

NEW JERSEY STATE BAR ASSOCIATION
New Jersey Law Center
One Constitution Square
New Brunswick, New Jersey 08901
(732)937-7505

State of New Jersey,	:	SUPREME COURT OF NEW JERSEY
	:	Docket No. 082209
Plaintiff/Respondent,	:	
	:	CRIMINAL ACTION
	:	
v.	:	Appellate Division
	:	Docket No.: A-000291-17
	:	
Robert Andrews,	:	Sat Below:
	:	Joseph L. Yannotti, P.J.A.D.
Defendant/Appellant.	:	Garry S. Rothstadt, J.A.D.
	:	Arnold L. Natali, Jr., J.A.D.
	:	
	:	

BRIEF OF AMICUS CURIAE NEW JERSEY STATE BAR ASSOCIATION

OF COUNSEL:

Evelyn Padin, Esq.
President, New Jersey State Bar Association
New Jersey Law Center
One Constitution Square
New Brunswick, New Jersey 08901
Attorney ID No.: 001991992

ON THE BRIEF:

Christopher J. Keating, Esq.
Attorney ID No.: 120472014

Richard F. Klineburger, Esq.
Attorney ID No.: 037671995

Brandon D. Minde, Esq.
Attorney ID No.: 027972004

Matheu D. Nunn, Esq.
Attorney ID No.: 013842007

TABLE OF CONTENTS

Table of Authorities ii

Preliminary Statement 1

Procedural History and Statement of Facts 3

Legal Argument 4

POINT I: THE FOREGONE CONCLUSION EXCEPTION SHOULD
NOT BE APPLIED TO COMPEL A DEFENDANT TO PROVIDE A
PASSWORD FOR THE DECRYPTION OF AN ELECTRONIC DEVICE
FOR THE PURPOSE OF OBTAINING INFORMATION THAT COULD
BE USED AGAINST THE DEFENDANT IN A CRIMINAL
PROSECUTION..... 4

POINT II: NEW JERSEY'S PROTECTIONS AGAINST SELF-
INCRIMINATION COMPEL AN APPROACH THAT LOOKS TO THE
CONTENTS OF THE SOUGHT-AFTER EVIDENCE AND NOT JUST
THE ACT OF PRODUCTION..... 16

Conclusion 20

TABLE OF AUTHORITIES

Cases

Boyd v. United States, 116 U.S. 616 (1886) 17

Commonwealth v. Gelfgatt, 11 N.E.3d 605 (Mass. 2014) 13

Commonwealth v. Jones, 117 N.E.3d 702 (Mass. 2019) 13

Couch v. United States, 409 U.S. 322 (1973) 17

Doe v. United States, 487 U.S. 201 (1988) 4,5,6,12

Fisher v. United States, 425 U.S. 391 (1976) 4,5,6

G.A.Q.L. v. State, 257 So.3d 1058
(Fla. Dist. Ct. App. 2018) 13

In re Grand Jury Subpoena Duces Tecum
Dated March 25, 2011,
670 F.3d 1335 (11th Cir. 2012) 6,8,11,12,13,14

In re Harris, 221 U.S. 274 (1911) 6

Matter of Grand Jury Proceedings of Guarino,
104 N.J. 218 (1986) 16,17

Matter of Residence in Oakland, California,
354 F. Supp. 3d 1010 (N.D. Cal. 2019) 12

Murphy v. Waterfront Comm'n, 378 U.S. 52 (1964) 17

Schmerber v. California, 384 U.S. 7571 (1966) 4

State v. Andrews, 457 N.J. Super. 14, 197 A.3d 200
(App. Div. 2018), leave to appeal granted, 237 N.J.
572, 206 A.3d 964 (2019) 14

State v. Diamond, 905 N.W.2d 87. (Minn.),
cert. denied, 138 S. Ct. 2003 (2018) 13

