Supreme Court of New Jersey

	:	Docket No. 82,209
STATE OF NEW JERSEY, Plaintiff-Respondent,	:	CRIMINAL ACTION
V.	:	On Leave to Appeal from the Superior Court of New Jersey, Appellate Division.
ROBERT ANDREWS, Defendant-Appellant.	:	
	:	Sat Below: Hon. Joseph L. Yannotti, P.J.A.D.
	:	Hon. Garry S. Rothstadt, J.A.D.
		Hon. Arnold L. Natali, Jr., J.S.C.

Supplemental Brief on behalf of the State of New Jersey

Theodore N. Stephens II
Acting Essex County Prosecutor
Attorney for Plaintiff-Respondent
Veterans Courthouse
Newark, New Jersey 07102
(973) 621-4700
Appellate@njecpo.org

Frank J. Ducoat – No. 000322007
Special Deputy Attorney General/Acting Assistant Prosecutor
Director, Appellate Section
Of Counsel

Caroline C. Galda – No. 271662018
Special Deputy Attorney General/Acting Assistant Prosecutor
Appellate Section
On the Brief

Table of Contents

Table of Authorities

Page(s)

Cases

Statutes

Rules

Other Sources

Table of Record Citations

1T = Motion transcript dated April 21, 2017
2T = Grand Jury transcript dated April 28, 2016
3T = Grand Jury transcript dated May 26, 2016
Da = Appendix to Defendant's Appellate Division's brief
Pa = Appendix to State's Appellate Division brief

Preliminary Statement

In September 2014, Apple Inc. announced that it was introducing a new mobile operating system specifically designed so that Apple would no longer have the ability to extract data from any mobile device, even if presented with a valid search warrant. "Unlike our competitors, Apple cannot bypass your passcode and therefore cannot access this data. So it's not technically feasible for us to respond to government warrants for the extraction of this data[.]" Apple's competitors quickly followed suit.

The following summer, in May of 2015, Quincy Lowery became the subject of an Essex County Sherriff's Office wiretap narcotics investigation. During that investigation, it became clear that the defendant, an Essex County Sheriff's Officer, was leaking information to Lowery about the investigation to help him avoid detection. Based on corroborating testimony from Lowery, it was determined that the defendant conspired with him through text messages, phone calls, and in-person meetings.

Police seized and obtained search warrants for two of defendant's phones, an iPhone 6 Plus and an iPhone 5. The phones were running versions of Apple's newest operating system, and thus could not be accessed without the defendant's passcode. The phones have remained in evidence since this time, inaccessible.

After defendant was indicted for official misconduct, the State sought an order compelling the defendant to disclose his iPhone passcodes. The trial court issued the order, finding that the "foregone conclusion" exception to the Fifth Amendment allowed disclosure of the passcode. The Appellate Division reached the same conclusion as the trial court.

This Court should also allow access to the devices through the disclosure of defendant's passcode. The passcode itself is merely a random sequence of numbers with no testimonial significance. Its testimonial value is so insignificant that it will not even be revealed to the State during the search of the devices. Moreover, any potentially incriminating inferences that may or may not be implied by the defendant's ability to unlock the phone are "foregone conclusions" because the State knows the phones are defendant's and that he knows the passcode. In unlocking the devices, the defendant does not reveal anything about any evidence stored on them. As such, neither the Fifth Amendment privilege against self-incrimination nor any of its New Jersey counterparts are implicated by this order.

Accordingly, this Court must affirm the lower courts' decisions and allow the State to execute its valid search warrant.

COUNTER-STATEMENT OF PROCEDURAL HISTORY

An Essex County Grand Jury in Indictment No. 2016-06-1781 charged defendant with two counts of second-degree official misconduct, N.J.S.A. 2C:30-2, two counts of third-degree hindering apprehension/prosecution, N.J.S.A. 2C:29-3(a)(2), and two counts of fourth-degree obstruction of the administration of law, N.J.S.A. 2C:29-1. (Pa 1 to 7).

On January 25, 2017, the State filed a Notice of Motion for an Order Compelling Defendant to Disclose his iPhone PINs/Passwords. (Pa 8). The Honorable Arthur J. Batista, J.S.C., heard oral argument on April 21, 2017. (1T).

On May 22, 2017, Judge Batista granted the State's motion in a detailed and well-reasoned written decision. (Da 8 to 27).

On June 8, 2017, defendant filed a Notice of Motion for Leave to File an Interlocutory Appeal. (Da 2 to 3). The Appellate Division denied defendant's Motion for Leave to Appeal, (Da 4), but this Court granted defendant's motion for leave to appeal, and summarily remanded the matter to the Appellate Division to consider on the merits. (Da 1).

The Appellate Division heard oral argument on the matter on October 16, 2018. The Appellate Division affirmed the trial court's order in a November 15, 2018 published opinion, allowing disclosure of the defendant's iPhone passcodes. 457 N.J. Super. 14.

Defendant filed a Motion for Leave to Appeal the Appellate Division's decision to the Supreme Court. This Court granted the motion on May 3, 2019. (Da125).

COUNTER-STATEMENT OF FACTS

Quincy Lowery's Statements

On June 30, 2015, Lowery was arrested as part of a larger narcotics investigation involving many parties during Operation Targeted Integrated Deployment Enforcement ("TIDE"). Following his arrest, Lowery voluntarily gave a statement to detectives from the Essex County Prosecutor's Office's ("ECPO") Professional Standards Bureau. At the outset of the interview, Lowery confirmed that he understood that he was being questioned by Detective John Mulligan and Lieutenant Daniel Francis because they dealt with police corruption. When asked for the names of the officers who were assisting him with his drug dealing enterprise, Lowery indicated that he only knew one individual who he referred to as "BOLO," a police acronym for "Be On The Lookout." Thereafter, Lowery provided a description of "BOLO" and identified him as defendant from a photograph identification. (Da 32 to 34; Da 36).

