

STATE OF NEW JERSEY,

*Plaintiff/Respondent*

v.

ROBERT ANDREWS

*Defendant/Appellant.*

APPELLATE DIVISION  
DOCKET NO.: A-000291-17  
(AM-000643-16T4)

INDICTMENT NO. 16-06-01781-I  
CRIMINAL ACTION

SAT BELOW TRIAL COURT:  
HON. ARTHUR J. BATISTA, J.S.C.

---

**MEMORANDUM OF LAW ON BEHALF OF AMICUS CURIAE, THE ASSOCIATION OF  
CRIMINAL DEFENSE LAWYERS OF NEW JERSEY**

---

Matthew S. Adams, Esq. (00141-2008)  
Jordan B. Kaplan, Esq. (06080-2013)  
Marissa Koblitz Kingman, Esq. (11054-2014)  
Victoria Salami, Esq. (24189-2017)  
*Attorneys for the Association of  
Criminal Defense Lawyers of New Jersey*  
*madams@foxrothschild.com*  
*jkaplan@foxrothschild.com*  
*mkingman@foxrothschild.com*  
*vsalami@foxrothschild.com*

**TABLE OF CONTENTS**

	<b><u>Page</u></b>
TABLE OF AUTHORITIES.....	ii
PRELIMINARY STATEMENT.....	1
LEGAL ARGUMENT.....	4
POINT I	
THE ACT OF PRODUCTION DOCTRINE PROTECTS MR. ANDREWS FROM BEING COMPELLED TO PRODUCE THE PASSWORDS FOR HIS MOBILE PHONES.....	4
A.    The Fifth Amendment to the United States Constitution Protects Mr. Andrews from Being Compelled to Disclose His Passwords.....	4
B.    Established New Jersey Law Also Shields Mr. Andrews from Being Compelled to Disclose his Mobile Phone Passwords.....	10
POINT II	
ENHANCED SCRUTINY SHOULD BE PLACED UPON THE STATE’S EFFORTS TO CIRCUMVENT THE RIGHT AGAINST SELF-INCRIMINATION WHERE ELECTRONICALLY STORED INFORMATION IS INVOLVED.....	13
CONCLUSION.....	16

**TABLE OF AUTHORITIES**

	<b><u>Page (s)</u></b>
<b>Cases</b>	
<u>In re Addonizio,</u> 53 <u>N.J.</u> 107 (1968) .....	5, 6
<u>Curcio v. United States,</u> 354 <u>U.S.</u> 118 (1957) .....	6
<u>Doe v. United States,</u> 487 <u>U.S.</u> 201 (1988) .....	4, 7
<u>Fisher v. United States,</u> 425 <u>U.S.</u> 391 (1976) .....	4, 13
<u>In re Grand Jury Subpoena Duces Tecum Dated March 25,</u> <u>2011,</u> 670 <u>F.3d</u> 1335 (11th Cir. 2012) .....	8
<u>Hoffman v. United States,</u> 341 <u>U.S.</u> 479 (1951) .....	4
<u>In re Martin,</u> 90 <u>N.J.</u> 295 (1982) .....	10
<u>Miranda v. Arizona,</u> 348 <u>U.S.</u> 436 (1966) .....	5
<u>Riley v. California,</u> 134 <u>S. Ct.</u> 2473 (2014) .....	2
<u>SEC v. Huang,</u> 2015 WL 5611644 (E.D.Pa., Sept. 23, 2015) .....	8
<u>State v. Deatore,</u> 70 <u>N.J.</u> 100 (1976) .....	9
<u>State v. Denelsbeck,</u> 225 <u>N.J.</u> 103 (2016), <u>cert. denied</u> , 137 <u>S. Ct.</u> 1063 (2017) .....	11
<u>State v. Earls,</u> 214 <u>N.J.</u> 564 (2013) .....	11, 12

