

SCIARRA & CATRAMBONE, LLC  
Charles J. Sciarra, Esq.  
Attorney Id. No.:(011371996)  
csciarra@sciarralaw.com  
Deborah Masker Edwards, Esq.  
Attorney Id. No.:(047181991)  
dedwards@sciarralaw.com  
1130 Clifton Ave.  
Clifton, New Jersey 07013  
(973) 242-2442 (Telephone)  
(973) 242-3118 (Facsimile)  
*Attorney for Defendant*  
*Robert Andrews*

---

State of New Jersey,	:	SUPREME COURT OF NEW JERSEY
	:	DOCKET NO.: 082209
	:	APPELLATE DIVISION DOCKET NO.:
	:	DOCKET NO.:A-000291-17
	:	MOTION NO.: M-007484-16
	:	JUDGES YANNOTTI, ROTHSTADT,
Plaintiff,	:	AND NATALI
	:	
	:	INDICTMENT NO.: 16-06-01781-I
	:	
v.	:	CRIMINAL ACTION
	:	
	:	
Robert Andrews,	:	Sat Below.
	:	Hon. Arthur J. Batista, J.S.C.
Defendant.	:	
	:	

---

DEFENDANT'S BRIEF IN SUPPORT OF  
HIS INTERLOCUTORY APPEAL OF THE APPELLATE DIVISION'S DECISION  
COMPELLING DEFENDANT TO DISCLOSE HIS CELL PHONE PASSWORDS IN  
VIOLATION OF HIS RIGHT AGAINST SELF-INCRIMINATION

---

Of Counsel:  
Charles J. Sciarra, Esq.

On the Brief:  
Deborah Masker Edwards, Esq.

TABLE OF CONTENTS

Table of Judgements . . . . .	ii
Table of Authorities . . . . .	iii
Preliminary Statement . . . . .	1
Procedural History . . . . .	2
Statement of Facts . . . . .	7
POINT I	
Andrews' Leave to Appeal the Interlocutory Order of the Appellate Division, affirming the violation of Andrews' right to not incriminate himself by compelling him to disclose his cell phone passwords, has been granted (Da1-Da24, Da125 . . . . .	10
POINT II	
Andrews' appeal should be granted reversing the Appellate Division's decision, affirming the Trial Court's decision, as Andrews cannot be compelled to disclose his cell phones' passwords as he is protected by the Fifth Amendment to the United States Constitution, New Jersey Common Law, <u>N.J.S.A. 2a:84a-19</u> and <u>N.J.R.E. 503</u> (Da1-Da24) . . . . .	11
A. The Fifth Amendment to the United States Constitution protects Andrews from being compelled to disclose his cell phone' passwords (Da1-Da20) . . . . .	11
B. New Jersey Common Law, Statutory Law, and the Rules of Evidence give Andrews the right to a privilege against self-incrimination from being compelled to disclose cell phone passwords. (Da20-Da24) . . . . .	17
POINT III	
Andrews' right to remain silent has been violated and the forgone conclusion exception was mischaracterized. (Da1-Da20) . . . . .	30

POINT IV

The Appellate Division misapplied the law and the facts in arriving at its decision and relied on out of State case law that are outliers contrary to Hubbell, New Jersey Common Law, Statutory Law, and the Rules of Evidence (Da1-Da20) . . . . . 40

Conclusion . . . . . 53

**TABLE OF JUDGEMENT**

Order and Opinion of the Appellate Division, Judges Yannotti, Rothstadt, and Natali, dated November 15, 2018 . . . . . Da1

Affirming:

Order of the Honorable Arthur J. Batista, J.S.C. Dated May 22, 2017 . . . . . Da32

Opinion of the Honorable Arthur J. Batista, J.S.C. Dated May 22, 2017. . . . . Da33

## TABLE OF AUTHORITIES

### **CASES**

<u>Boyd v. United States</u> , 116 U.S. 616 (1886) .....	19, 20, 21
<u>Carpenter v. United States</u> , ___ U.S. _____, 138 S.Ct. 2206, 2271 (2018) (Gorsuch, J. dissenting) .....	27, 49
<u>Commonwealth of Virginia v. David Charles Baust</u> , 89 Va Cir. 267 (October 28, 2014) .....	43, 50
<u>Commonwealth v. Davis</u> , 176 A.3d 869 (Pa. Super Ct. 2017) .....	37
<u>Commonwealth v. Gelfgatt</u> , 11 N.E.3d 605 (Mass. 2014) .....	34
<u>Commonwealth v. Jones</u> , 481 Mass. 540, 555-558 (2019) .....	35, 36
<u>Commonwealth v. Jones</u> , 481 Mass. 540, 563-564 fn1 (2019) (concurrence Lenk, J) .....	27, 28, 35, 36
<u>Couch v. United States</u> , 409 U.S. 322, 328 (1973) .....	12, 19
<u>Curcio v. United States</u> , 354 U.S. 118, 128 (1957) .....	16
<u>Doe v. United States</u> , 487 U.S. 201 (1988) 11, 12, 13, 14, 15, 16, 19, 31, 41	
<u>Fisher v United States</u> , 425 U.S. 391, 398 (1976) .	12, 13, 17, 19, 30, 31, 42
<u>G.A.Q.L. v. State of Florida</u> , 257 So.3d 1058 (October 24, 2018) .....	36, 46, 50, 51
<u>Her majesty the Queen and Suhail Shergill</u> , 2019 ONCJ 54 (Jan. 24, 2019) .....	26
<u>In re Addonizio</u> , 53 N.J. 107, 129 (1968) .....	18, 28
<u>In re Application for a Search Warrant</u> , 236 F. Supp. 3d 1066 (Feb. 16, 2017) .....	47, 48
<u>In re Boucher</u> , 2009 WL 424718(D.Vt. Feb. 19, 2009) .....	42
<u>In re Grand Jury Subpoena Duces Tecum dated March 25, 2011</u> , 670 F.3d 1335. 1345 (2012) .....	16, 31, 34, 41, 42, 43, 50, 51
<u>In re Martin</u> , 90 N.J. 295, 331 (1982) .....	18
<u>In re of the Search of a Residence in Oakland, California</u> , 354 F. Supp. 3d 1010, 1015-1016 (9 <sup>th</sup> Cir. 2019) .....	28, 48, 49
<u>In the Matter of Grand Jury Proceedings of Joseph Guarino</u> , 104 N.J. 218 (1986) .....	5, 19
<u>Klump v. Nazareth Area School District</u> , 425 F. Supp. 2d 622 (E.D. Pa 2006) .....	24
<u>Malloy v. Hogan</u> , 378 U.S. 1 (1964) .....	12
<u>Michigan v. Mosley</u> , 423 U.S. 96, 103-104 (1975) .....	12
<u>Miranda v. Arizona</u> , 384 U.S. 436 (1966) .....	12
<u>New Jersey v. T.L.O.</u> , 469 U.S. 325 (1985) .....	24
<u>People v. Spicer</u> , ___ N.E.3d ___ (2019) 2019 WL 1075261 (IL App. (3d) March 7, 2019) .....	46, 47, 50, 51
<u>Riley v. California</u> , 573 U.S. 373, 375(2014) .....	20, 21, 22
<u>Securities and Exchange Commission v. Bonan Huang, et al.</u> , Case 2:15-cv-00269 (September 23, 2015) .....	43, 50

<u>Seo v. State of Indiana</u> , 109 N.E.3d 418 (Ind. Ct. App.), transfer granted, opinion vacated, 119 N.E.ed 90 (Ind. 2018) .....	45
<u>State of Maine v. Trant</u> , 2015 WL 7575496 (Oct. 27, 2015) (Da166-Da169) .....	44
<u>State of Missouri v. Johnson</u> , ___ S.W.3d ___ (2019) 2019 WL 1028462 (Mo. App. W.D. March 5, 2019) .....	27
<u>State of New Jersey v. Jay C. Fisher</u> , 395 N.J. Super. 533, 541 (2007) .....	12, 18
<u>State of New Jersey v. Kelsey</u> , 429 N.J. Super. 449 (App. Div. 2013) .....	18
<u>State of New Jersey v. Kucinski</u> , 227 N.J. 603, 617 (2017) .	12, 18
<u>State v. Brown</u> , 190 N.J. 144, 157 (2007) .....	29
<u>State v. Hartley</u> , 103 N.J. 252 260 (1986) .....	18
<u>State v. Marrero</u> , 148 N.J. 469,480-481 (1997) .....	10
<u>State v. Muhammad</u> , 182 N.J. 551, 568 (2005) .....	18
<u>State v. Powell</u> , 294 N.J. Super. 557 (App. Div. 1996) .....	27
<u>State v. Stahl</u> , 206 So. Ed 124 (Fla Dist. Ct. App. 2016) 5, 33, 36	
<u>United States of America v. Spencer</u> , 2018 WL 1964588 (N.D. Cal. April 26, 2018) .....	34
<u>United States v. Apple MacPro Computer</u> , 851 F.3d 238 (3d Cir. 2017) .....	32, 33, 34
<u>United States v. Doe</u> , 465 U.S. 605, 613 and n.11 (1984) .....	14
<u>United States v. Hubbell</u> , 530 U.S. 27, 37 (2000) .	12, 15, 16, 17, 41, 42, 43, 50
<u>United States v. Kirschner</u> , 823 F. Supp.2d 665 (E.D. Michigan, Southern Division 2010) .....	40, 43, 50
<u>United States v. Mitchell</u> , 76 M.J. 413, 418 (2017) .....	44
<u>United States v. Sanchez</u> , 334 F. Supp. 3d 1284 (2018) .....	45