The duo's friendship began through their shared membership in "Extremely Dangerous," a motorcycle club. They were both

members of the club[1] and knew each other for approximately one year as of the date of Lowery's statement. Lowery detailed the close relationship that he shared with defendant. First, he explained that the vehicle he drove, a Jeep Cherokee, actually belonged to defendant. Lowery would also drive a motorcycle that defendant owned. (Da 33; Da 35).

After establishing the duo's close friendship, Lowery went on to discuss defendant's precarious financial situation and his willingness to help Lowery. Lowery stated that defendant had a "situation with child support" in which "they levied his account." Lowery went on to detail how defendant agreed to register the Jeep in his name, even though defendant knew that Lowery was a drug dealer. Lowery indicated that he gave defendant approximately $200 to register the vehicle and told him to keep any extra money. Defendant also registered Lowery's motorcycle in his name and paid the registration and insurance out of his own pocket.[2] (Da 38 to 40).

Lowery explained defendant's assistance in his drug enterprise. Although Lowery never saw defendant deal drugs, he heard him talk about doing it. Defendant would talk about wanting to deal drugs because he was "getting killed on child

[1] Defendant was president of the club and Lowery's cousin was the original founder. (Da 36 to 37).
[2] This is confirmed by Motor Vehicle Commission records.

support." Lowery claimed that he never gave defendant drugs to sell, but did not know whether anyone else might have given defendant "work." Defendant ended up moving in with his girlfriend at the time because he could not pay his rent. (Da 40 to 41).

According to Lowery, defendant's major assistance came from his willingness to share sensitive police information as opposed to actually selling drugs himself. Prior to his arrest on June 30, 2015, Lowery suspected that he was being followed by the ECPO when an individual outside his residence told him that he believed someone was surveilling Lowery. Lowery got into his vehicle, and as he drove away, he noticed that the other vehicle appeared to be following him. Based on his observations, he asked defendant to "run the license plate for him."[3] Defendant advised Lowery that the vehicle belonged to either the Sheriff's Department or the ECPO. (Da 41 to 42).

Lowery continued to detail defendant's efforts to help him and his fellow narcotics associates "get rid" of their cellular phones due to a wiretap. Approximately one month prior to June 30, 2015, Lowery stated that defendant called him and advised that a wiretap was in place. As a result, defendant recommended

[3] Lowery texted the license plate number to defendant on June 20, 2015. This license plate was, in fact, a vehicle being used by the ECPO as part of Operation TIDE. (Pa 10 to 12).

that Lowery get rid of his phones. (Da 42). Defendant told Lowery that he knew of the wiretap because a fellow officer was called to work on the wiretap. Based upon this information, Lowery got rid of all of his phones and told all of his narcotics associates to do the same.[4] (Da 57).

Lowery explained that he "stopped hustling" at the time as a direct result of defendant's information leak. (Da 56). Lowery indicated that defendant told him that he was a Crip gang member of the "Grapes" subsect. (Da 59). Lastly, Lowery stated that defendant knew that his driver's license was suspended and that he had recently been released from prison when he registered the vehicles for him. (Da 38 to 39). Lowery cooperated with law enforcement and consented to a complete and thorough electronic cellular phone search. (2T 64-25 to 74-3; Da 83 to 84).

On July 2, 2015, at approximately 1:20 p.m., Lowery was interviewed again while in custody at the Essex County Correctional Facility. During this interview, Lowery confirmed

---

[4] This is corroborated by the following two text messages sent by Lowery:

1. 05/24/2015 (10:53 a.m.): Quincy Lowery sent a SMS Message (Short Message Service/Text) to telephone number 973-444-3342 advising the unknown subscriber to "Go get new phones."
2. 05/24/2015 (11:00 a.m.): Quincy Lowery sent a SMS Message to telephone number 973-954-1680 stating to the unknown subscriber, "Everyone around u need to get new ones 2." (Da 83 to 84).

all of the facts from his prior interview, while also providing additional details. Lowery explained that defendant told him to put his Cherokee on a lift to see if a tracking device had been placed underneath. Lowery further explained that defendant was careful to convey all of his information in person as opposed to over the phone. (Da 69 to 79).

Lowery also recounted an occasion when he believed an officer was following him. He stated that he was at a restaurant on Routes 1 and 9 when he took a photograph of the person who he believed was following him. Lowery then met with defendant and showed him the photograph. Defendant told Lowery that, "[T]he N---a is Prosecutor's Office. He work with Viper Squad." (Da 77).

Significantly, Lowery admitted that he was living with defendant at the time this occurred, right before his arrest. (Da 78).

Grand Jury Testimony

On April 28, 2016, Detective Mulligan testified before the grand jury that defendant was employed as an Essex County Sheriff's Officer during the months of May and June of 2015. (2T 5-7 to 9). He testified that Lowery was the subject of a wiretap narcotics investigation during that same period of time. (2T 5-17 to 20). Although Lowery did not possess a driver's license, he was driving a Cherokee and motorcycle that were

owned by defendant. He also testified about the frequent telephone communications between Lowery and defendant. (2T 7-17 to 20). In particular, Detective Mulligan testified that Lowery's phone was part of the wiretap while defendant was leaking information to him. (2T 8-19 to 22).