State v. Hartley, 103 N.J. 252 (1986) 16

State v. Johnson, 576 S.W.3d 205 (Mo. Ct. App. 2019) 14

<u>State v. Stahl</u> , 206 So. 3d 124 (Fla. Dist. Ct. App. 2016)	13
<u>United States v. Apple MacPro Computer</u> , 851 F.3d 238, 248 n.7 (3d Cir. 2017), cert. denied sub nom. <u>Doe v. United States</u> , 138 S. Ct. 1988 (2018)	7,8,10,11,14
<u>United States v. Green</u> , 272 F.3d 748 (5th Cir. 2001) ...	8,12
<u>United States v. Greenfield</u> , 831 F.3d 106 (2d Cir. 2016)	10
<u>United States v. Hubbell</u> , 530 U.S. 27 (2000)	8,9,10,12

Constitution/Statutes/Rules

U.S. Const. amend. V	4
N.J.S.A. 2A:84A-17	16
N.J.S.A. 2A:84A-18	16,17
N.J.S.A. 2A:84A-19	16
N.J.R.E. 503	16

PRELIMINARY STATEMENT

The Fifth Amendment right against self-incrimination has long stood as the underpinning of our Constitution's bedrock principle that an individual is innocent until proven guilty. The Fifth Amendment provides individuals with a constitutional shield against being forced to assist the government in one's own prosecution. Exceptions to that right should be considered very carefully and only applied in the most limited and narrow circumstances.

The fast-paced evolution of technology presents challenging issues in connection with the analysis and application of this seemingly simple and straightforward concept. Decades of jurisprudence addressing Fifth Amendment issues never contemplated the complicated scenarios that today's individualized electronic devices present, such as the one presented here, where the Court is asked to interpret the foregone conclusion exception to the Fifth Amendment in the context of whether an individual should be compelled to produce a password to a personal electronic device to allow the government to extract potentially incriminating information.

The Court's ultimate decision will impact not just the rights of the defendant in this case, but the right of all individuals in New Jersey to refrain from disclosing decryption information about

their personal electronic devices that could lead to self-incriminating material. It is a case that will have far-reaching implications for the public, which has a keen interest in protecting the very personal information stored on electronic devices, as well as a heightened interest in ensuring law enforcement can adequately investigate and prosecute criminal cases.

Resolution of the questions raised in this matter is critical to the members of the New Jersey State Bar Association (NJSBA), the largest professional legal organization in the state, as well. Part of the organization's mission is to promote fairness in the administration of justice, which is at the heart of the constitutional arguments that must be analyzed here. NJSBA members encounter the issues present in this case on a daily basis from all viewpoints, and having clarity about how those issues should be rightfully addressed will go a long way toward assisting practitioners in providing clear guidance to their clients. In addition, the NJSBA can provide a unique outlook to the Court, as its members bring a practical perspective to the policy issues involved that can be separated from the particular facts on which this case is based.

After much research, analysis and debate, the NJSBA urges this Court to conclude that the foregone conclusion exception should not apply to PIN codes and passwords for electronic devices

that may be obtained only by compelling a defendant to produce that information. The history of the exception shows it was never contemplated that it would be used to compel defendants to produce information available only in their minds, or to provide access to electronic devices containing vast amounts of personal information that could become the basis of a criminal prosecution.

Instead, the NJSBA urges a cautious approach to the use of the foregone conclusion exception, which balances an individual's Fifth Amendment rights and the government's right to access information that it otherwise would not be entitled to in the course of an investigation. Under the circumstances in which an electronic device is merely the means to an end (i.e., access to the stored files or documents), the NJSBA believes the Court should view compelled entry of a passcode on, or decryption of, an electronic device as being part of the production of the stored electronic files, and a violation of a defendant's Fifth Amendment privilege against self-incrimination.

PROCEDURAL HISTORY AND STATEMENT OF FACTS

The NJSBA relies upon the Procedural History and Statement of the Facts as submitted by the parties.

LEGAL ARGUMENT

POINT I

THE FOREGONE CONCLUSION EXCEPTION SHOULD NOT BE APPLIED TO COMPEL A DEFENDANT TO PROVIDE A PASSWORD FOR THE DECRYPTION OF AN ELECTRONIC DEVICE FOR THE PURPOSE OF OBTAINING INFORMATION THAT COULD BE USED AGAINST THE DEFENDANT IN A CRIMINAL PROSECUTION