State v. Hannah,  
 448 N.J. Super. 78 (App. Div. 2016) .....14, 15, 16

State v. Hartley,  
 103 N.J. 252 (1986) .....10

State v. Hemptele,  
 120 N.J. 182 (1990) .....9

State v. Kucinski,  
 227 N.J. 603 (2017) .....10

State v. Muhammad,  
 182 N.J. 551 (2005) .....10, 11

State v. Novembrino,  
 105 N.J. 95 (1987) .....9

State v. Strong,  
 110 N.J. 583 (1988) .....11

State v. Tucker,  
 136 N.J. 158 (1994) .....9

United States v. Doe,  
 465 U.S. 605 (1984) .....5

United States v. Hubbell,  
 530 U.S. 27 (2000) .....4, 5, 13

United States v. Kirschner,  
 823 F. Supp. 2d 665 (E.D. Mich. 2010) .....7, 8

**Statutes**

N.J.S.A. 2A:84A-19 .....10

N.J.R.E. 503.....10

**Other Authorities**

David Grossman, How Do NASA’s Apollo Computers Stack  
 Up to an iPhone, POPULAR MECHANICS (Mar. 13, 2017),  
[https://www.popularmechanics.com/space/moon-  
 mars/a25655/nasa-computer-iphone-comparison/](https://www.popularmechanics.com/space/moon-mars/a25655/nasa-computer-iphone-comparison/) .....2

**PRELIMINARY STATEMENT**

The ACDL-NJ is a non-profit corporation organized under the laws of New Jersey to, among other purposes, "protect and insure by rule of law, those individual rights guaranteed by the New Jersey and United States Constitutions; to encourage cooperation among lawyers engaged in the furtherance of such objectives through educational programs and other assistance; and through such cooperation, education and assistance, to promote justice and the common good." ACDL-NJ By-Laws, Article II(a). A proper resolution of the issues raised herein is of great concern to the approximately 500 members of the ACDL-NJ who are committed to the appropriate development of New Jersey law with respect to issues that affect the fundamental rights of individuals. The ACDL-NJ's members and their clients will be directly affected by this Court's ruling on the matters before it, as will non-members including all individuals who appear before judges in New Jersey state courts in connection with criminal matters.

The rapid proliferation of technologies like mobile smartphones has forced our Courts to constantly reconsider the application of the individual rights afforded by the United States Constitution, the New Jersey Constitution, and the statutes and rules implicating the policies they stand for, to an evolving and dynamic technological landscape. Today, the average consumer has greater computing power and the ability to store more personal

information in a device that can be held in the palm of his or her hand than was available to NASA when guiding the Apollo 11 astronauts on their mission to the Moon<sup>1</sup>.

Recognizing the massive amount of personal information held in average citizens' mobile phones, the United States Supreme Court has remarked:

Modern 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.

Riley v. California, 134 S. Ct. 2473, 2494-95 (2014) (internal quotations omitted). In a society built upon individual liberties limiting the government's ability to unreasonably or unjustifiably infringe upon personal privacy or to use compulsion of law to force self-incrimination, the importance of safeguarding individual liberties is undeniable, notwithstanding the meteoric pace of technological advancement.

In this case, the State is attempting to significantly narrow the scope and application of the privilege against self-

---

<sup>1</sup> See, e.g., David Grossman, How Do NASA's Apollo Computers Stack Up to an iPhone, POPULAR MECHANICS (Mar. 13, 2017), <https://www.popularmechanics.com/space/moon-mars/a25655/nasa-computer-iphone-comparison/>

incrimination offered by the Fifth Amendment to the United States Constitution and authoritative New Jersey precedent by compelling Robert Andrews ("Andrews") to provide the passwords to his personal mobile phones so that the State may use them to collect evidence to be used against him in connection with a criminal proceeding. Compelling Andrews to provide his mobile phone passwords is no different than forcing him to provide the State with more traditional inculpatory statements or testamentary documents that may be used in a prosecution against him.

