'needs of law enforcement stand in constant tension with the Constitution's protection of the individual against certain exercises of official power,'" it "'is precisely the predictability of these pressures that counsels a resolute loyalty to Constitutional safeguards.'" State v. Hemele, 120 N.J. 182, 221 (1990) (quoting Almeida-Sanchez v. United States, 413 U.S. 266, 275 (1973) (Powell, J., concurring)). In the context of the Fifth Amendment, the United States Supreme Court observed the importance of safeguarding the right against the potential for government abuse:

Too many, even those who should be better advised, view this privilege as a shelter for wrongdoers. They too readily assume that those who invoke it are either guilty of crime or commit perjury in claiming the privilege. Such a view does scant honor to the patriots who sponsored the Bill of Rights as a condition to acceptance of the Constitution by the ratifying States. The Founders of the Nation were not naive or disregarding of the interests of justice.

[Ullman, 350 U.S. at 426-27.]

The Court cautioned that the right protects against "the tendency in human nature to abuse power," specifically by "law-enforcing agencies." Id. at 428. To protect against such abuses, the Court has "admonished that [the right] should be given a liberal application," as our "forefathers" were well-aware that the "privilege against self-incrimination serves as a protection to the innocent as well as to the guilty." Id. at 427.

Second, the Appellate Division's application of the foregone conclusion doctrine to the New Jersey common-law right was without precedent. New Jersey has never applied or adopted the foregone conclusion doctrine as an exception to the state common-law privilege. Over forty years ago, in Guarino, this Court had the opportunity to do so concerning business records to align our jurisprudence with Fisher. 104 N.J. 218. Instead, the Court chose to continue to apply a privacy-based analysis, finding that the business records were not within the zone of privacy sought to be protected by our common-law right. Id. at 232. Though the dissent recognized the foregone conclusion

doctrine as an exception to the Fifth Amendment, id. at 242 n.2, the majority declined to mention it in its analysis of the state common-law privilege.

Here, the appellate panel determined that the foregone conclusion exception applies, bypassing any discussion of whether a passcode and the contents revealed are within the private enclave protected by our state privilege. The court gave no reason for this departure from settled law besides an alleged law enforcement need.⁵ As explained above, the purpose of the common-law right against self-incrimination is to protect against government intrusions. Allowing law enforcement "need" to dictate the metes and bounds of the very rights enacted to protect against police power renders these rights meaningless.

Finally, the foregone conclusion doctrine has been sharply criticized. In creating this exception to a constitutional right, the United States Supreme Court "introduced the foregone conclusion doctrine without explaining either its origins or the scope of its operation." Robert P. Mosteller, Simplifying Subpoena Law: Taking the Fifth Amendment Seriously, 73 Va. L.

⁵ The existence of a warrant is of no moment. A warrant requires probable cause and protects different constitutional rights. As explained in State v. Kelsey, "the right against self-incrimination protects a defendant from being 'subpoenaed to produce the gun or the loot, no matter how probable the cause, for the Fifth [Amendment] protects the individual from coercion upon him to come forward with anything that can incriminate him.'" 429 N.J. Super. 449 (App. Div. 2013) (quoting In re Addonizio, 53 N.J. 107, 129 (1968)).

Rev. 1, 9 (1987). Its implicit reasoning that "the testimony inherent in production is irrelevant where the prosecution possesses abundant proof without it . . . flies in the face of the law of evidence." Id. at 31. An alternative rationale that a "de minimis threat of incrimination" does not offend the Fifth Amendment also fails, since "a statement made by a defendant in response to police interrogation remains incriminating in fifth amendment terms even if the police already have other substantial evidence on the issue." Ibid. In declining to apply the exception in Hubbell, even the United States Supreme Court acknowledged the doctrine's lack of clarity. United States v. Hubbell, 530 U.S. 27, 44 (2000). This Court should not adopt an exception to a fundamental state right that lacks clarity and rests on questionable reasoning.

There is no reason to depart from settled jurisprudence and adopt a doctrine at odds with our decades-old, privacy-based framework. Because the government may not compel a person to reveal information within that "private enclave" of a person's life, New Jersey's common law privilege protects against the State forcing a person to disclose the passcode on their phone.

C. The disclosure of cell phone passcodes is protected by our statutory right against self-incrimination.

In addition to the common-law right, the Legislature codified the right against self-incrimination in N.J.S.A.

2A:84A-19. See also N.J.R.E. 503 (with identical language). The statute guarantees "every natural person" a "right to refuse to disclose in an action or to a police officer or other official any matter that will incriminate him or expose him to a penalty or a forfeiture of his estate" with four enumerated exceptions. N.J.S.A. 2A:84A-19; N.J.R.E. 503 (emphasis added). The first deals with disclosure of physical identifying characteristics such as a fingerprint. N.J.S.A. 2A:84A-19(a); see State v. Green, 209 N.J. Super. 347, 353 (App. Div. 1986) (right does not apply if evidence sought does "not seek to compel from the defendant any knowledge he might have" or involve his "communicative facilities in any way"). The second deals with court orders for physical property belonging to another person having a "superior right of possession" over that object. N.J.S.A. 2A:84A-19(b); see State v. Cassalty, 93 N.J. Super. 111, 122 (App. Div. 1966), certif. denied, 48 N.J. 448 (1967). The third involves the "required records exception," pertaining to documents maintained by law. N.J.S.A. 2A:84A-19(c); see State v. Stroger, 97 N.J. 391, 405 (1984), cert. denied, 469 U.S. 1193 (1985). The last concerns impeachment evidence if the person voluntarily waives his right and testifies. N.J.S.A. 2A:84A-19(d); see State v. Buonadonna, 122 N.J. 22, 37 (1991).