The Fifth Amendment to the United States Constitution provides in pertinent part that “[n]o person . . . shall be compelled in any criminal case to be a witness against himself[.]” U.S. Const. amend. V. The privilege against self-incrimination “protects a person only against being incriminated by his own compelled testimonial communications[.]” Doe v. United States, 487 U.S. 201, 207 (1988) (quoting Fisher v. United States, 425 U.S. 391, 409 (1976)), or “otherwise provide the State with evidence of a testimonial or communicative nature” Schmerber v. California, 384 U.S. 757, 761 (1966). “[I]n order to be testimonial, an accused’s communication must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a ‘witness’ against himself.” Doe, 487 U.S. at 210 (footnote omitted). It is well-settled that acts like providing a blood sample or voice exemplar, wearing an item of clothing, or being subjected to a “line-up” are not covered by the Fifth Amendment protection because they do not require a suspect to “disclose any knowledge he might have” or “speak his

guilt." Id. at 211. Notwithstanding these long-held Fifth Amendment principles, the Supreme Court's singular use of the phrase "foregone conclusion" in Fisher, 425 U.S. at 411, has created significant litigation and a diversity of decisions in both federal and state courts regarding the extent to which an exception to an individual's Fifth Amendment right can be applied where it is a "foregone conclusion" that the target or defendant is in possession of information sought by the government.

In Fisher, the Internal Revenue Service (IRS) sought to obtain taxpayer-prepared documents that the taxpayers provided to their attorneys. Fisher, 425 U.S. at 393-94. The IRS served subpoenas on each of the taxpayers requiring the taxpayers' attorneys to turn over documents, which included accountant work papers, copies of the returns, and copies of reports and correspondence. Id. at 394. The attorneys refused to produce the documents (citing the Fifth Amendment privilege against self-incrimination); the respective District Courts disagreed and compelled production of the evidence. Id. at 395. After granting certiorari, the Supreme Court held that:

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. . . . Surely the Government is in no way relying on the "truth telling" of the taxpayer to prove the existence of or his access to the documents. 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."

[Ibid. (quoting In re Harris, 221 U.S. 274, 279 (1911) (citation omitted))(emphasis added).]

The above-passage stands for the following proposition of law: "[w]here the location, existence, and authenticity of the purported evidence is known with reasonable particularity, the contents of the individual's mind are not used against him, and therefore no Fifth Amendment protection is available." In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1344 (11th Cir. 2012) ("In re Grand Jury").

Twelve years after Fisher, the Supreme Court again addressed compelled disclosure or the compelled "act of production" in Doe, 487 U.S. at 201. There, the Supreme Court held that the target of a grand jury investigation could be compelled to execute a consent directive to permit foreign banks to disclose banking records because the consent directive did not have testimonial significance. Id. at 217-19. The Court reasoned that "neither the form nor its execution communicates any factual assertions, implicit or explicit, or conveys any information to the Government" such as the existence of a specific account or "that it is controlled" by the target. Id. at 215.

The Supreme Court's use of the "foregone conclusion" exception and "act of production" doctrine have led to disparate legal holdings where electronic devices are involved. Although this exception has been addressed by the United States Supreme Court, the United States Courts of Appeals for the Second, Third, Ninth and Eleventh circuits, and various state courts, there remains ambiguity as to what constitutes a "foregone conclusion" where the subject matter is a password-protected electronic device or encrypted computer hardware. The arguments can be narrowed to the following competing approaches: (i) *"I am Jane Doe, this is my cell phone, and therefore it is a foregone conclusion that I have knowledge of the password"*; or, in the alternative, (ii) *"I am Jane Doe, this is my cell phone, it is a foregone conclusion that I have knowledge of the password and therefore I can be compelled to enter my password because the contents of the phone are a 'foregone conclusion.'"* The Third Circuit recognized the distinction in footnote 7 of its opinion in United States v. Apple MacPro Computer, 851 F.3d 238, 248 n.7 (3d Cir. 2017), cert. denied sub nom. Doe v. United States, 138 S. Ct. 1988 (2018):

It is important to note that we are not concluding that the Government's knowledge of the content of the devices is necessarily the correct focus of the "foregone conclusion" inquiry in the context of a compelled decryption order. Instead, 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. In 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." Based upon the testimony presented at the contempt proceeding, that fact is a foregone conclusion. However, because our review is limited to plain error, and no plain error was committed by the District Court in finding that the Government established that the contents of the encrypted hard drives are known to it, we need not decide here that the inquiry can be limited to the question of whether Doe's knowledge of the password itself is sufficient to support application of the foregone conclusion doctrine.