The issues presented here are likely to repeat in future cases. Citizens use their mobile telephones for a wide array of daily tasks like banking and managing healthcare, to say nothing of the fact that text messages and emails have catapulted over other forms of communication in order of preference by citizens.

Our courts must, at every opportunity, endeavor to keep up with modern technology in order to ensure that the individual rights afforded under the United States Constitution and established New Jersey law are never rendered obsolete. The framers of these cherished, liberty-defining instruments intended for them to withstand the passage of time. While the framers may never have imagined smartphones, text messages, and emails, history has demonstrated that the very instruments that shape our

democracy have withstood the test of time when confronted with new challenges and should once again do so here.

**LEGAL ARGUMENT**

**POINT I**

**THE ACT OF PRODUCTION DOCTRINE PROTECTS MR. ANDREWS FROM BEING COMPELLED TO PRODUCE THE PASSWORDS FOR HIS MOBILE PHONES**

**A. The Fifth Amendment to the United States Constitution Protects Mr. Andrews from Being Compelled to Disclose His Passwords**

The Fifth Amendment to the United States Constitution provides that "no person shall ... be compelled in any criminal case to be a witness against himself ..." U.S. CONST. amend. V; Fisher v. United States, 425 U.S. 391, 398 (1976). The privilege against self-incrimination "not only extends to answers that would in themselves support a conviction [. . .] but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant [.]" United States v. Hubbell, 530 U.S. 27, 38 (2000) (citing Hoffman v. United States, 341 U.S. 479, 486 (1951)). "Compelled testimony that communicates information that may 'lead to incriminating evidence' is privileged even if the information itself is not inculpatory." Id. (citing Doe v. United States, 487 U.S. 201, 208, n. 6 (1988)).

In Hubbell, the United States Supreme Court established the "Act of Production Doctrine," which recognizes that "the act of

producing documents . . . may have a compelled testimonial aspect...." Hubbell, 530 U.S. at 36; see also, United States v. Doe, 465 U.S. 605, 612 (1984) (holding that "[a]lthough the contents of a document may not be privileged, the act of producing the document may be" because the person is compelled "to perform an act that may have testimonial aspects and an incriminating effect."). The act of producing information is "testimonial," and therefore subject to privilege afforded by the Act of Production Doctrine when the act of production communicates some explicit or implicit statement of fact that would otherwise be considered the contents of the defendant's mind, such as that certain "papers existed, were in his possession or control, and were authentic." Id.

Through the Fourteenth Amendment to the United States Constitution, the Fifth Amendment has been applied to the states. See, e.g., Miranda v. Arizona, 348 U.S. 436 (1966). New Jersey courts have specifically applied the Act of Production Doctrine to individuals that are the subject of a grand jury investigation. In re Addonizio, 53 N.J. 107 (1968). In Addonizio, the State issued a grand jury subpoena directing Mr. Addonizio to produce his confidential financial information, including, but not limited to, bank account statements, tax returns, and lists of business entities with which he was involved. Id. at 113. Mr. Addonizio,

the then-mayor of the City of Newark, objected to the subpoena and argued that the subpoenaed records would tend to incriminate him with respect to some crime constituting corruption in public office. Id. at 14. The New Jersey Supreme Court sustained Mr. Addonizio's refusal to produce his records, finding that the Act of Production Doctrine protected Mr. Addonizio from producing his confidential financial information. The New Jersey Supreme Court held:

But it is evident that Addonizio is himself the target of the grand jury's investigation, for it is inconceivable that the records of Addonizio could reveal criminality upon the part of others without also implicating him. When a witness is thus a target of the grand jury's inquiry, no more need appear to support his Fifth Amendment claim.

In re Addonizio, 53 N.J. 107, 117 (1968).