The grand jury also heard Detective Mulligan's testimony regarding the GPS tracking unit that was placed on Lowery's vehicle, and defendant's "advice" to him on how to check for such a device and remove it. (2T 8-23 to 25). Detective Mulligan explained to the grand jury how the Sheriff's Department and the ECPO are located in the same building. (2T 11-25 to 12-5). The structure of Operation TIDE was also explained to the grand jury, including the investigation itself and how it led to a "takedown." (2T 12-21 to 13-4).

Finally, Detective Mulligan detailed the following Sheriff's Office Rules and Regulations:

> Section 3:1.15: Members shall neither attempt to interrupt the legal process nor participate in or be involved in any activity, which may interfere with the due process of law.
>
> Section 3:4.3: Members shall not communicate any information, directly or indirectly, verbally or in writing, which may tend to defeat the ends of justice.
>
> Section 8:2.1: Members are responsible for their own actions or omissions. Ignorance of the law, department rules, regulations, policies, procedures or orders will not be acceptable as an excuse or justification for an act or omission in violation of same.

> Section 8:2.3: Members shall observe and obey federal and state laws, county and municipal ordinance[s] and the rules, regulation[s], policies, procedures and the orders of the Sheriff's Office.
>
> Section 8:2.5: Members shall not withhold knowledge of a crime, but shall communicate the information to their command.
>
> [(2T 15-7 to 16-21).]

On May 26, 2016, Lowery testified before the grand jury. Lowery testified consistently with his sworn statements. He also confirmed that he was not threatened in any manner to give the statements, and that they were and still are truthful. Lowery testified that he had been friends with defendant for approximately a year as of June 2015. (3T 5-1 to 6-19). At first, Lowery was afraid to trust defendant because he was a law enforcement officer, but they eventually became friends anyway. (3T 7-2 to 6). They were also members of the same motorcycle club. (3T 6-15 to 17).

At one point, Lowery explained that he needed to buy a vehicle, but his license was suspended. Despite knowing this, defendant agreed to register the vehicle under his name so that Lowery could drive it. Defendant also registered a motorcycle under his name for Lowery. Lowery testified that defendant knew that he was dealing drugs. Although Lowery never saw defendant deal drugs, he heard him talk about wanting to do so. Lowery

explained that defendant would complain about how child support was killing him and he needed money. (3T 7-7 to 8-10).

Lowery detailed for the grand jury how defendant helped him with his narcotics enterprise. First, he told the grand jury how defendant tipped him off that a vehicle that was following him was either a Sheriff's Office or ECPO vehicle. Next, Lowery told the grand jury that defendant called him to advise that the ECPO was doing a wiretap and that he and his co-conspirators should get rid of their phones. Lowery testified that defendant told him that various law enforcement agencies were planning to do a "run" or arrest individuals as part of the wiretap investigation. Based upon this information, Lowery told his narcotics associates to get rid of their phones. As a precaution, Lowery also stopped dealing drugs at the time. (3T 8-11 to 10-22).

During this same time period, defendant told Lowery to check his vehicle for a GPS tracking device and to remove it. (3T 10-23 to 11-1). Lowery testified that it was during this time he thought he was being followed by an undercover officer. (3T 11-10 to 12). After taking a photograph of this person, he showed it to defendant, who confirmed that the individual was an undercover detective from the ECPO. (3T 12-2 to 9). That undercover detective was Hervey Cherilien.

Detective Hervey Cherilien's Statement

On July 17, 2015, Detective Cherilien of the ECPO's Narcotics Task Force was interviewed at the ECPO's Professional Standards Bureau Office. Detective Cherilien stated that he had no personal relationship with defendant, but recalled that they had seen each other several times within the courthouse complex. Detective Cherilien was aware that defendant had been involved in an off-duty shooting incident at some point, and recalled acknowledging him once in a courthouse elevator several months after that incident. Detective Cherilien believed that defendant was able to identify him as being assigned to the Narcotics Task Force because it is the only unit within the ECPO that "dresses down" in anything other than business attire. (Da 89).

Myeesha Harris's Statement

On July 17, 2015, Corrections Officer Myeesha Harris, mother of defendant's children, was interviewed. Harris confirmed her relationship with defendant and the fact that they have two children together. She stated that defendant usually stays with her and their children at her apartment. She confirmed defendant's relationship with Lowery, who she knew as "Qua." Harris identified a known photograph of Lowery, and further confirmed that "Qua" had stayed with her and defendant at her apartment for at least one night in June 2015. (Da 89).

Sheriff's Officer Richard Brown's Statement

On July 20, 2015, Essex County Sheriff's Officer Richard Brown was interviewed at the ECPO Professional Standards Bureau. Officer Brown stated that he knew defendant for approximately three years, and recalled that they worked together on patrol duty on two occasions. Officer Brown stated that they did not get along. When they worked patrol together, defendant had stopped for several hours at his motorcycle club while on duty, and associated with numerous "street jokers." (Da 89).

Officer Brown was the only sheriff's officer assigned to the ECPO Narcotics Task Force, joining the force approximately two months before Operation TIDE began. Officer Brown stated that members of the Essex County Sheriff's Office Detective Bureau and Bureau of Narcotics had all been briefed to avoid operations in the area of South 19th Street, so as not to interfere with the ECPO investigation and wire operations. (Da 89 to 90).

Leon Graves's Statement

On August 3, 2015, the ECPO interviewed Leon Graves regarding Grave's purchase of Lowery's silver 2002 Jeep Cherokee. Graves, Lowery, and defendant were all members of the "Extremely Dangerous Motorcycle Club." Graves stated that on June 24, 2015, he had purchased the Jeep directly from Lowery for $1,500. He indicated that the Jeep needed a lot of work and

he parked it in his yard, where he was making repairs before he registered it. (Da 91).