[(Emphasis added).]

While the distinction may seem minor at first, it is critical. The Fifth Amendment's protections require something more than the narrow approach to this issue: "*these are my devices and therefore it is a foregone conclusion that I know the passwords.*" Indeed, such a narrow view would allow law enforcement personnel to compel criminal defendants to turn over self-incriminating testimonial evidence -- the contents of the devices, hard drives, etc. -- with mere probable cause. This narrow view has been eschewed by the United States Supreme Court decision in United States v. Hubbell, 530 U.S. 27 (2000), as well as the Third Circuit decision, Apple MacPro Computer, 851 F.3d at 238, and Eleventh Circuit decision, In re Grand Jury, 670 F.3d at 1335. The legal reasoning underpinning the decision in United States v. Green, 272 F.3d 748 (5th Cir. 2001) further supports this notion.

In Hubbell, a grand jury issued a subpoena duces tecum requiring the target of an investigation to provide documents "reflecting, referring, or relating to any direct or indirect sources of money or other things of value received by or provided to [the target], his wife, or children." Hubbell, 530 U.S. at 46. The target invoked the Fifth Amendment privilege; the government obtained a district court order granting Hubbell § 6002 (derivative use) immunity. Id. at 31. In turn, the target complied with the subpoena and turned over the requested documents. Ibid. Following the production, the grand jury indicted the target with several federal crimes. Ibid. The target moved to dismiss the indictment and argued that the government could not convict him without the immunized documents. Id. at 31-33. Following a hearing, the United States District Court for the District of Columbia held that the government lacked an independent source for the contents of the documents (as well as the documents themselves) and dismissed the indictment. Id. at 31-32. On the government's appeal to the United States Supreme Court, the Court distinguished the compelled act in Hubbell with that in Fisher:

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.

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

It is clear from Hubbell that the focus of the foregone conclusion exception is on the extent of the government's knowledge of the requested information at the time the information is sought. See also United States v. Greenfield, 831 F.3d 106, 125 (2d Cir. 2016) (following the holding in Hubbell and rejecting the government's argument that it did not need to show that the "existence, control, and authenticity of the sought documents at the time of the issuance of the Summons" were a foregone conclusion).

In Apple MacPro Computer, a case involving child pornography, law enforcement personnel executed a search warrant and seized phones and an Apple computer with two attached external hard drives. Apple MacPro Computer, 851 F.3d at 842. The external hard drives were in an encrypted state. Ibid. The defendant voluntarily provided law enforcement with the password for his phone, but he refused to provide the passcodes needed to access the computer or the hard drives. Ibid. Although law enforcement could not access the actual computer files, a forensic analysis revealed that the computer had been used to visit sites known for "child exploitation" and that files associated with child pornography had been downloaded; the files, however, were located on the encrypted

external hard drives - a fact confirmed by the defendant's sister. Id. at 242-43. A federal judge ordered the defendant to produce the devices and hard drives in a "fully unencrypted state." Id. at 243. Thereafter, the defendant attempted several incorrect passwords for the encrypted hard drives and claimed that he could not remember the passcodes. As a result of his actions, the defendant was charged with contempt. The defendant appealed the contempt order, citing the Fifth Amendment. The Third Circuit held that although the Fifth Amendment may be implicated by compelled decryption, any "testimonial" component of the compelled decryption amounted to a "foregone conclusion" and "added little or nothing to the information already obtained by the Government." Id. at 248.

In In re Grand Jury, the government served a subpoena duces tecum on an individual that required him to appear before a grand jury and produce the unencrypted contents of hard drives located in his laptops as well as five external hard drives. In re Grand Jury, 670 F.3d at 1337. The court held that "(1) [the individual's] decryption and production of the contents of the drives would be testimonial, not merely a physical act; and (2) the explicit and implicit factual communications associated with the decryption and production are not foregone conclusions." The court noted that "[n]othing in the record before us reveals that the Government knows whether any files exist and are located on the hard drives;

what's more, nothing in the record illustrates that the Government knows with reasonable particularity that [he] is even capable of accessing the encrypted portions of the drives." In reaching its decision, the court rejected the Government's argument that "production of the unencrypted files would be nothing more than a physical nontestimonial transfer." Id. at 1346.