While Addonizio addresses only the production of potentially incriminating documents themselves, courts have also held that the Act of Production Doctrine applies where the government seeks to compel a defendant to provide the location of the documents, or, perhaps more analogous to the situation in the case at bar, provide the combination to a locked safe that potentially contains incriminating information. See, e.g., Curcio v. United States, 354 U.S. 118, 128 (1957) (holding that secretary-treasurer of local union could invoke personal privilege against self-incrimination

as to questions regarding whereabouts of missing union books and records which had been subpoenaed but not produced); Doe v. United States, 487 U.S. 201, 210, n.9 (1987) ("It is the extortion of information from the accused, the attempt to force him to disclose the contents of his own mind that implicates the Self-Incrimination Clause. . . it is like 'be[ing] compelled to reveal the combination to [petitioner's] wall safe.'").

Outside of New Jersey, in United States v. Kirschner, 823 F. Supp. 2d 665 (E.D. Mich. 2010), the United States District Court for the Eastern District of Michigan, Southern Division, quashed a subpoena that required a defendant to provide the password to his computer in connection with a grand jury investigation targeting the defendant. Reasoning that compelling the defendant to provide his computer password would violate the defendant's Fifth Amendment privilege against compelled self-incrimination, the District Court wrote:

In the instant case, even if the government provides Defendant with immunity with regard to the act of producing the password to the grand jury, that does not suffice to protect Defendant's invocation of his Fifth Amendment privilege in response to questioning that would require him to reveal his password. In this case, the government is not seeking documents or objects – it is seeking testimony from the Defendant, requiring him to divulge through his mental processes his password – that will be used to incriminate him.

[. . .]

Accordingly, the Court quashes the subpoena requiring Defendant to testify—giving up his password—thereby protecting his invocation of his Fifth Amendment privilege against compelled self-incrimination.

Kirschner, 823 F. Supp. 2d at 669 (E.D. Mich. 2010).

Other courts across the Country have reached the same conclusion, quashing subpoenas that compel production of passwords to electronic devices. See, e.g., SEC v. Huang, 2015 WL 5611644 (E.D.Pa., Sept. 23, 2015) (finding that “Defendants’ confidential passcodes are personal in nature and Defendants may properly invoke the Fifth Amendment privilege to avoid production of the passcodes.”); In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012) (holding that the required production of decrypted hard drives in response to a grand jury subpoena “would be tantamount to testimony by Doe” because it “would require the use of the content of Doe’s mind and would not be fairly characterized as a physical act that would be nontestimonial in nature.”).

Compelling production of a mobile phone password here is the same as compelling production of a defendant’s personal documents or the combination to a locked safe. Such information is entitled to the full protections of the Fifth Amendment to the United States Constitution and the privilege against self-incrimination. The

evolution of technology necessitates the evolution of Constitutional principles to ensure that the purposes of the right against self-incrimination is not chilled merely by the technological advancement that is the hallmark of modern, evolved society. There is no reason why New Jersey courts should reach a different conclusion, especially because our courts have consistently held that individual rights under New Jersey state law are viewed more broadly than their federal counterparts. See, e.g., State v. Novembrino, 105 N.J. 95 (1987) (Our New Jersey Supreme Court rejected the good faith exception. The Court in Novembrino held that the exclusionary rule, unmodified by good-faith exception, is integral element of state constitutional guarantee that search warrants will not issue without probable cause.); State v. Hempele, 120 N.J. 182 (1990) (Contrary to the Supreme Court of the United States, the New Jersey Supreme Court held that a person has reasonable expectation of privacy in garbage left curbside that is protected by State Constitution); State v. Tucker, 136 N.J. 158 (1994) (The New Jersey Supreme Court, unlike the Supreme Court of the United States, held that running from police did not justify seizure, and contraband thrown by defendant after unreasonable seizure was not abandoned and should have been suppressed); State v. Deatore, 70 N.J. 100 (1976) (Noting conflicting federal law, the New Jersey Supreme Court held that it

was error to permit one defendant, who asserted alibi defense at trial, to be cross-examined concerning his failure to have informed the police of his alibi at the time of his arrest.); State v. Muhammad, 182 N.J. 551 (2005) (Holding Our state-law privilege against self-incrimination offers broader protection than its federal counterpart under the Fifth Amendment).