Lowery was the person who gave Graves the title and key to the Jeep. When Graves noticed that the title was in defendant's name, he attempted to contact defendant several times. When defendant returned his call, he stated words to the effect that he did not want to discuss the matter. Graves stated that the police eventually towed his Jeep on July 3, 2015, and they still possessed it. (Da 91).

Edward Brailsford's Statement

On July 15, 2015, Edward Brailsford was interviewed. Brailsford stated that at Latisha Neal's request, he placed an advertisement on Craigslist to sell her 2002 Jeep Cherokee. In response to the advertisement, he was contacted by an individual and the sale was made at Brailsford's garage located at 54 Chancellor Avenue. He stated that the Jeep was sold for $2,800 cash, but he was paid $2,700. Brailsford removed the license plates and instructed the purchaser to go to the DMV to change the title. (Da 88 to 89).

Brailsford described the purchaser as a black male over 35 years old, very heavy set, with a beard and very short hair. The purchaser was accompanied by two other males, one of whom never left the back seat of his vehicle. The driver of the vehicle was described as a black male, very tall, with an

athletic build and dark skin. This individual drove a late model black Dodge Charger, just like defendant did at the time. (Da 88 to 89).

On July 24, 2015, Brailsford viewed two photo arrays and identified both Lowery and defendant. (Da 90).

Defendant's Locked iPhones

Data extractions from Lowery's cellular phone contained a wealth of information, corroborative of his sworn statements and grand jury testimony. (2T 64-25 to 74-23; Da 77; Da 83 to 84;). While Lowery's data extraction was successfully completed, the same could not be said for defendant's.

During the pertinent time period, defendant owned two cellular phones. The first was a black iPhone 6 Plus, phone number 732-318-7376, IMSI[5] 310260227466755. This number was associated with the name "BOLO" in Lowery's phone. The second was a cracked black iPhone 5s, phone number 973-342-9755, IMSI 310120106396676. (Pa 18 to 19).

On June 30, 2015, defendant's phones were seized from his possession. On July 7, 2015, search warrants were obtained for both phones. (Pa 18 to 29). Since the iPhones had operating

[5] The International Mobile Subscriber Identity ("IMSI") is a unique number embedded in the SIM card of each phone to identify a subscriber. See IMSI ("International Mobile Subscriber Identity", http://www.tech-faq.com/imsi.html) (last visited Aug. 28, 2019).

systems greater than iOS 8.1, it was "extremely difficult" to access the locked phones without the owner's PINs/passwords.[6] The ECPO sought assistance from other agencies in unlocking the phones. Both the Jersey City Police Department and the Federal Bureau of Investigation ("FBI") were unable to unlock the phones due to Apple's proprietary method of encryption. The phones have remained in evidence since that time. (Da 88).

However, based upon the contents of Lowery's cellular phone, as well as the phone records obtained from Sprint and T-Mobile, it is uncontroverted that defendant used his phones to

[6] In Riley v. California, the United States Supreme Court held that police conducing searches incident to arrest generally could not search an arrestee's cellular phone absent a warrant authorizing them to do so. 573 U.S. 373 (2014). In September 2014, less than five months after Riley, Apple announced a new company policy that made it impossible for the company to turn over data from most iPhones and iPads to law enforcement, even with a valid search warrant. Any operating system after iOS 8 has an encryption that prevents the company and anyone but the device's owner from gaining access to the stored user data. The new privacy policy for iOS 8 and beyond no longer allows Apple to maintain the ability to unlock some content on the devices for legally binding police requests, as it allowed in the past. Apple still retains the ability and legal responsibility to turn over user data stored elsewhere, such as the iCloud. See Craig Timberg, Apple Will No Longer Unlock Most iPhones, iPads for Police, Even with Search Warrants, The Washington Post, September 18 2014, https://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html?utm_term=.c765069524e2(last visited Aug. 29, 2019); see also Apple.com Privacy page, September 19, 2014, https://web.archive.org/web/20140919170856/http://www.apple.com/privacy/governemnt-information-requests/ (last viewed Aug. 29, 2019).

communicate with Lowery. The text messages showed that the duo communicated casually via text message, and certain things were left for in-person meetings. For example, on June 22, 2015, defendant texted Lowery that they needed to meet and talk in person. This text message was only two days after Lowery sent a text message with the license plate number of the vehicle that he believed was surveilling him. (Pa 10 to 12).

Two specific text messages are particularly corroborative of Lowery's sworn statements and grand jury testimony. The first is regarding the photograph Lowery stated he took of the undercover officer at the restaurant on Routes 1 and 9. During his testimony, Lowery indicated that he texted the picture to his other phone and showed it to defendant in person. Lowery's phone contains the referenced text message, and the attached picture is certainly of the undercover detective. (3T 11-10 to 12; 3T 12-2 to 9; Pa 11 to 12).

The second text message of note relates to defendant's knowledge that Lowery's driver's license was suspended. On June 5, 2015, defendant sent a text message to Lowery, which contained a picture of a flier advertising how to restore a suspended license. (Pa 10).

In addition to text messages and in-person meetings, there were also approximately 187 phone conversations between Lowery

and defendant during the month prior to Lowery's arrest. (Pa 13 to 17).

Legal Argument

POINT I[7]

To extend the privilege against self-incrimination to include production of a passcode would be "an extravagant extension of the Fifth Amendment" because the content of the passcode does not have testimonial significance.