In a similar vein, but with different facts, in Green, 272 F.3d at 748, the court considered whether law enforcement, who violated a suspect's Miranda rights, could use the suspect's disclosure of the location of locked cases containing firearms and the suspect's act of opening the combination locks. The court held that the compelled disclosure and the compelled act of unlocking the cases were testimonial acts, in violation of Doe, 487 U.S. at 210 n.9. See Green, 272 F.3d at 753; cf. Matter of Residence in Oakland, California, 354 F. Supp. 3d 1010, 1018 (N.D. Cal. 2019) (holding that compelled use of biometric features to unlock a device is testimonial and foregone conclusion doctrine "does not apply when the government cannot show prior knowledge of the existence or the whereabouts of the documents ultimately produced in response to a subpoena") (citing Hubbell, 530 U.S. at 45.)

To be sure, a narrower approach that focuses only on compelled disclosure of a passcode (or decryption efforts) and not the location and authenticity of the underlying evidence to be seized from the device - the actual files, documents, or images - has

been adopted by other courts. For example, the Massachusetts Supreme Court held that the state must prove "beyond a reasonable doubt" that the defendant knows the password for the device for the foregone conclusion exception to apply. See Commonwealth v. Jones, 117 N.E.3d 702 (Mass. 2019); see also Commonwealth v. Gelfgatt, 11 N.E.3d 605 (Mass. 2014) (holding that compelled entry of decryption keys on seized computers did not trigger privilege against self-incrimination under the Fifth Amendment). Similarly, in State v. Diamond, 905 N.W.2d 870, 875 (Minn.), cert. denied, 138 S. Ct. 2003 (2018), the Minnesota Supreme Court held that "producing a fingerprint [to unlock a phone] is more like exhibiting the body than producing documents," and therefore it is "not a testimonial communication under the Fifth Amendment." In State v. Stahl, 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016), a Florida Court of Appeals held that when deciding "whether providing the 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." (emphasis in original). But see G.A.Q.L. v. State, 257 So.3d 1058 (Fla. Dist. Ct. App. 2018) (holding that compelled entry of passcodes on an iPhone by a minor amounted to "testimonial communications in violation of the minor's invocation of his Fifth Amendment rights"). Lastly, a Missouri Court of Appeals also

rejected the legal reasoning from In re Grand Jury Subpoena, 670 F.3d at 1335, and concluded that a defendant should be compelled to produce the passcode to his mobile phone because “[t]he focus of the foregone conclusion exception is the extent of the State’s knowledge of the existence of the facts conveyed through the compelled act of producing the passcode.” State v. Johnson, 576 S.W.3d 205, 227 (Mo. Ct. App. 2019) (citing Apple MacPro Computer, 851 F.3d at 238 and State v. Andrews, 457 N.J. Super. 14, 197 A.3d 200 (App. Div. 2018), leave to appeal granted, 237 N.J. 572, 206 A.3d 964 (2019)).

Compelling a defendant under the foregone conclusion exception to provide a password or decryption codes reaches far beyond the physical into the mind of the suspect. By virtue of the issue at stake -- compelled disclosure -- it is clear that the password is not merely being confirmed against an existing password already in the possession of the state to see if they match. Rather, when law enforcement demands a password, without more, the demand can only be seen as an effort by law enforcement to assist them with their efforts to make a stronger case against the defendant -- and most certainly not in a manner that “adds little or nothing” to the State’s case.

While other amici present credible arguments that question whether the foregone conclusion exception should apply outside of the narrow circumstances presented in Fisher, the United States

Supreme Court declined to clarify the application of the exception when it declined certiorari in Apple MacPro Computer. Accordingly, the NJSBA urges the Court to conclude that, where an electronic device is merely the means to the ends - the retrieval of the stored files or documents on the device - compelled entry of a passcode on, or decryption of, an electronic device is part-and-parcel of the production of the stored electronic files and, thus, a violation of an individual's Fifth Amendment right against self-incrimination.