**B. Established New Jersey Law Also Shields Mr. Andrews from Being Compelled to Disclose his Mobile Phone Passwords**

Although the New Jersey Constitution does not contain an express provision that protects its citizens from forced self-incrimination in the same way that its federal counterpart does, the privilege itself "is firmly established as part of the common law of New Jersey and has been incorporated into our Rules of Evidence." State v. Hartley, 103 N.J. 252, 260 (1986) (citing In re Martin, 90 N.J. 295, 331 (1982)). While absent from the express language our state's constitution, the Legislature codified the right to remain silent in N.J.S.A. 2A:84A-19 and N.J.R.E. 503. Moreover, consistent with the broader protections afforded to individual rights under New Jersey law as opposed to Federal law, the New Jersey Supreme Court has held that the "state-law privilege against self-incrimination offers broader protection than its federal counterpart under the Fifth Amendment." State v. Kucinski,

227 N.J. 603, 617 (2017); State v. Muhammad, 182 N.J. 551, 568 (2005).

In State v. Strong, 110 N.J. 583 (1988), the New Jersey Supreme Court analyzed the scope of the right against self-incrimination and held that:

[T]he protection against self-incrimination at issue here is heightened because we are dealing with judicially compelled testimony. . . the [F]ifth [A]mendment mandates the strictest scrutiny of and the strongest protections against possible prosecutorial misuse of testimony with respect to a witness. . . **We add that our state-law privilege against self-incrimination is, if anything, more protective than the fifth amendment.** . . We therefore conclude that this result, entailing both the strictest scrutiny of and the greatest protections against prosecutorial use of compelled testimony, is required under our state-law privilege against self-incrimination.

Id. at 594-95 (emphasis added).

With respect to the privacy rights of mobile phone users, New Jersey courts have also held that New Jersey law provides even greater privacy protections to citizens than does the Federal Constitution. See, e.g., State v. Denelsbeck, 225 N.J. 103, 136 (2016), cert. denied, 137 S. Ct. 1063 (2017) (citing State v. Earls, 214 N.J. 564, 568-69 (2013)). For example, in Earls, supra., the New Jersey Supreme Court stated:

Advances in technology offer great benefits to society in many areas. At the same time, they

can pose significant risks to individual privacy rights. . . Historically, the State Constitution has offered greater protection to New Jersey residents than the Fourth Amendment. **Under settled New Jersey law, individuals do not lose their right to privacy simply because they have to give information to a third-party provider, like a phone company or bank, to get service.** . . . We therefore find that individuals have a reasonable expectation of privacy in the location of their cell phones under the State Constitution.

State v. Earls, 214 N.J. 564, 568-69(2013) (emphasis added).

When evaluating the scope and application of the right against self-incrimination, the New Jersey Supreme Court has made clear that the "question before the Court, then, [should be] informed by changes in technology[.]" Id. at 587. Recognizing the need to address self-incrimination issues against the modern backdrop of how individuals live and work in modern, technologically driven times, the New Jersey Supreme Court noted that "law and practice have evolved in this area in response to changes in technology." Id. at 588.

New Jersey law should continue to evolve in order to keep pace with technology. If it does not, the ramifications to individual rights will be devastating. It is conceivable that the failure of the privilege against self-incrimination to evolve at the pace of modern technology might result in the destruction of the privilege altogether. Accordingly, this Court must prevent the

advancement of technology from undermining New Jersey's broad policy against compulsory self-incrimination.

**POINT II**

**ENHANCED SCRUTINY SHOULD BE PLACED UPON THE STATE'S EFFORTS TO CIRCUMVENT THE RIGHT AGAINST SELF-INCRIMINATION WHERE ELECTRONICALLY STORED INFORMATION IS INVOLVED**

The so-called Foregone Conclusion Doctrine does not appear to have been conclusively adopted by New Jersey Courts as an exception to the privilege against self-incrimination. Interpreting the Fifth Amendment to the United States Constitution, federal courts, however, have developed and adopted the Foregone Conclusion Doctrine as a potential exception to the otherwise broad prohibition against compulsory self-incrimination that is widely recognized under state and federal law.