The Fifth Amendment to the United States Constitution provides that "[n]o person...shall be compelled to be a witness against himself[.]" U.S. Const. Amend. V. "The word 'witness' in the constitutional text limits the relevant category of compelled incriminating communications to those that are 'testimonial' in character." United States v. Hubbell, 530 U.S. 27, 34 (2000). "[I]n order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a "witness" against himself." Doe v. United States, 487 U.S. 201, 210 (1988). The Fifth Amendment privilege is not limited to verbal and written communications, but also includes the production of documents when the act of

[7] This argument addresses Point II.A of Defendant's Brief. The State does not contest Defendant's Point I: that Leave to Appeal the Interlocutory Order of the Appellate Division has been granted.

production itself could communicate incriminatory statements of fact.[8] Fisher v. United States, 425 U.S. 391, 410 (1976).

Ultimately, "the constitutional foundation underlying the privilege. . .demands that the government seeking to punish an individual produce the evidence against him by its own independent labors, rather than by the cruel, simple expedient of compelling it from his own mouth." Miranda v. Arizona, 384 U.S. 436, 461 (1966). However, "the privilege has never been given the full scope which the values it helps to protect suggest." Schmerber v. California, 384 U.S. 757, 762 (1966).

The limits of the Fifth Amendment privilege against self-incrimination were first established in Holt v. United States, 218 U.S. 245, 252 (1910). Therein, a suspect was compelled to try on a blouse that had been worn by a then-unidentified murderer. Holt, 218 U.S. at 252. The blouse fit, and the suspect was later convicted of murder. Ibid. He appealed, arguing that being forced to try on the blouse violated his right against self-incrimination because he tried it on "under the same duress that made his statement inadmissible." Ibid.

The Supreme Court disagreed and found this to be "an extravagant extension of the 5th Amendment." Ibid. In no

[8] See Point II for an explanation of the "act of production" doctrine as applicable to the circumstances presented in this case.

uncertain terms, the Court declared that "the prohibition on compelling a man in a criminal court to be witness against himself is a prohibition of the physical or moral compulsion to extort communications from him[.]" Id. at 252-53.

In keeping with this foundation, the privilege against self-incrimination "does not prevent a defendant from being compelled to provide blood and fingerprints, [or] to stand in a lineup," even though these acts are both compelled and incriminating. United States v. Harris, 660 F.3d 47, 52 (1st Cir. 2011) (citing Hubbell, 530 U.S. at 35; United States v. Wade, 388 U.S. 218, 221–23(1967)). "The distinction which has emerged, often expressed in different ways, is that the privilege is a bar against compelling 'communications' or 'testimony,' but that compulsion which makes a suspect or accused the source of 'real or physical evidence' does not violate it." Schmerber, 384 U.S. at 764. "These decisions are grounded on the proposition that 'the privilege protects an accused only from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature.'" Doe, 487 U.S. at 210 (quoting Schmerber, 384 U.S. at 761).

However, "it is not enough that the compelled communication is sought for its content[,] [t]he content itself must have testimonial significance." Doe, 487 U.S. at 208-09 n.6 (1988)

(emphasis added). Ultimately, "if a compelled statement is 'not testimonial and for that reason not protected by the privilege, it cannot become so because it will lead to incriminating evidence." Ibid. (quoting In re Grand Jury Subpoena, 826 F.2d 1166, 1171 n.2 (2d Cir. 1987) (Newman, J., concurring)).

For this reason, compulsion of handwriting samples does not violate the privilege, despite handwriting being communicative in nature. Gilbert v. California, 388 U.S. 263, 266 (1967). "[O]ne's voice and handwriting are, of course, means of communication. It by no means follows, however, that every compulsion of an accused to use his voice or write compels a communication within the cover of the privilege." Ibid. The Gilbert Court held that the distinction lay in whether law enforcement sought the factual content of the handwriting, such as a confession, which cannot be compelled, or sought the handwriting itself as evidence. Ibid. Even though by producing the sample the accused "implicitly 'acknowledged' that the writing...was his...this kind of simple acknowledgment—that the suspect in fact performed the compelled act—is not 'sufficiently testimonial for purposes of the privilege.'" Doe, 487 U.S. at 217 n. 15 (quoting Fisher, 425 U.S. at 411).

As technology advanced, courts extended this reasoning to exclude compulsion of blood and DNA samples from Fifth Amendment protection, despite their incriminating and sometimes physically

invasive nature. See Maryland v. King, 569 U.S. 435, 456 (2013); Schmerber, 384 U.S. at 761. The Schmerber Court acknowledged that "[t]he withdrawal of blood necessarily involves puncturing the skin for extraction, and the percent by weight of alcohol in that blood...is evidence of criminal guilt." Id. at 762. Additionally, since the test enables the State to rely on evidence forced from the accused, the compulsion violates at least one meaning of the requirement that the State procure the evidence against an accused "by its own independent labors." Schmerber, 384 U.S. at 762. However, the Court held that "[n]ot even a shadow of testimonial compulsion upon or enforced communication by the accused was involved either in the extraction or in the chemical analysis [because] Petitioner's testimonial capacities were in no way implicated[.]" Id. at 765.

The compelled disclosure of a passcode is not testimonial in the same way that Holt being compelled to try on the blouse, Schmerber being compelled to provide a blood sample, and Gilbert being compelled to provide a handwriting sample were not. In 1910, Holt trying on the shirt was not testimonial merely because the blouse ended up fitting, and the fact that he complied "under the same duress that [would] ma[k]e his statement inadmissible" did not render the action testimonial for Fifth Amendment purposes. In 1966, Schmerber enduring a

needle through his skin lacked "even a shadow of testimonial compulsion." In 1967, Gilbert being forced to provide a handwriting sample did not implicate the Fifth Amendment merely because the sample was communicative in nature, and the "simple acknowledgment—that the suspect in fact performed the compelled act—is not 'sufficiently testimonial for purposes of the privilege.'" Doe, 487 U.S. at 217, n. 15 (quoting Fisher, 425 U.S. at 411).