## STATUTES

ENCRYPT Act of 2018, H.R. 6044, 115 <sup>th</sup> Cong., § 2 (June 7, 2018)	22
Hawaii Legislature, A Bill for an Act relating to the Uniform Employee and Student Online Privacy and Protection Act, H.R. Thirtieth Legislature, H.B. No. 6, February 4, 2019 .....	24
<u>N.J.S.A. 18A:3-30</u> .....	23
<u>N.J.S.A. 2A:84A-19</u> .....	11, 18, 26
<u>N.J.S.A. 2A:84A-19 (b)</u> .....	7
<u>N.J.S.A. 34:6B-6</u> .....	23
New York Legislature, Senate, 2019-2020, Act to Amend Labor Law in relation to the Uniform Employee and Student Online Privacy Protection Act, S2728, Add Art. 33 §§950-955 Lab. L, January 29, 2019 .....	25
Secure Date Act of 2018, H.R. 5823, 115 <sup>th</sup> Cong., § 2 (May 15, 2018) .....	22

**OTHER AUTHORITIES**

Jon Schuppe, Give up your password or go to jail; Police push legal boundaries to get into cell phones, nbcnews.com, June 7, 2019, <https://www.nbcnews.com/news/us-news/give-your-password-or-go-jail-police-push-legal-boundaries-n1014266> ..... 33

National Conference of State Legislatures, LegisBrief, Social Media Privacy Laws, Vol. 22, No 16, April 2014 ..... 23, 24

National Conference of State Legislatures, State Social Media Privacy Laws, May 22, 2019 ..... 23

Netherlands Legislation, Criminal Procedure Code, Section 126nd, October 8, 2012 ..... 26

United Nations Office on Drugs and Crime, Sharing Electronic Resources and Laws on Crime, Finland Legislation, Section 23 of Chapter 8 of the Law on Coercive Measures Act, July 22, 2011 25

**RULES**

N.J.R.E. 502 . . . . . 26

N.J.R.E. 503 ..... 7, 11, 18, 26

R. 2:2-2(a) ..... 10

**CONSTITUTIONAL PROVISIONS**

Fifth Amendment to the United States Constitution ..... 11

**PRELIMINARY STATEMENT**

The Appellate Division has established a first of its kind standard that eviscerates all criminal defendants' rights to not incriminate themselves and ignores the long standing precedent that New Jersey state law privileges offer broader protections than the Federal counterpart under the Fifth Amendment.

The Appellate Division has ruled that compelling a defendant to use his mind to disclose his cell phone passwords was not a testimonial communication worthy of protection. Moreover, the Appellate Division's analysis adulterated the forgone conclusion exception to the Fifth Amendment. The issue presented in this appeal is whether the New Jersey common law, statutory rights, Rules of Evidence, and the United States Constitution's Fifth Amendment protects Robert Andrews ("Andrews" or "Defendant") from being compelled to disclose his cell phone's passwords.

Andrews will be irreparably harmed if compelled to disclose the cell phone passwords in violation of his right not to incriminate himself. This case is of general public importance and a case of first impression with the intersection of advanced technology, expansive private material, and the right not to be compelled to incriminate one's self. The interests of justice require that the Appellate Division's decision be reversed and

Andrew's rights not to incriminate himself be preserved.

### PROCEDURAL HISTORY

Two years after Andrew's arrest, and close to a year after Andrews was indicted for Official Misconduct, Hindering Apprehension or Prosecution, and Obstruction of the Administration of Law, the State filed a motion to compel Andrews to disclose two cell phone passwords. (Da5, Da47).

During the oral argument of the State's Motion to Compel Andrews to disclose two cell phones' passwords the State argued this was a case of first impression, but it was distinguished from other cell phone cases as there was a "handful" of text messages that supported its motion denying Andrews of his right to remain silent. (1T4:18-5:15)<sup>1</sup>. Although the State argued that Andrews was very safe in his cell phone dealings with their main witness, Quincy Lowery ("Lowery"), the State simultaneously argued that Andrews accepted text messages from Lowery that were incriminating. (1T6:6-11). As pointed out by Defendant's counsel at oral argument, the State wanted the Court to believe that Andrews was smart enough to not communicate via text, but not smart enough to say do not text me. (1T34:21-35:7). The State argued that Andrews never responded to any incriminating license plate numbers sent to him or undercover

---

<sup>1</sup> Motion Hearing Transcript dated April 21, 2017 is hereinafter referenced as "1T".



pictures, but then referenced a text message taken out of context and identified by Lowery as pertaining to a job opportunity with a bus company. (1T6:6-13).

The State's argument supporting its application was that Andrews and Lowery appear to have engaged in numerous telephone exchanges over a one month period.<sup>2</sup> However, the State conceded that the Court had to make an "inference" as to what those calls meant. (1T7:11-20). There is no recording of the calls between the two men, just the mere fact that they called each other sometimes a few times a day. (1T36:2-37:2).

The Trial Court asked the State to identify the "text messages" that were being utilized to demonstrate the State's reasonable particularity as to what was on the cell phones. The State referenced that Lowery identified a license plate number in a text to Andrews. (1T11:1-8). The State then failed to produce any other evidence that demonstrated that Andrews received this message and acted on it, stating to the Court it should just rely on "their inferences". (1T11:9-12:1). The State then tried to lead the Court to believe that Lowery took a picture of an undercover detective and sent it to Andrews. After the Court made multiple inquires, the

---

<sup>2</sup> It is significant to note that although the State relied on the alleged phone calls made between Andrews and Lowery to support its application, there was no recording of any of the alleged calls made although there was an alleged wiretap of Lowery's phone.

State finally conceded that there was not a text message between Andrews and Lowery regarding any undercover detective nor was a picture sent. The State again referenced a text about a meeting that its own witness reported was regarding a job opportunity at a bus company. (1T12:12-13:5). With regard to the call logs, the State conceded that the calls designated on Lowery's phone that were over a minute had a specified amount of time the call lasted, anything under a minute could have been a disconnect or a small amount of conversation. (1T:16:18-24). The State further conceded that the passwords required to be provided by Andrews could lead to a "certain inference" as to what the PIN meant. (1T22:9-15).

When the State discussed with the Court the phones that it wanted the passwords of, the State conceded that it had not provided the Court identification as to what phones had what communications on them, as one phone was predominately used. (1T19:10-25; 1T29:12-17). There was no evidence presented at the hearing as to which phones belonged to Andrews and how he was ordered in the confines of his employment to turn over the phones on his person. (T42:1-43:7). When the Court asked as to the scope of its request, the State responded that it wanted "everything" on the phone. (1T25:18-24). Defense counsel pointed out to the Court at oral argument that the State's star witness, Lowery, stated that "none of that shit was on the phone." (1T34:6-20).

On May 22, 2017, the Trial Court ordered Andrews to provide a

testimonial communication against his privilege not to incriminate himself. Andrews' compelled disclosure of his passwords will give the State access to Andrews' iPhones pertaining to the "phone" and "text message" icon applications. (Da32-Da51). The Trial Court erroneously found this compulsion was not testimonial. (Da48). The Trial Court opined that it was a "foregone conclusion" that the State knew what evidence existed, the evidence was in the possession of the accused, and the evidence was authentic. (Da48-Da50).

Although the Trial Court stated that it reconciled the Supreme Court's ruling in In the Matter of Grand Jury Proceedings of Joseph Guarino, 104 N.J. 218 (1986) by the foregone conclusion exception, its conclusions of law and findings of facts were directly contrary to case law and the evidence presented at the hearing relying on out-of-state jurisdictions, specifically State v. Stahl, 206 So. Ed 124 (Fla Dist. Ct. App. 2016). (Da37-Da45, Da48, Da49).

On June 8, 2017, Andrews filed a Motion for Leave to File an Interlocutory Appeal. (Da30-Da31). On July 10, 2017, the Honorable Joseph L. Yannotti, P.J.A.D. of the Appellate Court denied Andrews' Motion for Leave to Appeal. (Da29). On July 20, 2017, Defendant appealed the Appellate Division's Order to the Supreme Court. (Da26-Da27). On September 11, 2017, the Supreme Court granted Defendant's Motion for Leave to Appeal and remanded the matter to the Appellate Division for consideration on the merits. (Da25).

On November 15, 2018, the Appellate Division, in an opinion

authored by Judge Yannotti, who initially denied Defendant's leave to appeal, affirmed the Trial Court's Order.<sup>3</sup>(Da1-Da24). Respectfully, the Appellate Division's decision vacillates as to whether or not the compulsion of the passwords is testimonial. (Da7-Da9). The Court conceded there is a "testimonial aspect" to the compulsion, but created a safe harbor by crafting a simplified version of the "forgone conclusion" exception.(Da10-Da20). The Appellate Division ultimately ruled that the compelled disclosure was not a testimonial communication, thus affirming the Trial Court's ruling. (Da24, Da48-Da51).

In error, the Appellate Division simplified the application of the forgone conclusion exception against precedent. (Da10-Da20). The Appellate Division did not perform a substantive analysis of the "reasonable particularity" standard of the foregone conclusion exception. Rather, using a simplistic mechanical approach, it found the State established that Defendant knew the passcodes and that the State had described with "reasonable particularity" what it was seeking which was "simply the passwords." (Da10).

The Appellate Division went further by rejecting the precedent of the broader protections provided by state statutory and common law, compared with its Federal counterpart, relative to the right

---

<sup>3</sup>The Appellate Division permitted the Association of Criminal Defense Lawyers of New Jersey to appear *amicus curiae* yet denied its participation at oral argument and then improperly dismissed its arguments out-of-hand in its opinion. (Da19).

not to incriminate one's self. (Da20-Da22). The Appellate Division concluded that N.J.S.A. 2A:84A-19 (b) and N.J.R.E. 503(b) were not violated since the State already knew the important facts, i.e. there was a password, and a search warrant had been issued. The Appellate Division erroneously ruled that the State had a "superior right of possession" simply because it issued a search warrant, trumping Defendant's rights. (Da22-Da24).