POINT II

NEW JERSEY'S PROTECTIONS AGAINST SELF- INCRIMINATION COMPEL AN APPROACH THAT LOOKS TO THE CONTENTS OF THE SOUGHT-AFTER EVIDENCE AND NOT JUST THE ACT OF PRODUCTION

New Jersey's statutes and common law provide even broader self-incrimination protections than the United States Constitution. Matter of Grand Jury Proceedings of Guarino, 104 N.J. 218, 231 (1986) ("Guarino"); See also, State v. Hartley, 103 N.J. 252, 286 (1986); N.J.S.A. 2A:84A-17; N.J.S.A. 2A:84A-18; N.J.S.A. 2A:84A-19; N.J.R.E. 503. Although this Court may not have envisioned the breadth of electronic communications, electronic data storage, means of encryption, or the corollary privacy issues attendant to the explosion in the use, transmission, and storage of electronic data in its 1986 Guarino decision, the Court's wisdom at that time provided sage guidance for this case: "[i]n the case of documents, therefore, a court must look to their contents, not to the testimonial compulsion involved in the act of producing them" Guarino, 104 N.J. at 232. Stated differently, the privilege against self-incrimination requires an assessment of the evidence to be seized and the invasion of privacy on the accused, not merely the manner in which an accused is compelled to produce the evidence.

In Guarino, a case decided *after* the United States Supreme Court decisions in Fisher and Doe, this Court declined to extend

New Jersey's protection against self-incrimination to purely business records. Id. at 232-33. The Court, however, reaffirmed its adherence to Boyd v. United States, 116 U.S. 616 (1886), and provided "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.'" Guarino, 104 N.J. at 231 (quoting Murphy v. Waterfront Comm'n, 378 U.S. 52, 55 (1964)). The Court added, "[t]o determine whether the evidence sought by the government lies within that sphere of personal privacy a court must look to the 'nature of the evidence'" Id. at 231-32 (quoting Couch v. United States, 409 U.S. 322, 350 (1973) (Marshall, J., dissenting)) (emphasis added).

Guarino's reasoning provides guidance here in this Court's assessment and application of the foregone conclusion exception. That is, when considering whether to compel a suspect to enter a passcode or decrypt a hard drive, the focus should be on the evidence to be seized as well as the compelled act. Only through an approach that considers both the compelled act and the underlying evidence to be seized will this Court adhere to the legal underpinnings woven throughout Guarino and Boyd. Further support is found in the expansive definition of "incrimination" provided in N.J.S.A. 2A:84A-18:

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; 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.

[(Emphasis added)]

Under this level of scrutiny, the concept of a "foregone conclusion" demands a searching inquiry. Consider, for example, a situation where a defendant states he murdered another person and hid that person's body, has memorized the coordinates of the location of the body, and has recorded the coordinates in his password-protected mobile phone. The Fifth Amendment would clearly protect against the defendant being compelled to reveal the coordinates he has memorized. Likewise, it should also protect the defendant from providing a personal password that will, in effect, yield the same information. Thus, the NJSBA submits that where the decryption of a computer or inputting of a password may produce new evidence that potentially exposes the defendant to criminal liability, the compelled decryption or inputting of a password

violates the defendant's Fifth Amendment right to self-incrimination and should be prohibited.

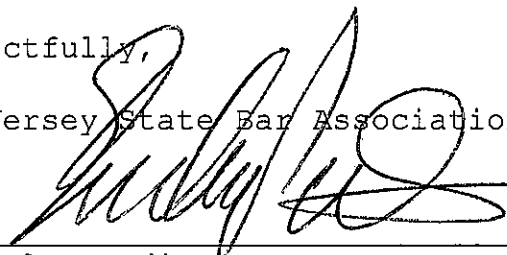
CONCLUSION

For the reasons expressed above, the NJSBA urges this Court to conclude that the foregone conclusion exception does not apply to compel disclosure of a PIN code or password to unlock an electronic device. Rather, the real focus of such compulsion should be the potentially incriminating evidence that can be accessed through such compulsion, the disclosure of which is protected by an individual's Fifth Amendment privilege against self-incrimination.

Respectfully,

New Jersey State Bar Association

By


Evelyn Padin, Esq.

President

Attorney ID Number: 001991992

Dated: 9/20/19