And in 2019, for the same reasons, the defendant's passcode has no testimonial significance. The content of the passcode is so testimonially insignificant that it will not even be revealed to the State. Instead, the passcode will be revealed in chambers, and the search of the phone will be performed without the State ever learning the passcode. As such, the fact that defendant is being compelled to unlock his device "under the same duress that [would] ma[k]e his statement inadmissible" and the "simple acknowledgment—that the suspect in fact performed the compelled act" do not render the unlocking of the device testimonial for Fifth Amendment purposes. Holt, 218 U.S. at 252; Doe, 487 U.S. at 217, n. 15. Excluding the disclosure of a device's passcode from protection under the privilege against self-incrimination is the next logical step in the application of the Fifth Amendment to evolving technology, and to conclude

otherwise would be "an extravagant extension of the 5th Amendment." Holt, 218 U.S. at 252.

Courts have extended the Holt, Schmerber, and Gilbert body of case law described above to conclude that compelling the use of biometrics to unlock a device is not protected by the privilege against self-incrimination. See, e.g., In re Search of [Redacted], 317 F. Supp. 3d 523 (D.D.C. 2018); State v. Diamond, 905 N.W.2d 870 (Minn. 2018); Commonwealth v. Baust, 89 Va. Cir. 267 (2014). The cases that have contravened this general rule all involve a common theme: the device was recovered during a search of a shared living space and the identity of the phone's owner was unknown. Courts have held that under these uncertain circumstances it would be overbroad to allow law enforcement to test the biometrics of everyone present during the search to unlock the phone. See, e.g., I.M.O. the Search of A White Google Pixel 3XL Cellphone, ___ F. Supp. 3d __, 2019 WL 34019990 (D. Idaho 2019); I.M.O. the Search of a Residence in Oakland, California, 354 F.Supp.3d 1010 (N.D. Cal. January 10, 2019). The State agrees with this principle, and emphasizes that this conclusion is the result of Fourth Amendment protections, not Fifth Amendment privileges. These courts all concluded that the search warrants allowing police to test anyone's biometrics – without reasonable suspicion that the individual was linked to the phone - were unreasonable.

Defendant's passcode has no more testimonial significance than a biometric lock. "If the societal interests in privacy, fairness, and restraint of governmental power" allow "the accused to have his body serve as evidence that leads to the development of highly incriminating testimony, as Schmerber and its progeny make clear," then "it is difficult to understand how compelling a suspect to make a nonfactual statement that facilitates the production of evidence by someone else offends the privilege." Doe, 487 U.S. at 213, n. 11. The unique sequence of numbers comprising defendant's passcode has no more factual meaning than the unique arches, loops, and whorls of defendant's fingerprint. In providing the passcode, the defendant would not be admitting that the phone contains evidence of official misconduct, in the same way that a defendant who provides a fingerprint to unlock the phone would not be admitting to its contents. Id. at 215.

Moreover, the State has a warrant to search the phone and it has already been identified as the source of relevant evidence, so entering the passcode does not "betray any knowledge [defendant] may have about the circumstances of the offenses" with which he is charged. Id. at 219. As such, defendant's passcode should not be subject to any greater protection than defendant's biometrics would be. Neither is testimonial.

However, despite there being no difference in testimonial significance between a random sequence of numbers and a biometric feature, the courts that have confronted this issue have maintained a distinction between the two under the Fifth Amendment. This distinction relies on a single sentence in the dissenting opinion in Doe v. United States, a 1988 case. Therein, Justice Stevens stated that a defendant could "in some cases be forced to surrender a key to a strongbox containing incriminating documents, but...he can [not] be compelled to reveal the combination to his wall safe – by word or deed." Doe, 487 U.S. at 219 (Stevens, J., dissenting). Justice Stevens reasoned that to force a defendant to do so would impermissibly compel him "to use his mind to assist the prosecution in convicting him of a crime." Ibid. Defendant relies on this same sentiment here to support his argument that he is protected from revealing the passcode to his phone because to do so would require him to "use his mind."

Although this quote appears in many cases, not a single one actually involves a defendant being forced to surrender a key. See State v. Stahl, 206 So.3d 124, 134-35 (Fla. Dist. Ct. App. 2016) ("Despite the many cases referencing the quote, we have found none that provide details of 'surrender[ing] a key.'"). Moreover, compelling a defendant to turn over a physical key would require him to "use the contents of his mind," in much the

same way that turning over a passcode would; he would have to recall where the key is kept and then retrieve it. Accordingly, distinguishing the testimonial significance of turning over a key from that of turning over a passcode based on the thought processes involved leads to a distinction with no real difference.

The absurdities of this distinction went unconsidered for nearly three decades because a literal application of the principle was never tested. Until recently, a court never needed to compel the production of either a key or a combination to a locked container, because law enforcement always had a way of bypassing the lock "by its own independent labors." This is no longer the reality facing the courts and law enforcement. This container cannot be physically broken into; nor can it be accessed by entering all possible passcodes until it unlocks. Such "'brute force' attempts may result in the contents of the device becoming permanently inaccessible once the maximum number of passcode attempts is reached."[9] There are no independent labors that can access these containers, as evidenced by the converse problem these containers have created for law

[9] See Report of The Manhattan District Attorney's Office On Smartphone Encryption and Public Safety, (Nov. 2015), at 4, https://www.manhattanda.org/wp-content/themes/dany/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf. (last accessed August 28, 2019).

enforcement: phones belonging to homicide victims remain in storage, inaccessible and useless.[10] Ultimately, this Court should join the Stahl court in "question[ing] the continuing viability of any distinction as technology advances." 206 So.3d at 135.