On January 3, 2019, Andrews filed a Motion for Leave to Appeal the Appellate Division's decision to the Supreme Court. On May 3, 2019, the Supreme Court granted Defendant's Motion for Leave to Appeal. (Da125). Defendant files the herein supplemental brief in support of his appeal.

#### STATEMENT OF FACTS

The Grand Jury proceedings in this case were on April 28, 2016 and May 26, 2016. The State presented a Detective from the Essex County Prosecutor's Office and defendant Quincy Lowery.<sup>4</sup> On June 30, 2015 and July 2, 2015, Lowery provided statements to the Essex County Prosecutor's Office. These statements were taken after his arrest and while in custody. (Da52-Da91a, Da93-103; 2T14:2-12).

The Trial Court adopted the State's position that Lowery's cell

---

<sup>4</sup> Grand Jury Transcript dated April 28, 2016 is hereinafter referenced as "2T".

Grand Jury Transcript dated May 26, 2016 is hereinafter referenced as "3T".

phone contained an "abundance" of information corroborating his statements, the only information evidenced is that of Lowery's own conduct that had no link to Andrews. (Da49). The Appellate Decision suggests that there were a series of text messages with Defendant, without further elucidation. The Appellate Division failed to identify any items on Lowery's cell phone that corroborated his statement. (Da3).

The Appellate Division is silent as to the two texts, respectively the June 20, 2015 and June 22, 2015 text, which the State relied upon in its oral argument as demonstrating its "particularity of knowledge" as to what was on the phone. On June 20, 2015, Lowery sent an unsolicited text to Andrews with the number H25-EKK of a car he thought was following him. (Da106, 1T6:6-13). There was no response from Andrews via text, no evidence that Andrews ran the plate, or that anyone associated with him ran the plate. This was contrary to Lowery's statement that Andrews ran the plate on June 20, 2015. (Da88 72:22-73:13; Da7322:8-25; Da107-Da110; Da112; Da116-Da117, 1T11:1-12:1). Further, contrary to the Appellate Division's finding, there was no "picture" in evidence of a license plate. (Da4).

Lowery reported that the text on June 22, 2015 where Andrews texted him and stated in part "Bro call me we need to talk face to face when I get off work" was not about the license plate, but about a business/job related to a bus company. The Trial Court

relied on the State's assertion at oral argument that the June 22, 2017 text was directly related to the license plate contradicting Lowery. (1T6:6-13, 1T11:1-12:1, 1T:12:12-13:5, 2T10:1-25).

There was no evidence that Andrews electronically communicated with Lowery regarding the disposal of cell phones or that Andrews was the source of the information. (Da108). Lowery could not provide any date when he discussed this with Andrews and reported that he did his own surveillance and then discarded his phone. (2T18:16-23, 3T9:5-19, Da66 29:11-18, Da68 32:19-33:2, Da77 50:18-58:17).

Lowery specifically stated in his July 2, 2015 interview, with regard to communicating with Andrews regarding the alleged illegal activity related to undercover transactions or wiretapping, "none of that shit was on the phone." (Da99). As conceded by the State at oral argument, other than the mere fact the two men called each other there is no evidence of any connection to the alleged events confirming Lowery's statements, nor was there any wiretap evidence. (1T7:11-20, 1T11:9-12:1, 1T16:18-24, 1T36:2-37:2).

At oral argument, the State acknowledged that it did not know what was on the phones, did not know what phones had what on it, and asked the Court to make inferences as to what should be on the phones. (1T19:10-25, 1T25:18-24, 1T29:12-17).

POINT I

ANDREWS' LEAVE TO APPEAL THE INTERLOCUTORY ORDER OF THE APPELLATE DIVISION, AFFIRMING THE VIOLATION OF ANDREWS' RIGHT TO NOT INCRIMINATE HIMSELF BY COMPELLING HIM TO DISCLOSE HIS CELL PHONE PASSWORDS, HAS BEEN GRANTED. (D1-Da24, Da125)

Pursuant to R. 2:2-2(a) leave to appeal from the Appellate Division may be taken when it is necessary to prevent irreparable harm or if a broad public policy issue is presented. State v. Marrero, 148 N.J. 469,480-481 (1997). Andrews has demonstrated he will suffer irreparable harm if the Court permits a violation of his rights under the Fifth Amendment to the United States Constitution, State statutory and common law, and evidentiary rules by compelling disclosure of the cell phones' passwords.

This appeal raises issues of significant public interest and policy as a dangerous precedent has been established by the Appellate Division decision which has decimated not only Andrews' rights, but the rights of every other criminal defendant in the State of New Jersey. The Court should reverse the decision of the Appellate Division, which affirmed the Trial Court's ruling, as it misconstrued the facts and failed to accurately apply the law.



POINT II

ANDREWS' APPEAL SHOULD BE GRANTED REVERSING THE APPELLATE DIVISION'S DECISION, AFFIRMING THE TRIAL COURT'S DECISION, AS ANDREWS CANNOT BE COMPELLED TO DISCLOSE HIS CELL PHONES' PASSWORDS AS HE IS PROTECTED BY THE FIFTH AMENDMENT TO THE UNITED STATE CONSTITUTION, NEW JERSEY COMMON LAW, N.J.S.A. 2a:84a-19 AND N.J.R.E. 503. (Da1-Da24)

A. The Fifth Amendment to the United States Constitution protects Andrews from being compelled to disclose the cell phones' passwords. (Da1-Da20)

Contrary to the Appellate Division's opinion, the compelled disclosure of Andrews' passwords to the cell phones is prohibited by the Fifth Amendment to the United States Constitution, New Jersey Common Law, N.J.S.A. 2A:84A-19, and N.J.R.E. 503. Although the Courts in New Jersey have not specifically addressed the compelled disclosure of cell phone passcodes, there is a long line of case law that supports Andrews' right not to be compelled to disclose his cell phones' passwords. The advent of advanced technology should not be an excuse to erode the principles of the Fifth Amendment and the protections afforded by the New Jersey Common Law, statutory authority, and rules of evidence.

The Appellate Division erroneously found that compelling a person to disclose their passwords to their cell phones is not testimonial. The Appellate Division failed to appropriately apply federal case law, ignoring the established precedent set forth in Doe v. United States, 487 U.S. 201 (1988) and essentially ignoring United States v. Hubbell, 530 U.S. 27, 37 (2000).

The Fifth Amendment to the United States Constitution

guarantees that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself. U.S. Const. amend V. "The federal protection against compelled self-incrimination must be 'scrupulously honored.'" State of New Jersey v. Kucinski, 227 N.J. 603, 617 (2017) *citing* Michigan v. Mosley, 423 U.S. 96, 103-104 (1975) *quoting* Miranda v. Arizona, 384 U.S. 436 (1966). The protections of the Fifth Amendment to the United States Constitution is extended to the States through the Due Process Clause of the Fourteenth Amendment. State of New Jersey v. Jay C. Fisher, 395 N.J. Super. 533, 541 (2007); Malloy v. Hogan, 378 U.S. 1 (1964).

As stated by the United States Supreme Court, "[i]t is extortion of information from the accused himself that offends our sense of justice." Fisher v United States, 425 U.S. 391, 398 (1976) *quoting* Couch v. United States, 409 U.S. 322, 328 (1973). The Fifth Amendment protects compelled statements that lead to discovery of incriminating evidence even though the statements themselves are not incriminating. United States v. Hubbell, 530 U.S. 27, 37 (2000).

Under both Doe and Hubbell, whether or not the act is testimonial depends on whether the target was being compelled to use the knowledge from his or her own mind. Doe, 487 U.S. at 210; Hubbell, 530 U.S. at 43. An analogy used by courts has been if the compulsion was like "being forced to surrender a key to a strong box containing incriminating documents [or is it] like being

compelled to reveal the combination to petitioner's wall safe." Doe, 487 U.S. at 210, n 9.

Being forced to convey from one's mind a password that could lead to the discovery of incriminating evidence, even if this password is not in and of itself incriminating, is completely distinguishable from the production of documents that were not created by a defendant, in his possession, or identified by defendant as discussed in Fisher and Doe.

The foregone conclusion exception as identified in Fisher and Doe is a narrow exception to the act of production doctrine. As digital technology is distinctly different than paper documents the foregone conclusion exception should not be considered applicable. Fisher, 425 U.S. 391 at 426 fn 7. However, even assuming *arguendo* the foregone conclusion exception is applicable to compelled private and personal digital technology, contrary to the Appellate Division's decision, this scenario as presented in Andrews' matter is distinctly different than Doe or Fisher. The State in this matter does not know what the passwords are, if Andrews knows them, or what is on the phones.

In Fisher, a defendant/taxpayer was subpoenaed to produce documents in his custody that had been prepared by defendant's accountant. Fisher, 425 U.S. at 394-395. The Court found that the defendant by producing the documents was not compelled to give oral testimony, the documents were not his work, nor was there a

testimonial declaration required from defendant to authenticate the documents. Id. at 409. However, the Court found that there could be acts of producing evidence in response to a subpoena that could have a communicative aspect. Id. at 410. The production could amount to the admission of the existence and control of the documents and result in their authentication. Id. at 410. The Court found that the documents subpoenaed were a foregone conclusion and the defendant/taxpayer added little or nothing to the sum total of the government's information. Id. at 411.