In Fisher, the United States Supreme Court held that the Foregone Conclusion Doctrine applies only where the state establishes, with reasonable particularity, that, *inter alia*, the materials sought are authentic. Fisher, supra. at 410-13. See also, Hubbell, 530 U.S. at 40-41. In other words, the authenticity of the sought-after materials must rise to the level of being the very "foregone conclusion" for the Foregone Conclusion Doctrine to apply.

When it comes to electronically stored information ("ESI") such as the contents of a mobile phone, authenticity of ESI should

be analyzed with an enhanced level of scrutiny due to the ease with which ESI can be manipulated, altered, and destroyed. With the touch of a button, ESI can be modified to create a false reality, making the burden of authentication of original ESI difficult or impossible. In a criminal case, where the State carries the highest evidentiary burden known to the law -- beyond a reasonable doubt -- that risk is striking.

New Jersey courts have yet to analyze fully the intricacies involved in authenticating complex ESI. Instead, our courts have reviewed more simplistic forms of ESI, such as social media postings that can be interpreted by most lay witnesses. For example, in State v. Hannah, 448 N.J. Super. 78 (App. Div. 2016), the Appellate Division analyzed the contents of a "tweet" posted on the social media site Twitter and reasoned that "[t]he simple fact that a tweet is created on the internet does not set it apart from other writings. Accordingly, we apply our traditional rules of authentication under N.J.R.E. 901." Id. at 79. The Appellate Division panel went on to describe the indicia of authenticity that it believed surrounded the tweet, on its face, supporting its authenticity.

While Hannah provides authoritative guidance with respect to the authentication of social media evidence (only), the Appellate Division's decision in Hannah specifically does not address more

sophisticated forms of digital evidence, such as the unbounded and limitless contents of a mobile phone. The Appellate Division may have addressed lingering arguments pertaining to one form of digital evidence in Hannah, but the decision should not serve a one-size-fits-all, cookie cutter framework that should apply to each and every type of digital evidence that might be encountered in connection with a criminal case.

Relative to complex ESI, such as the unbounded and limitless contents of a mobile phone, a social media post is low on the sophistication scale. The content of a social media post stands for itself, and with a proper foundation, is largely self-authenticated like the pages of a book or an article in a magazine or a newspaper. While there are unique technical components of a social media post that could be used to lend to a conclusion as to its authenticity based upon the medium used for its publication, those unique electronic components do not play the same role as they do, for example, in connection with a text message, email or a video or audio recording. In those latter examples of far more sophisticated digital evidence, metadata, by way of example, classifiable according to most computer scientists as either descriptive, structural or administrative, unlocks the truth behind what appears on the surface of the evidence.

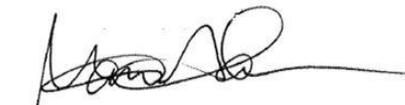
In cases involving complex ESI, such as the unbounded and limitless contents of mobile phones at issue here, caution must be exercised in extending Hannah beyond its basic context-- a screenshot of a straightforward social media post. The Court should, therefore, adopt an enhanced level of scrutiny when analyzing the authenticity of the contents of more complex ESI, and apply the Foregone Conclusion Doctrine or other so-called exceptions to the privileged against self-incrimination to complex ESI like that which is at issue in the case at bar in only the rarest of circumstances.

**CONCLUSION**

For the foregoing reasons, *Amicus Curiae*, the ACDL-NJ respectfully requests that this Court grant Mr. Andrews' motion in its entirety.

Respectfully submitted,

**FOX ROTHSCHILD LLP**



---

Matthew S. Adams  
Jordan B. Kaplan  
Marissa Koblitz Kingman  
Victoria Salami

Dated: March 14, 2018