Moreover, drawing a distinction between these two methods is not only irrational in 2019, but also creates an impenetrable safe harbor for criminals who happen to lock their device with a random sequence of numbers instead of their fingerprint or facial features. The Fifth Amendment was never intended to completely shield suspects from law enforcement's reach and for this reason has "never been given the full scope which the values it helps to protect suggest." Schmerber, 384 U.S. at 762. As such, this Court should disregard the Doe dissent, and apply the Schmerber lineage of cases to passcodes, rectifying the absurd distinction between a lock using a unique sequence of numbers and a lock using a suspect's unique biometric features.

[10] See Aarti Shahani, Mom Asks: Who Will Unlock My Murdered Daughter's iPhone, National Public Radio, March 30, 2016, https://www.npr.org/sections/alltechconsidered/2016/03/30/472302719/mom-asks-who-will-unlock-her-murdered-daughters-iphone (last accessed Aug. 29, 2019).

POINT II

Providing the passcode to a device is not a testimonial act of production.

The Fifth Amendment privilege against self-incrimination is not only limited to verbal and written communications, but also includes the production of documents when the act of production itself could communicate incriminatory statements of fact. Fisher, 425 U.S. at 410. The traditional example of a testimonial act of production is when a witness "produc[es] documents in compliance with a subpoena, the witness would admit that the papers existed, were in his possession or control, and were authentic." Hubbell, 530 U.S. at 36. Some states have found that decrypting or unlocking a device is equivalent to the production of documents because unlocking or decrypting the device communicates that a defendant has possession and control over the device. However, this "rheotoric is overstated." See In re Search of [Redacted], 317 F.Supp.3d at 533 (holding "to the extent that the [defense] is concerned...that using an individual's fingerprint to unlock a device leads 'necessarily' to the conclusion that the individual possesses or controls the device, its rhetoric is overstated. Digital devices can be set up so that more than one individual's fingerprints will unlock them.").

The defendant's knowledge of the device's passcode does not translate into proof of ownership. The disclosure of the passcode is more similar to the consent directive in Doe,[11] a non-testimonial statement allowing production of evidence by someone else; than it is to the subpoena in Fisher[12] and Hubbell,[13] which mandated that those defendants sort through documents in their possession and produce any that they believed to be incriminating. The defendant has "non-inculpatory explanations" for being able to access the device such as, "although I have access to it, that device...[or] its contents are not mine." Ibid. The defendant could know the passcode because the phone belongs to a significant other or close friend. Or alternatively, the defendant may have shared his passcode with others who used his phone to contact Lowery. Ultimately, the State still must prove independently not only that the defendant had possession and control over the device, but that he had possession and control over the device at the time any incriminating texts were sent from the phone.

Therefore, the defendant's ability to unlock the device is not a testimonial act of production. His mere knowledge of the passcode is not an "incriminatory statement[] of fact," because

[11] 487 U.S. at 215.
[12] 425 U.S. at 36.
[13] 530 U.S. at 36-38.

admitting he has the ability to access the phone is not an admission of his possession or control of any evidence on the phone, nor an admission of the authenticity of said evidence. Accordingly, the Fifth Amendment privilege does not attach to this disclosure.

POINT III

Even if the Court finds the passcode is testimonial, the State can still compel its disclosure under the foregone conclusion exception to the Fifth Amendment.

As the question of how to handle devices that are inaccessible without a passcode looms over every state, most courts have applied the "foregone conclusion" exception to the Fifth Amendment, or a variation thereof, in confronting the problem. The "foregone conclusion" principle is an exception to the act of production doctrine. The principle exempts an otherwise testimonial act of production from Fifth Amendment protection if the government meets certain conditions. As explained above, an act of production is testimonial when "'the act of production' itself...implicitly communicate[s] 'statements of fact.'" Hubbell, 530 U.S. at 36.

For an act of production to be a foregone conclusion, the State must show with reasonable particularity: (1) knowledge of the existence of the evidence demanded; (2) defendant's possession and control of that evidence, and; (3) the authenticity of that evidence. Id. at 30, 40-41; Fisher, 425

U.S. at 410-13. If all three elements of this test are met, then a defendant's act of production "adds little or nothing to the sum total of the Government's information" and is a "foregone conclusion." Id. at 411. Ultimately, if the compelled act of production is a foregone conclusion, then "'no constitutional rights are touched. The question is not of testimony but of surrender.'" Ibid. (quoting In re Harris, 221 U.S. 274, 279 (1911)).

Importantly, courts have taken two divergent approaches to applying the "foregone conclusion" doctrine to orders compelling a defendant to decrypt or unlock a device.[14] Some courts have required the government to demonstrate that the contents of the device are known ahead of time, while others have asked the government to demonstrate that the existence of the passcode, and user's knowledge of it, are known facts.[15]

While the State could meet the required showing under either method here, the first approach is incorrect, as several courts have recognized. See, e.g., United States v. Apple MacPro Computer, 851 F.3d 238, 248 n. 7 (3d Cir. 2017)

---

[14] Updated Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety, Nov. 2018, https://www.manhattanda.org/wp-content/uploads/2018/11/2018-Report-of-the-Manhattan-District-Attorney27s-Office-on-Smartphone-En....pdf (last accessed Aug. 28, 2019).