In Doe v. United States, the Court held that because the consent directive was not testimonial in nature compelling the target to sign it did not violate his Fifth Amendment privilege against self-incrimination. "In order to be 'testimonial', an accused's oral or written communication, or act, must itself, explicitly or implicitly, relate a factual assertion or disclose information." 487 U.S. at 210. An act of production could "constitute protected testimonial communication because it might entail implicit statement of fact; by producing documents in compliance with a subpoena, the witness would admit that papers existed, were in his possession or control, and were authentic." Id. at 209 citing United States v. Doe, 465 U.S. 605, 613 and n.11 (1984). The Court found that in determining whether a compelled communication is testimonial depends on the facts and circumstances of each case. Doe, 487 U.S. at 215. The consent directive was found

not to reference a specific account, that it was controlled by the subject, or that the account existed. The consent directive was not found to compel any knowledge that the subject had. Id. at 217-218. The Court found the compulsion was more like "being forced to surrender a key to a strong box containing incriminating documents than it is like being compelled to reveal the combination to petitioner's wall safe." Id. at 210, n.9 (omitting internal quotations).

Oddly the Appellate Division stopped its analysis at Doe and was essentially silent as to Hubbell. In Hubbell, a defendant was subpoenaed to identify eleven categories of documents as part of a prior plea deal and he invoked his Fifth Amendment privilege. Hubbell, 530 U.S. at 30-34. The Court stated, "[i]t has, . . . , long been settled that [Fifth Amendment] protection encompasses compelled statements that lead to the discovery of incriminating evidence even though the statement themselves are not incriminating and are not introduced into evidence." Id. at 37. The Court found that privilege of self-incrimination protected the target from being compelled to answer questions designed to elicit information about the existence of sources of potentially incriminating evidence. Id. at 45. The foregone conclusion exception did not apply, as the documents existence could not be independently confirmed and authenticated. Id.

The Hubbell Court found that production of the documents was

the equivalent of a defendant answering a series of interrogatories making use of the "contents of his own mind" that provided the link to the incriminating evidence." Id. at 41, 47. Unlike Doe, the Court found this to be similar to telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strong box. Id.

The test "is whether an act of production is testimonial is whether the government compels the individual to use the 'contents of his own mind' to explicitly or implicitly communicate some statement of fact." In re Grand Jury Subpoena Duces Tecum dated March 25, 2011, 670 F.3d 1335. 1345 (2012) *quoting* Curcio v. United States, 354 U.S. 118, 128 (1957). The compelled statements themselves do not necessarily have to be incriminating for it to be testimonial and entitled to protection. The Fifth Amendment protections encompass compelled statements that lead to the discovery of incriminating evidence. Hubbell, 530 U.S. at 37.

Contrary to the Appellate Division's decision, the Fifth Amendment prohibits the compelled disclosure of Andrews' passwords to his cell phones and the authentication of all the private and personal material in the cell phones. The State's compulsion for Andrews to divulge passwords to his cell phones is a testimonial communication that relates to either express or implied assertions of fact or belief which are incriminating. Unlike the compulsion in Doe, here the State must compel Andrews' "knowledge" to gain his

passwords that are a direct link to potentially incriminating evidence.

The Appellate Division closed its eyes to the integral nature of identifying the passwords and its inherent connection to the contents of the cell phones. The Appellate Division in failing to properly analyze Hubbell ignored the fact that Andrews will have to use the "contents of his own mind" to disclose the cell phone passwords. The Appellate Division's position that compulsion of Andrews to divulge his password is not testimonial, but a mere act that is inconsequential, ignores the controlling case law and the integral nature of identifying the passwords and its inherent connection to the contents of the cell phones which is unlike the business documents identified in Fisher and its progeny.

The Court has attempted to minimize the implications of technology and the expansive private material on cell phones by simplifying the analogy to paper based business documents and truncating the foregone conclusion analysis. This narrow exception to the Fifth Amendment and application to the New Jersey Common Law, statutory authority, and rules of evidence is not applicable under the law and the facts of this case.

**B. New Jersey Common Law, Statutory Law, and Rules of Evidence give Andrews the right to a privilege against self-incrimination from being compelled to disclose cell phone passwords. (Da20-Da24)**

Contrary to the Appellate Division's analysis, New Jersey protects Andrews from being compelled to provide the cell phone

passwords. In New Jersey, the privilege against self-incrimination "is firmly established as part of the common law of New Jersey and has been incorporated into our Rules of Evidence" and in our statutory enactments. State v. Hartley, 103 N.J. 252 260 (1986) quoting In re Martin, 90 N.J. 295, 331 (1982); N.J.R.E. 503; N.J.S.A. 2A:84A-19; N.J.R.E. 502; State of New Jersey v. Kelsey, 429 N.J. Super. 449 (App. Div. 2013).

The "state-law privilege against self-incrimination offers broader protection than its Federal counterpart under the Fifth Amendment." Kucinski, 227 N.J. at 617; State v. Muhammad, 182 N.J. 551, 568 (2005). The Supreme Court of New Jersey has a strong tradition of protecting the right to remain silent. Kucinski, 227 N.J. at 622. The "Fifth Amendment and the State privilege against self-incrimination apply to compelled actions as well as compelled testimony." State of New Jersey v. Fisher, 395 N.J. Super. 533, 541 (App. Div. 2007). Thus, the right against self-incrimination protects a defendant from being "subpoenaed to produce the gun or 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." In re Addonizio, 53 N.J. 107, 129 (1968).

This Court has concluded the State's common-law privilege against self-incrimination protects an individual's right to a private enclave where he may lead a private life. In the Matter of



Grand Jury Proceedings of Joseph Guarino, 104 N.J. 218, 231 (1986). In Guarino, a defendant who was a sole proprietor was served with a subpoena to produce specific documents and he asserted his right against self-incrimination. Guarino, 104 N.J. at 220-222. The New Jersey Supreme Court discussing Fisher and Doe found the Fifth Amendment "applies only when the accused is compelled to make a testimonial communication that is incriminating" and Guarino's business records were not protected. Guarino, 104 N.J. at 224, 228.

However, the Guarino Court continued its analysis discussing the personal privacy rights first embodied in the 1886 case of Boyd v. United States, 116 U.S. 616 (1886) *citing* Justice Brennan in the concurrence in Fisher. The New Jersey Supreme Court held that as this was a case of first impression it affirmed its belief in the Boyd doctrine and 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 230. The Court found that the nature of evidence must be examined to determine if it lies within that sphere of personal privacy. Id. at 231-232 *citing* Couch v. United States, 409 U.S. 322 (1973) (Marshall J. dissenting). The Court held that in the case of documents, the court must look to their contents not to the testimonial compulsion, failing to follow the rationale in Doe. Guarino, 104 N.J. at 232. However, the Court found that Guarino's business documents "did not lie within that special zone of privacy

that forms the core of the documents protected by Boyd and its progeny, and that are protected by the New Jersey privilege against self-incrimination." Id.

The Appellate Division's departure from this well-established precedent is monumental and will be a slippery slope for protection of privacy interests in New Jersey. The Appellate Division, with an anachronistic view of technology, dismissed Defendant's argument as to the connection of the testimonial communication of the password and its direct connection to the personal and private nature of a cell phone's contents. (Da20-Da22). The United States Supreme Court has recognized that cell phones are pervasive in modern life and there are substantial privacy interests at stake when digital data is involved. Riley v. California, 573 U.S. 373, 375(2014). As discussed in Riley, "modern cell phones [ ] are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." Id. at 386. The Riley Court recognized the distinct privacy issues related to cell phones and held there was higher Fourth Amendment protections when a defendant's phone was seized incident to an arrest. Thus, a warrant was required to search the cell phone. Id. at 403. The Riley Court noted that the "[t]he term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily

be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." Id. at 393. In the digital age, the balancing of individual privacy and governmental interests with regard to constitutional rights cannot rely on antiquated rationales or over simplification, but requires a more comprehensive legal analysis. Riley, 573 U.S. at 385-386. The Supreme Court in Riley recognized that cell phones by all they contain and may reveal hold for many Americans "the privacies of life" as cited in Boyd. Id. at 404 (*quoting Boyd v. United States*, 116 U.S. 116, 630 (1886)). Thus, the fundamental principles of Boyd still remain relevant in today's jurisprudence.

Further, the Appellate Division acted inappropriately when it found criminal investigations will be thwarted by password protection, therefore Defendant's privilege against self-incrimination must be expendable. (Da21-Da22). It is up to the Legislature to address issues with privacy rights regarding new technology. It is not an appropriate workaround for courts to unilaterally curtail Fifth Amendment and privacy rights when politicians fail to act. It has been acknowledged by Justice Alto in his concurrence in Riley, that the Courts would be better equipped to address these issues related to technology and privacy if "either Congress or state legislatures, after assessing the legitimate needs of law enforcement and the privacy interests of

cell phone owners, enact[ed] legislation". Riley, 573 U.S. at 407-408. As discussed in Riley, considering the sensitive privacy interests involved in searching cell phones it is suggested that the Legislature, elected by the people, not the courts, are in the better position to assess and respond to the present and future changes in digital technology. Id. at 408.

The United States Congress has started to address certain aspects of encryption related to manufactures, developers and sellers. In May of 2018, the Secure Data Act of 2018 was introduced in the House of Representatives. It proposed that no court should be able to issue an order to compel a manufacturer to alter security functions of or allow the search of a device. See Secure Date Act of 2018, H.R. 5823, 115<sup>th</sup> Cong., § 2 (May 15, 2018) (Da203-Da205). In June of 2018, the ENCRYPT Act of 2018 was introduced in the House of Representatives. See ENCRYPT Act of 2018, H.R. 6044, 115<sup>th</sup> Cong., § 2 (June 7, 2018). (Da200-202). The proposed Legislation is aimed at protecting a manufacturer, developer, seller, or provider of covered products from being forced to alter security features in a product or service to allow the government to use the device for surveillance.(Da204). It is further proposed that the government cannot force a manufacturer to decrypt information created for their devices or prohibit the sale of items that are encrypted.(Da204). Since July of 2018, no action has been taken on either of the proposed Legislations since they were forwarded to

the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations.