The Appellate Division incorrectly found that the second exception applies here, averring that the State has a "superior

right of possession" based on the issuance of search warrants. Andrews, 457 N.J. at 32-33. Contrary to the panel's belief, a search warrant does not extinguish a person's possessory rights over a place or object. For example, the search warrant for a home does not give law enforcement a "superior right of possession" than the homeowner. The government could not sell the home based on the warrant. Nor could it even sell the phones it now possesses. It merely gives the government the authority to access and conduct a search therein.

Applying the language of the statute, a person may not be compelled to disclose "any matter" that will incriminate him. N.J.S.A. 2A:84A-18 further explains that a "matter will incriminate" if it "is a clue to the discovery of a matter" that "constitutes an element of a crime" or "is a circumstance which with other circumstances would be a basis for a reasonable inference of the commission of such a crime." This broad language certainly encompasses a passcode revealing the duration of calls or texts with a cooperating witness. None of the enumerated exceptions apply to this statutorily guaranteed right. Nor is the foregone conclusion doctrine listed as one of its exceptions. Because a passcode does not fall into any of the exceptions for the statutory-based privilege, and because this Court cannot overrule the intent of the Legislature, the State may not compel a defendant to disclose his passcode.

D. Recent out-of-state cases demonstrate a trend toward protecting against government compulsion to disclose a cell phone passcode.

The Office of the Public Defender agrees with the interpretation by defendant and amici of the numerous state and federal cases concerning compelled disclosure of passcodes. Since this Court granted leave to appeal, several courts in other jurisdictions have addressed this issue. All apply the Fifth Amendment framework for determining the scope of the protection. And all have reached the conclusion that provision of the passcode is a testimonial communication. Though courts differ in application of the foregone conclusion doctrine, the latest opinions demonstrate a curtailing of its application.

In People v. Spicer, 2019 Ill. App. LEXIS 129 (Ill. App. Ct. Mar. 7, 2019), the court found that disclosure of the passcode was a testimonial act but that the foregone conclusion doctrine did not apply. Id. at *10. "The focus," the court explained, "is not on the passcode but on the information the passcode protects." Ibid. Because the state could not provide a particularized description of information it was seeking, the court found that the state was engaging in a "fishing expedition." Id. at *11. Even if the focus was on the passcode, the court explained that while "the State is aware that the passcode existed and the [defendant] knew it, the State could

not know that the passcode was authentic until after it was used to decrypt [defendant's] phone." Id. at *12.

The United States District Court for the Northern District of California held that using a biometric feature⁶ to unlock a phone is a testimonial act and that the foregone conclusion doctrine did not apply. In re Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1015-1018 (N.D. Cal. 2019). The court explained that a biometric feature serves the same purpose as a passcode, and forcing someone to place their finger on a digital device is "fundamentally different" than submitting a person to fingerprinting because the very act "concedes that the phone was in the possession and control of the suspect, and authenticates ownership or access to the phone and all of its digital contents." Id. at 1006. The court further explained that "mobile phones are subject to different treatment than more traditional storage devices, such as safes, and should be afforded more protection." Id. at 1017. It concluded that the foregone conclusion doctrine does not apply because the state "inherently lacks the requisite prior knowledge of the information and documents" contained on the phone so that their disclosure "would not be a question of mere surrender." Id. at 1017-18.

⁶ Whether a biometric feature passcode is testimonial is not a question before this Court.

And in United States v. Maffei, the United States District Court for the Northern District of California found that provision of a passcode was testimonial because it “bears a striking similarity to telling an inquisitor the combination to a wall safe.” 2019 U.S. Dist. LEXIS 70314, at *18-19 (N.D. Cal. April 25, 2019) (internal quotation and citation omitted). The court suppressed the evidence because the defendant was asked for the passcode after invoking her right to counsel. Id. at *25.

While a Missouri appellate court found that compelled disclosure of a passcode was testimonial and that the foregone conclusion exception applied to permit disclosure, it did so under a narrow reading of the doctrine based on the fact that the police had personally observed the defendant voluntarily enter his passcode into his phone in order to access it. State v. Johnson, 2019 Mo. App. LEXIS 297, *40 (Mo. Ct. App. Mar. 5, 2019). Consequently, “the existence of the passcode, its possession or control by him, and the passcode’s authenticity” were already known to the State. Id. at *41.

Lastly, in Commonwealth v. Jones, 117 N.E.3d 702, 716 (Mass. 2019), the Massachusetts Supreme Court narrowed the State’s ability to compel a passcode pursuant its prior ruling in Commonwealth v. Gelfgatt, 11 N.E.3d 605 (2014). In Jones, the question before the Court was what burden of proof was needed to

satisfy the foregone conclusion doctrine discussed in Gelfgatt, 117 N.E.3d at 707. Though the Commonwealth argued for a clear and convincing evidence standard, the Court concluded that a high standard of proof was required so that the government is "certain that the compelled act of production will not implicitly convey facts not otherwise known to" law enforcement. Id. at 716. Thus, the Court held that the Commonwealth must meet its burden beyond a reasonable doubt in order for the foregone conclusion doctrine to apply. Ibid.

These cases demonstrate a national trend firmly concluding that disclosing one's passcode is a testimonial communication, while tightly circumscribing the instances in which compelled disclosure is nonetheless permitted.

CONCLUSION

For the foregoing reasons, this Court should hold that New Jersey's common-law privilege protects against government compulsion to disclose the passcode to a phone.

Respectfully submitted,

JOSEPH E. KRAKORA
Public Defender
Attorney for the Office of the Public Defender

BY: Elizabeth C. Jarit
ELIZABETH C. JARIT
Deputy Public Defender II