Since 2012, in an attempt to address digital privacy, state legislatures throughout the United States have introduced legislation prohibiting employers or educational institutions from requiring employees, applicants, or students from having to turn over passwords to social media accounts. See National Conference of State Legislatures, State Social Media Privacy Laws, May 22, 2019.<sup>5</sup>(Da126-Da128); National Conference of State Legislatures, LegisBrief, Social Media Privacy Laws, Vol. 22, No 16, April 2014<sup>6</sup>,.(Da129-Da131). Specifically, New Jersey has passed Legislation that prohibits public or private institutions of higher education from requiring a student or applicant to provide or disclose any user name or password to a personal account or service. N.J.S.A. 18A:3-30. Similarly, employers are prohibited from requiring or requesting a current or prospective employee to provide or disclose any user name or password to a personal account. N.J.S.A. 34:6B-6. It is noted that primarily state laws that protect students apply only to public and private postsecondary educational

---

5 Website: <http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-prohibiting-access-to-social-media-username-and-passwords.aspx>

6 Website:  
<http://ncsl.org/LinkClick.aspx?fileticket=BVJdSjQJWeA%3d&tabid=28043&portalid=1>

institutions. See LegisBrief, Social Media Privacy Laws, at 2 (Da130).<sup>7</sup>

In 2016, due to increasing legislation in the area of employee and student online privacy, the Uniform Law Commission adopted a proposed uniform state law titled "Uniform Employee and Student Online Privacy Protection Act" See National Conference of State Legislatures, LegisBrief, State Social Media Privacy Laws, May 22, 2019.<sup>8</sup> (D126). This proposed uniform state law has been utilized as guidance by States in addressing the issue of social media access relative to employees and students. See Hawaii Legislature, A Bill for an Act relating to the Uniform Employee and Student Online Privacy and Protection Act, H.R. Thirtieth Legislature, H.B. No. 6, February 4, 2019 (last amendment April 25, 2019 in Conference Committee).<sup>9</sup>(Da211-Da227); New York Legislature, Senate, 2019-2020, Act to Amend Labor Law in relation to the Uniform Employee and

---

7 There is a diminished expectation of privacy between elementary and high school with regard to the ability of schools to conduct searches and seizures. However, this diminished expectation of privacy is not extended to law enforcement with regard to minors in the elementary and high school setting. New Jersey v. T.L.O., 469 U.S. 325 (1985). The T.L.O. analysis has been extended to cell phone searches by school personnel. Klump v. Nazareth Area School District, 425 F. Supp. 2d 622 (E.D. Pa 2006).

8 Website:

<http://ncsl.org/LinkClick.aspx?fileticket=BVJdSjQJWeA%3d&tabid=28043&portalid=1>

9 Website:

[https://www.capitol.hawaii.gov/measure\\_indiv.aspx?billtype=SB&billnumber=296](https://www.capitol.hawaii.gov/measure_indiv.aspx?billtype=SB&billnumber=296)

Student Online Privacy Protection Act, S2728, Add Art. 33 §§950-955 Lab. L, January 29, 2019 (currently being amended in Committee)<sup>10</sup>(Da228-Da232).

Certain countries have legislatively addressed the protection of electronic communications regarding the compelling of passwords related to suspects and incrimination. For example in Finland, subscribers and users of electronic communications services have a right to protect their communications and identification information how they wish unless otherwise provided by law. Although Finish law provides that a person can be required to hand over passwords/decryption if keys are necessary to conduct a search of a device, the person cannot be a suspect or the accused. See United Nations Office on Drugs and Crime, Sharing Electronic Resources and Laws on Crime, Finland Legislation, Section 23 of Chapter 8 of the Law on Coercive Measures Act, July 22, 2011.<sup>11</sup> (Da206-Da207).

In the Netherlands, there is legislation that an investigating judge can order someone to decrypt a device, however this request cannot be directed to the person who is the suspect. See Netherlands Legislation, Criminal Procedure Code, Section

---

10 Website: <https://legislation.nysenate.gov/pdf/bills/2019/S2728>

11 Website:

[https://sherloc.unodc.org/cld/en/legislation/fin/coercive\\_measures\\_act/chapter\\_8/sections\\_20-29/sections\\_20-29.html?](https://sherloc.unodc.org/cld/en/legislation/fin/coercive_measures_act/chapter_8/sections_20-29/sections_20-29.html?)

126nd, October 8, 2012.<sup>12</sup>(Da208-210).

On January 24, 2019, the Ontario Court of Justice found that an accused could not be compelled to provide his cell phone password. It was found this compelled disclosure would violate his rights not to incriminate himself as it would be required to "speak his mind". Her majesty the Queen and Suhail Shergill, 2019 ONCJ 54 (Jan. 24, 2019) (D132-Da144). The Court acknowledged the difficulty and need for balance between the rights of the individual and the rights of the state. (Da142-Da143). The Court in acknowledging the difficulties of the digital landscape suggested that legislative initiatives or modifications may be more appropriate to deal with this issue in the interest of justice. Id. at 12 (Da143).

Although there is no specific laws or rules pertaining to target or suspects being required to disclose their passwords to digital devices, N.J.R.E. 502, N.J.R.E. 503 and statutory law N.J.S.A. 2A:84A-19 protect Andrews from being compelled to disclose his cell phones' passwords. In an effort to gloss over these protections, the Appellate Division dramatically asserts that the State has a "superior right of possession" to the phones since there was a search warrant. There is no constitutional authority for a search warrant being the equivalent of ownership in this

---

<sup>12</sup> Website:

[http://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/Wetboek vanStrafvordering\\_ENG\\_PV.pdf](http://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/Wetboek%20vanStrafvordering_ENG_PV.pdf)



context. In fact, the Appellate Division cites no authority for its "superior right of possession" theory as a result of a search warrant. The Court has conflated access that satisfies the Fourth Amendment with ownership to validate the right to force a person to incriminate himself. This was a misapplication of well-established constitutional law. State v. Powell, 294 N.J. Super. 557 (App. Div. 1996). Judges and scholars have disputed the relationship between the Fourth and Fifth Amendment in the criminal context. Commonwealth v. Jones, 481 Mass. 540, 563-564 fn1 (2019) (concurrency Lenk, J); See also Carpenter v. United States, \_\_\_ U.S. \_\_\_\_, 138 S.Ct. 2206, 2271 (2018) (Gorsuch, J. dissenting). The mere fact that the Fourth Amendment has been satisfied by the issuance of a warrant does not erode the constraints imposed by the Fifth Amendment.<sup>13</sup> As discussed by Justice Lenk of the Pennsylvania Supreme Court "the coequal amendments do not dwell in splendid isolation, and that the Fourth Amendment does not somehow limit or

---

13 In State of Missouri v. Johnson, \_\_\_ S.W.3d \_\_\_ (2019) 2019 WL 1028462 (Mo. App. W.D. March 5, 2019) (Da176-Da198) the Court addressed not only the issues relative to defendant's Fourth Amendment rights and then addressed his Fifth Amendments rights. Just because the search warrant was found to have complied with the Fourth Amendment did not mean that the defendant's Fifth Amendment rights were not analyzed. This was a case of first impression for Missouri wherein it found the compelled act of production was not testimonial and not protected by the Fifth Amendment as the defendant had opened his cell phone with a password in front of law enforcement and defense counsel for the purpose of having his expert examine the phone, thus compelling the password for a second time was a foregone conclusion. Id. at \* 20-21 (Da195-Da196).

trump the Fifth Amendment whenever there may be a valid search warrant." Jones, 481 Mass. at 563-564 fn 1 (concurring Lenk, J); In re of the Search of a Residence in Oakland, California, 354 F. Supp. 3d 1010, 1015-1016 (9<sup>th</sup> Cir. 2019) (even if there is a valid search warrant Fifth Amendment rights are given full consideration). The fact that a search warrant was issued in Andrews' matter does not make arguments related to incrimination and privacy obsolete. The theory of the Appellate Division provides law enforcement with *carte blanche* court sanctioned fishing expeditions.

In espousing this novel theory that a warrant overrides the protections and considerations of the Fifth Amendment, the Appellate Division also ignored the fact that defendants are not represented at the warrant application process. Similarly, just because a suspect is arrested pursuant to an arrest warrant issued under the Fourth Amendment does not mean that the same defendant waives his right against self-incrimination provided by the Fifth Amendment absent a *Miranda* warning. The Appellate Division's "superior right of possession" theory cannot withstand Constitutional scrutiny. Contrary to the Appellate Division's decision, the passwords and phone contents are so intertwined that one cannot be separated from the other. The contents of the password from Andrews' mind unlocks the "safe" that is Andrews' phones, the "loot" as referenced by the Supreme Court in In re Addonizio. The

Fourth Amendment in this instance does not trump Andrews' right not to incriminate himself.

The New Jersey common law and the Fifth Amendment to the United States Constitution prohibits Andrews from being compelled to disclose his cell phone passwords, clearly a testimonial communication. *Stare decisis* controls in this matter and the Appellate Court failed to follow the precedential cases regarding the privilege not to incriminate one's self. State v. Brown, 190 N.J. 144, 157 (2007). "Even in constitutional cases, the doctrine [of *stare decisis*] carries such persuasive force that we have always required a departure from precedent to be supported by some special justification." Id. There was no special justification to depart from precedent in Andrews' matter that eliminated his protections not to incriminate himself.

New Jersey case law required the Appellate Division to look at the nature of the evidence to determine if the evidence sought by the Government was within the sphere of personal privacy. Andrews cannot be compelled to divulge his private cell phones' passwords from his inner thoughts and the evidence that this would reveal. Cell phones are used as personal diaries, a recorder of personal images and videos, address books, calendars, libraries, and research devices. Thus, compelled disclosure of a password to a personal cell phone is not only testimonial and a compulsion of an inner thought, but the contents of the evidence lies within the

sphere of personal privacy. This is an obvious distinction between the contents of a personal cell phone and business related documents. Logic dictates that the more private and personal an item to an individual, such as the digital information on cell phones, the less intrusion the State is permitted. The contents of a cell phone is exactly the type of information protected by Guarino. The Court should, most respectfully, grant Andrews' appeal and reverse the Appellate Division's affirmance of the Trial Court Order.

### POINT III

**ANDREWS' RIGHT TO REMAIN SILENT HAS BEEN VIOLATED AND THE FOREGONE CONCLUSION EXCEPTION WAS MISCHARACTERIZED. (Da1-Da20)**

The erroneous decision by the Appellate Division that the compelled disclosure of Andrews' cell phone was not a protected testimonial communication was compounded when it adulterated the foregone conclusion exception to the Fifth Amendment and found that this exception was satisfied. Assuming the Court finds the foregone conclusion exception applicable in this matter, the Appellate Division, in what appears to be a hedge to overcome the compelling testimonial communication and violating Andrews' rights, erroneously relied on its own newly formulated exception. Fisher, 425 U.S. at 410. The Appellate Division gutted the analysis and application of the exception breaking it down to its simplest form,

to the point where it has no meaning eviscerating Defendant's constitutional protections, ignoring the requirement that the State must demonstrate its knowledge with "reasonable particularity" as to what it knows it will find on Andrews' cell phones.

The foregone conclusion doctrine is only applicable if the compelled information is already known to the government and this revelation by the defendant offers little or nothing to the sum total of the government's information. Fisher, 425 U.S. at 411. For an act of production, the State must demonstrate that the item exists, it is in the possession or control of the target, and the item is authentic. Doe, 465 U.S. at 613, fn 11. The standard is that the State must demonstrate with "'reasonable particularity' that, at the time it sought to compel the act of production, it already knew of the materials, thereby making any testimonial aspect a 'foregone conclusion'". In re Grand Jury Subpoena Duces Tecum dated March 25, 2011, 670 F.3d at 1346.

Simply put, the foregone conclusion exception to the Fifth Amendment is not applicable in this case. Andrews' passcodes are not a foregone conclusion as the State does not know what they are. For all the State knows, the passcodes themselves, once revealed by Andrews' mind, could be in and of themselves incriminating.<sup>14</sup>

---

<sup>14</sup> The mere fact that the password is required to be disclosed *in camera* does not remedy the fact that the State does not know the passwords or if the Defendant even has knowledge of them years after the phones were seized. Moreover, once a password is

The Appellate Division's application of the exception was in totality the following: Defendant knew the passwords, was in possession or control of the phones, and his knowledge of the passwords added nothing to sum total of the State's information as to what it is seeking which is the password. This approach, was an end run around the complexity of the record and the State's genuine lack of "reasonable particularity". The Court then continues that Defendant was only ordered to disclose his password "not the contents of the phones unlocked by those passwords." (Da10). We confess to being seriously flummoxed by this analysis in the age of digital technology and the integral nature between the password and decryption of the contents of the cell phone. By compelling the passwords are not the contents disclosed?

The Appellate Division's reasoning in distinguishing the cases cited by Defendant was not persuasive and contradicted by its reliance on United States v. Apple MacPro Computer, 851 F.3d 238 (3d Cir. 2017). (Da18-Da19). The reliance on United States v. Apple MacPro Computer is misplaced as that Court found the compulsion of decryption was a testimonial communication and the foregone conclusion exception was applied as to the substance of the facts, not the constitutionally violative analysis set forth in the

---

disclosed, with the potential of it being in and of itself incriminating, the cat is essentially out of the bag and the incrimination complete whether or not disclosed to the State as the Court now knows.

instant decision. Moreover, the facts of Apple MacPro are distinguishable from Andrews' matter.

Apple MacPro was a contempt case, with an onerous message to defendants that if you don't remember or provide your passwords, regardless of time or memory, you are going to jail. This is alarming and problematic on its face.<sup>15</sup> The Apple MacPro case sought external hard drives that had already been identified by forensic analysis, by eye witnesses, and the defendant himself by unlocking his cell phone that contained child pornography. Apple MacPro, 851 F.3d at 248. Although the Appellate Division dismissed the reasoning in In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, in Apple MacPro the Court relied on the instruction of that case finding that the compulsion of decryption code was testimonial. Id. at 247-248. Moreover, relying on In re Grand Jury

---

<sup>15</sup> As reported by Jon Schuppe of nbcnews.com, on June 7, 2019 William Montanez was held in jail in Florida for refusing to provide his cell phone passwords at the time of being arrested, and later in response to a warrant, related to traffic stop that resulted in alleged drug and weapons charges. Law enforcement and the Florida Court relied on the State v. Stahl, 206 S. 3d 124 (Fla Dist. Ct. App. 2016) decision and held Montanez in contempt. Montanez reportedly was concerned about a fishing expedition for illegal activity and disclosure of his private personal matters on his phone that included intimate pictures of his girlfriend. After being in jail for 44 days for failing to provide his passwords the underlying charges were dropped and the contempt order dismissed. See Jon Schuppe, Give up your password or go to jail; Police push legal boundaries to get into cell phones, nbcnews.com, June 7, 2019, <https://www.nbcnews.com/news/us-news/give-your-password-or-go-jail-police-push-legal-boundaries-n1014266> (Da145-Da151).

Subpoena Duces Tecum Dated Mar. 25, 2011 the Apple MacPro Court found that the Government had satisfied "reasonable particularity" as to what was on the external hard drives by the specific forensic analysis and witnesses. Apple MacPro, 851 F.3d at 247-248.

Although the Appellate Division relied on Apple MacPro it failed to apply the analysis set forth in the decision. The Apple MacPro Court specifically did not decide if the inquiry was limited to the question of whether simple knowledge of the passwords itself is sufficient to support an application of the foregone conclusion doctrine. Apple MacPro, 851 F.3d at 248 fn 7. Further, the Court's reliance on Commonwealth v. Gelfgatt, 11 N.E.3d 605 (Mass. 2014) is distinguishable as the State in that case, unlike here, was able to see the documents that were located on external hard drives and the defendant made statements to the authorities regarding the documents that the State sought.

Since the ruling in Gelfgatt, the Massachusetts Supreme Court has held that State must prove a defendant knows the password to decrypt an electronic device beyond a reasonable doubt for the foregone conclusion exception to apply.<sup>16</sup> Commonwealth v. Jones, 481

---

<sup>16</sup> The inconsistency in the application of the standard of proof for the foregone conclusion exception with regard to decryption is further identified in the case of United States of America v. Spencer, 2018 WL 1964588 (N.D. Cal. April 26, 2018) (Da152-Da155) where the State was seeking the actual decrypted devices and distinguished itself stating it was not seeking the written or oral disclosure of a password although the Court found this still could be incriminating. The standard used by the Court for



Mass. 540, 555-558 (2019). The Court found that a lower standard creates a greater risk of incorrectly imputing knowledge to a defendant who does not know the password. Id. at 555. The Court acknowledged that if there was an erroneous imputation of knowledge and a defendant could not comply, not only would there be a violations of his rights, but the jeopardy of a finding of civil or criminal contempt. Id.

As stated by Justice Lenk in the concurrence of Jones, "[t]he Court's decision today sounds the death knell for a constitutional protection against compelled self-incrimination in the digital age." Id. at 566. Justice Lenk disagreed with the analysis of the majority finding that the foregone conclusion doctrine required

---

compelled decryption was by clear and convincing evidence with regard to the foregone conclusion exception. Id. at \* 2-3 (N.D. Cal., April 26, 2018) (Da152-Da153).

A year later in the United States v. Maffei, 2019 WL 1864712 (N.D. Cal., April 25, 2019) (Da156-Da165) the Court found that compelling the password was a testimonial communication as the contents of a person's mind had to be used and this resulted in implied statements of fact. Id. at \*6 (Da161). The foregone conclusion analysis was not reached as there was no facts in the case that defendant knew the passwords distinguishing the case from Spencer. Id. at \*9 fn 5 (Da164). In this case the Court found that the defendant's Fourth Amendment rights were violated by exceeding the search warrant when the State asserted the compelled disclosure of a verbal or written password was the same as the authorized biometric key. Id. at \*7-8 (Da162-Da163). Further, the Court found that defendant's Miranda and Sixth Amendment rights were violated when while she was under arrest she had asked for counsel and was still approached about providing her passwords to her Apple iPhone devices which she complied with leading to incriminating evidence. Id. at \* 8-9 (Da163-Da164).

that the government be able to describe with reasonable particularity the documents or evidence it seeks to compel. Jones, 481 Mass. at 563-564.

As per the majority in Jones, in Andrews' matter the State would not meet the bar of beyond a reasonable doubt to establish the foregone conclusion was applicable as they do not even know if Andrews' knows the passwords or what phone has what alleged information.

The Appellate Division dropped into a footnote the Florida case of State v. Stahl, 206 So.3d 124 (Fla. 2d. DCS 2016), the primary authority relied on by the instant Trial Court, and mirrors the Appellate Division's decision in its simplicity and findings. (Da15).

Stahl has been identified as an outlier by the Florida case of G.A.Q.L. v. State of Florida, 257 So.3d 1058 (October 24, 2018). In Contrast to Stahl, the G.A.Q.L. Court found that the compelled disclosure of a cell phone password is a testimonial communication and protected by the Fifth Amendment. Id. at 1062-1063. The Court ruled that it is not simply the password the Government was seeking, but the communication behind the password wall. Further, it found that the foregone conclusion exception is not satisfied by simply determining that the password existed. Id. at 1063-1065.<sup>17</sup>

---

<sup>17</sup> The Appellate Division in footnote 1, in an effort to support its decision, cited the Pennsylvania case of Commonwealth v.

The Appellate Division erred by not reviewing the "reasonable particularity" identified by the Trial Court. The Appellate Division ignored the required analysis of determining what the specific evidence the State was seeking by asserting it was immaterial as to the contents of the phone and that all that was being compelled was simply the disclosure of the cell phone password. If the Appellate Division had performed the proper analysis, it would have determined that the Trial Court incorrectly determined that the State satisfied the factual prerequisites for "reasonable particularity". The State does not know what if any information is on Andrews' cell phones and/or where it believes this information is located on the cell phones.<sup>18</sup> The State waited over two years before seeking the compulsion of Andrews' cell

---

Davis, 176 A.3d 869 (Pa. Super Ct. 2017) that found the compelling of a password was not testimonial. However, in contrast to the analysis utilized in Andrews' matter, the Davis Court touched upon the foregone conclusion by detailing what had been expected to be found on the computer stating that there was a high probability that child pornography existed on the computer and there was the tacit acknowledgement by the defendant that the State knew what was on the computer and giving his password was like putting a gun to his head. Id. at 876. The Davis case has been appealed to the Supreme Court of Pennsylvania. Commonwealth v. Davis, 195 A.3d 557 (2018).

<sup>18</sup>An issue of control was raised before the Trial Court as one of the cell phones was not registered in Andrew's name. This issue should not have been ignored by the Trial Court and the Appellate Division since the State could not even identify which one of the two phones it believed had the predominate communications. This further establishes the State did not have any reasonable particularity required for the foregone conclusion exception.

phones' passwords. This was a last ditch effort on the part of the State in an attempt to find evidence to support its paper thin prosecution of Andrews. The State conceded that it wanted everything on the two phones as it did not know what actually was on the phones. Shockingly, the State admitted it could not even pin point what phone it was referencing, a significant fact that was overlooked by the Trial Court and the Appellate Division.

As to the call logs relied on by the State, the Trial Court was told that it had to "infer" what these logs meant to support the invasion of Andrews' Fifth Amendment rights. There was no evidence that the calls between the men were criminal in nature. The mere fact these men called each other is insufficient to satisfy the foregone conclusion doctrine. Case law is clear that mere inference does not satisfy the trampling of Constitutional rights.

There was no evidence that Andrews communicated with Lowery on his cell phone regarding the alleged crimes related to the GPS, wiretap communication, or undercover agents. Lowery specifically said "none of that shit was on the phone." (Da99). It is significant that the State had no evidence that Andrews and Lowery even met in person and no evidence of any illegal communications. Lowery could not provide any dates for the alleged meetings or when Andrews allegedly told him to get rid of his phones. In fact, Lowery said after "he noticed" he was being followed he got rid of his phones. None of these actions involved Andrews. Finally, there is no

evidence that Lowery sent Andrews any information regarding the undercover detective. The Trial Court's decision to believe some of Lowery's statements and disregard other statements cannot be reconciled and was a result driven determination. For example, the Trial Court believed Lowery's Grand Jury testimony that he had conversations with Andrews about getting rid of phones, but ignored Lowery's testimony that the phones were never used to communicate.

The Trial Court's erroneous reliance on one text message from Lowery, and "inferences", does not support the foregone conclusion doctrine. The singular text message from Andrews was as per Lowery related to a job. The text of a license plate number was unilaterally sent by Lowery with no response from Andrews and no evidence the plate was run.

Oddly, almost all the facts cited by the Appellate Division do not relate to any alleged information on the cell phones. Further, the Appellate Division failed to distinguish that Andrews as a Sheriff's Officer would have to obey an Order to surrender his phones. However, he never made any statements regarding the phones contents nor did he indicate knowledge of the passwords. The Appellate Division's failure to review the foregone conclusion analysis as related to the facts has instead circumvented it entirely, thus calling for this Court's review and reversal of the Appellate Division's affirmance of the Trial Court's Order.

#### POINT IV

THE APPELLATE DIVISION MISAPPLIED THE LAW AND THE FACTS IN ARRIVING AT ITS DECISION AND RELIED ON OUT OF STATE CASE LAW THAT ARE OUTLIERS CONTRARY TO HUBBELL, NEW JERSEY COMMON LAW, STATUTORY LAW, AND THE RULES OF EVIDENCE. (Da1-Da20)

Just as in New Jersey, many states have been grappling with the challenges related to digital technology and encryption. Andrews presents the following cases that are on point as instructive and persuasive authority supporting the proposition that his compelled disclosure of passwords is a testimonial communication protected by the Fifth Amendment to the United States Constitution. Further, the foregone conclusion exception requires substantive analysis, not the mere fact that the Government knows a passwords exists.

The Appellate Division, without success, attempted to distinguish the case of United States v. Kirschner, 823 F. Supp.2d 665 (E.D. Michigan, Southern Division 2010). In Kirschner, a defendant, who was alleged to have child pornography on his computer, was not compelled to disclose all his passwords used or associated with his computer and files. The computer had files that were encrypted. Kirschner, 823 F.Supp2d at 666-667. Defendant refused to provide the computer passwords based on his Fifth Amendment privilege against self-incrimination. Id. at 668. The issue before the Court was whether requiring Defendant to provide the password was a testimonial communication. Id. The Court found

that the compulsion of the password would be divulged from the defendant's mind and lead to evidence that would be used to incriminate him. The Court relied on Doe v. United States, 487 U.S. 201 (1987) and Hubbell, 530 U.S. 27 (2000). Id. at 668-669.

The Court distinguished the consent directive in Doe with the compelled disclosure of the password from a person's mind to the computer. The password was considered communicating a factual assertion to the government and was testimonial. This was considered a communication of knowledge. Id. at 669. The Court found this compulsion about producing specific testimony asserting a fact. The Court found Hubbell was directly relevant when compelled testimony led to incriminating evidence. Id. The Court quashed the subpoenas requiring the defendant to testify, giving up the password, thereby protecting his Fifth Amendment privilege against self-incrimination. Id.

Courts have continued to find disclosure of encrypted files testimonial and have followed the standard with regard to "reasonable particularity" when applying the foregone conclusion exception to the Fifth Amendment with regard to encrypted computer files. The Appellate Division made a great effort to distinguish In re Grand Jury Subpoena Duces Tecum Dated March, 25, 2011, 670 F.3d 1335 (U.S. Ct. App. 11th Cir. 2012). In In re Grand Jury, a target accused of having child pornography on computer drives could not be compelled to provide a decryption password as the

communication would be testimonial and tantamount to providing potentially incriminating files and the testimony was not a foregone conclusion as the Government did not know what if any files existed on the computer. The Court found the compulsion was akin to requiring the production of a combination to a safe. It required the use of the mind and implied factual statements. Id. at 1345.

The Court found the compelled testimony was not a foregone conclusion. Id. at 1346. The Government could not demonstrate whether any files existed or where they were located on the hard drives. Further, there was no evidence the target could even open the files. Just because there was storage space to hold the files did not mean that the drives contained the files sought after. Id. The Court cited the distinction between the case of Fisher wherein the Government knew what documents were in the attorney's possession and in Hubbell wherein the Government had not shown it had any knowledge of the existence or whereabouts of the documents. Id. The Government could not cure its lack of knowledge by referencing broad categories of documents and or files and relying on inferences. Id. at 1348. The Court distinguished this case from In re Boucher, 2009 WL 424718 (D.Vt. Feb. 19, 2009) (106a-109a) where the government had viewed the portions of an encrypted file with the suspect and saw the images of the child pornography. Id. at 1348.



Compulsion of passwords for smart phones have been found to be testimonial and protected by the Fifth Amendment. In the case of Commonwealth of Virginia v. David Charles Baust, 89 Va Cir. 267 (October 28, 2014), a defendant could not be compelled to disclose a password to a cell phone as it was considered testimonial and not subject to the foregone conclusion as it was not known outside the defendant's mind. If the password was actually a foregone conclusion the Government would not need defendant to produce the password because they would already know it. Id. The Court found Kirschner and Hubbell instructive. Id. The Appellate Division gave no weight to this decision.

In the case of the Securities and Exchange Commission v. Bonan Huang, et al., Case 2:15-cv-00269 (September 23, 2015), targets of subpoenas were not compelled to disclose smart phone passwords as the compulsion involved the personal thought process of the targets and was considered testimonial. (Da118-Da124). The foregone conclusion exception was not satisfied by the targets simply possessing the cell phone. The mere possession was insufficient since the SEC could not show what documents were on the device or if they existed at all. (Da118-Da124). The Court cited the reasoning in In re Grand Jury Duces Tecum, Dated March 25, 2011, and Kirschner. (Da122-Da124). The motion to compel the passwords was denied as the compulsion was testimonial in nature and Defendants had properly invoked their Fifth Amendment privilege and the

foregone conclusion did not apply. (Da124). Although Andrews cited this case the Appellate Division was silent as to this decision.

The United States Court of Appeals for the Armed Forces has also found that the compulsion of a cell phone password is "incriminating information in the Fifth Amendment sense, and thus privileged." United States v. Mitchell, 76 M.J. 413, 418 (2017). The Court reasoned that forcing a target in custody to provide a password is akin to providing an answer in an interrogation which would furnish a link in the chain of evidence to prosecute a target. Id. This case was also identified as instructive to the Appellate Division, it was not considered.

The compulsion to disclose one's password can lead to the impossible choice of either incriminating yourself or being found in contempt. In the case of State of Maine v. Trant, 2015 WL 7575496 (Oct. 27, 2015) (Da166-Da169) the Court held that forcing a defendant to produce a password is a mental process. Id. at \*2 (Da167). The State attempted to avoid the testimonial hurdle by asserting it was only requesting the defendant to open the phone not provide a password. The Court did not find this argument persuasive and found that the compelled disclosure left defendant with either the choice of acknowledging that he can access the phone and potentially incriminate himself or lie about his inability to do so. The Court noted that failure to comply, or his inability to do so, would subject him to contempt proceedings. Id.

(Da167). The Court found that the State did not satisfy the foregone conclusion exception as there was no proof that defendant knew his passwords, had control over the cell phone, or what information was stored on the phone. Id. at \*3 (Da. 168).<sup>19</sup>

In the case of United States v. Sanchez, 334 F. Supp. 3d 1284 (2018) the Court found that compelled production of a parolee's cell phone passwords was in violation of his Fifth Amendment rights. Id. at 1296. In this case a parolee initially refused to produce his passwords, and then produced same only after being advised his failure to do so would result in his arrest which ultimately

---

<sup>19</sup> The Supreme Court of Indiana recently heard arguments in a decryption case that resulted in criminal contempt charges. In the case of Seo v. State of Indiana, 109 N.E.3d 418 (Ind. Ct. App.), transfer granted, opinion vacated, 119 N.E.2d 90 (Ind. 2018) Seo was charged with stalking and invasion of privacy and a warrant was issued to compel the unlocking of her cell phone. Seo refused, was found in contempt and jailed. Id. at 421-423. Seo appealed and the Court found the contempt order violated Seo's Fifth Amendment rights as she was being forced to provide a testimonial communication from her mind to obtain incriminating information. The Court found the compelling of the password akin to a safe combination and each time the phone is decrypted the files were recreated. The Court found a distinction between paper documents and storage to electronic data. Id. at 430-431. The Court also found the foregone conclusion exception did not apply as the State could not infer what information was on the cell phone and failed to describe the digital information it sought to compel. Id. at 433.

The State filed a petition to transfer challenging the Court of Appeals opinion. The Indiana Supreme Court granted the transfer, vacated the decision, and assumed jurisdiction. Seo v. State of Indiana, 109 N.E.3d 418 (Ind. Ct. App.), transfer granted, opinion vacated, 119 N.E. 3d 90 (Ind. 2018). The Supreme Court of Indiana heard arguments in this matter in April of 2019.

happened for failing to follow orders of his parole officer with regard to the production. Id. at 1291-1292. The Court found the parolee could not be arrested for refusing to incriminate himself and the incriminating evidence was considered the "fruit of the poisonous tree." Id. at 1298-1299.

In the case of People v. Spicer, \_\_\_ N.E.3d \_\_\_ (2019) 2019 WL 1075261 (IL App. (3d) March 7, 2019) (Da170-Da175) Spicer was a passenger in a car that was pulled over at a traffic stop. A search of the vehicle found cocaine in the area of where Spicer was sitting. He was arrested for possessing a controlled substance with intent to distribute. A cell phone was found on Spicer's person incident to the arrest. The State received a search warrant and sought to compel the password. Spicer refused to provide the password. People v. Spicer, \_\_\_ N.E.3d \_\_\_ (2019) 2019 WL 1075261 \* 3 (IL App. (3d) March 7, 2019) (Da172). The Court noted that Illinois Courts had not decided whether compelling a defendant to provide a password was testimonial. Id. at \*5 (Da174). The Court compared the out of state jurisdictions and found the decision in G.A.Q.L v, State, 257 So.3d 1058 (Fla. Dist. Ct. App. October 24, 2018) as persuasive and a reasoned decision. Id. at \*5-6 (Da174-175). The Court found that the revealing of the password was testimonial. It ruled that it was not the password *per se* that the State was seeking, but the information that it would decrypt. In performing a foregone conclusion analysis the proper focus was not

the password itself, but the information the password protects. Id. at \*6 (Da176). In this case the State had not provided a particularized description of the information or evidence that was allegedly on the phone with any reasonable particularity, thus the foregone conclusion did not apply. The Court denied the State's motion to compel defendant to provide his password. Id. at \*6. (Da176).

As further evidence of the private personal nature of digital devices, targets have also been protected from being compelled to provide Biometrics to open electronic devices. In the case of In re Application for a Search Warrant, 236 F. Supp. 3d 1066 (Feb. 16, 2017) a warrant was issued that compelled individuals on a premises of a location that was trafficking in child pornography to provide fingerprints or thumbprints to unlock Apple electronic devices to obtain their contents. Id. at 1067. The Court found the warrant did not establish sufficient probable cause to compel any person who happened to be at the location to give his fingerprint to unlock unspecified Apple electronic devices. Id. at 1068.

The Court in this matter also found that the warrant application raised Fifth Amendment concerns. The Court found that by using a finger a suspect was producing the contents of his phone and testifying that he has accessed the phone before and has some control over it. Id. at 1073. The Court found that the use of a fingerprint to access a database gave access to someone's most

private information and this was starkly different than using a fingerprint to place someone at a particular location. Id. The Court stated this was a fact sensitive analysis and that the existence and nature of the electronic information sought would have to be a foregone conclusion to overcome the concerns relative to the Fifth Amendment. Id. at 1074. The Court found the government had not established a proper basis to force any individual at the premises to provide a fingerprint or thumbprint to attempt to unlock any Appel device found. Id.

In the case of In re of the Search of a Residence in Oakland, California, 354 F. Supp. 3d 1010 (9<sup>th</sup> Cir.2019) the government was investigating a case of extortion and issued a search and seizure warrant for various items that included electronic devices. The government was also seeking the authority to compel any individual at the time of search to press a finger, thumb, or other biometric feature to unlock the devices. In re of the Search of a Residence in Oakland, California, 354 F. Supp. 3d 1010, 1013-1014 (2019).

The Court found that the Fourth Amendment was not satisfied as the search warrant was overbroad and there was not sufficient probable cause to compel anyone on the premises to provide their thumb, finger, or other biometric feature. Id. at 1014.

The Court further found that even if there was probable cause to seize the devices during a lawful search it did not permit the government to compel a suspect to waive rights otherwise afforded

by the Constitution including the Fifth Amendment. Id. at 1015-1016. The Court cited the Supreme Court of the United States wherein it instructed courts to adopt rules that take into account sophisticated systems and that Courts have an obligation to safeguard constitutional rights that should not be diminished merely due to the advancement of technology. Id. at 1014 *citing* Carpenter v. United States, 138 S. Ct 2206, 2214, 2218-19 (June 22, 2018).

The Court found that the act of compelling a communication of a password is testimonial, whether verbal or written, as it is an expression of an individual's mind and protected by the Fifth Amendment. In re of the Search of a Residence in Oakland, California, 354 F. Supp. 3d at 1015-1016. Utilizing a biometric feature to unlock an electronic device was found not to be similar to fingerprinting or a DNA swab. The Court stated that since compelling a password is a testimonial communication a person cannot be forced to unlock the same device using a biometric feature. The act of using the biometric feature concedes the device was in the possession and control of the suspect and authenticates ownership or access to the phone and all its contents. Id. at 1015-1016.

The Court found the foregone conclusion exception did not apply since the government lacked the requisite prior knowledge of the information and documents that could be obtained via a search

of the unknown digital devices. The Court identified that by compelling a suspect to unlock his device a mobile application previously unknown for cloud storage could be disclosed which is the equivalent of a locked cabinet the government did not know about. In this case the government could not articulate facts of unlocking devices by biometric features of unknown individuals. Id. at 1017-1018.

Similar to Kirschner and In re Grand Jury, where the act of disclosing a password for an encrypted computer or files should be considered testimonial and incriminating, so should a cell phone password. As instructed by Baust, Huang, Spicer, and G.A.Q.L., Andrews is protected by the privilege to not incriminate himself by being forced to disclose his password from his mind. As instructed in these out of jurisdiction cases, Andrews mere possession of cell phones, and that calls were made on the phones which required inferences to be drawn without any factual support, is not sufficient to demonstrate that any other evidence exists on the cell phones. Just because it is "passwords" that are being compelled from Andrews does not eviscerate the privileged nature of the compulsion as this is not a simple surrender as found in Baust, Kirschner, and Hubbell. It is not the password the State is seeking, but the information that this password would decrypt.

Any assertion otherwise is creating a false narrative as to the stripping of Constitutional safeguards in an effort to ignore



the advanced technology and the private and personal information encapsulated within this technology. Andrew's case is similar to In re Grand Jury, Spicer, and G.A.Q.L. as the compelled testimony is not a foregone conclusion. The simplicity that the password itself is the foregone conclusion and that is all that is being sought is a falsehood. Further, it has been established that the State has no idea what it is looking for on Andrews' cell phones. This also raises the concern for impermissible access to cloud storage through phone applications, which is also unknown to the State, which adds a further degree of violation of Andrews' rights to not have his personal private material violated and subject him to incrimination. The Trial Court made unfounded inferences which do not satisfy reasonable particularity.

Finally, the Court must consider the implication of the Appellate Division's decision as it is only a matter of time in the great State of New Jersey before someone, if not Andrews, is held in contempt for failing to produce a password. What the Appellate Division has set in motion is nothing more than a Hobson's choice for targets and defendants, either provide the password and the intricately connected private information that may or may not be incriminating or go to jail. There is also the third scenario that must be acknowledged where a target or defendant simply has forgotten the password and an overzealous prosecution leads to unjustified incarceration for an innocent failure to recall a

password.

As discussed herein, these difficult choices are being made throughout the Country resulting in persons being held in jail for contempt for exercising their constitutional rights. The mere fact that the Appellate Division hinted at this result should sound alarm bells and is chilling for the fair and just application of due process and Constitutional rights in the State of New Jersey.

CONCLUSION

Andrews' privilege against self-incrimination must be honored. For the foregoing reasons, the Appellate Division's opinion should be reversed and the State's Notice of Motion to compel disclosure of Andrews' cell phone passcodes should be denied in its entirety.

Respectfully submitted,  
Sciarrà & Catrambone, LLC

By: Charles J. Sciarrà / By: DME  
Charles J. Sciarrà, Esq.

By: [Signature]  
Deborah Masker Edwards, Esq.

Dated: June 27, 2019