[15] See State v. Stahl, 206 So.3d at 135-37; Commonwealth v. Gelfgatt, 11 N.E.3d 605, 613-17 (Mass. 2014).

(explaining that the court was not agreeing that the government's knowledge of the content of the devices was the correct focus of the foregone conclusion rule, rather the plain error rule limited the court's analysis to reviewing this conclusion for abuses of discretion, and "a very strong argument can be made that the foregone conclusion doctrine properly focuses on whether the government already knows...[that defendant knows] the password for these devices."); Stahl, 206 So. 3d at 136; Commonwealth v. Jones, 117 N.E. 3d 700 (Mass. 2019).

Here, the "evidence demanded" by the government in the relevant court order is the passcode. The first approach to the "foregone conclusion" exception analysis would be correct if the State were using its subpoena power to require the defendant to compile and then turn over his incriminating texts and call history to the government himself. Instead, the State is seeking access to the device to carry out a valid search warrant. Any challenge to the government's knowledge about the device's contents concerns the validity of the search warrant, and is thus properly raised under the Fourth Amendment, not the Fifth. Stahl, 206 So. 3d at 136. As such, the second approach, which focuses on the existence of the passcode and defendant's knowledge of it, is the correct analysis.

Accordingly, the application of the foregone conclusion exception in this case turns on whether the State has knowledge that (1) a passcode exists; (2) that the defendant is in possession and control of the passcode; and (3) that the passcode is authentic. Each of these is a factual determination, and reviewed for an abuse of discretion by higher courts. State v. Harris, 181 N.J. 391, 416 (2004) ("Typically, '[w]e give deference to the trial court's factual findings ... 'when supported by adequate, substantial and credible evidence.'") (quoting Rova Farms Resort, Inc. v. Investors Ins. Co. of Am., 65 N.J. 474, 484 (1974)).

Turning to the State's knowledge that a passcode exists; courts have concluded that if the device cannot be accessed without a passcode then the government has knowledge that one exists. Stahl, 206 So.3d at 136. Possession and control of the passcode can be shown through cellphone carrier records that identify a suspect as the owner of that phone number, in addition to the phone being recovered from a defendant's possession. Ibid. When it comes to the authenticity of the passcode, "we must recognize that the technology is self-authenticating...if the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic." Ibid.

Here, the State has met all three prongs, as the trial court properly found. The State cannot access the device without defendant's passcode. The State has evidence from the cellphone carrier that the phone belongs to the defendant, and the phones were recovered from the defendant's possession. As described in Stahl, the passcode is "self-authenticating" and its authenticity will be confirmed once it is entered into the device. As such, the defendant's act of producing the passcode "adds little or nothing to the sum total of the Government's information" and is a "foregone conclusion." Fisher, 425 U.S. at 411. Therefore, in turning over the passcode, "no constitutional rights are touched. The question is not of testimony but of surrender." Ibid. at 411 (quoting In re Harris, 221 U.S. at 279).

POINT IV[16]

Allowing access to the defendant's cell phone through his passcode does not violate either the New Jersey common law, or the statutory or evidentiary privilege against self-incrimination.

"New Jersey's privilege against self-incrimination, although not enshrined in the State Constitution, is deeply rooted in this State's common law and codified in both statute and an evidence rule." State v. Muhammad, 182 N.J. 551, 567 (2005). "The privilege reflects 'our respect for the

[16] This Point addresses defendant's Point II.B.

inviolability of the human personality and of the right of each individual to a private enclave where he may lead a private life.'" In re Grand Jury Proceedings of Guarino, 104 N.J. 218, 231 (1986) (quoting Murphy v. Waterfront Comm'n of N.Y. Harbor, 378 U.S. 52, 55 (1964)). "To determine whether the evidence sought by the government lies within that sphere of personal privacy a court must look to the 'nature of the evidence.'" Guarino, 104 N.J. at 232-33. The nature of the evidence must be such that it is "an extension of the more intimate aspects of one's life." Id. at 233.

Defendant's cellphone does not fall within this special "sphere of personal privacy," since the warrant is limited to searching his text messages and call log for contact with his co-conspirator. "Diaries and personal letters that record only their author's personal thoughts lie at the heart of our sense of privacy. In contrast, [there is] no bar in the Fourth or Fifth Amendments to the seizure of a letter from one conspirator to another directing the recipient to take steps that further the conspiracy." Id. at 233 (quoting Couch v. United States, 409 U.S. 322, 350 (1973) (Marshall, J., dissenting)). The fact that defendant may have other, more private evidence, stored on his cell phone is not relevant to the analysis here because the

State is not seeking that evidence.[17] Instead, the State is seeking communications between the defendant and his co-conspirator. Ultimately, "[i]n today's highly computerized, commercialized and regulated world, there is little expectation of privacy for such records that touch so little on the intimate aspects of one's personal life." Id. at 234. As such, the state common law privilege does not protect the defendant's text messages and calls with his co-conspirator from being disclosed to the State.

Additionally, neither is the evidence protected by the state statutory or evidentiary privileges. The statute and evidence rule both provide, in identical language, that "every natural person has a right to refuse to disclose in an action or to a police officer or other official any matter that will incriminate him or expose him to a penalty," unless one of four exceptions applies. N.J.S.A. 2A:84A-19; N.J.R.E. 503. The exceptions are as follows:

(a) no person has the privilege to refuse to submit to examination for the purpose of discovering or recording his corporal features and other identifying characteristics or his physical or mental condition;

(b) no person has the privilege to refuse to obey an order made by a court to produce for use as evidence or

[17] Defendant's argument that access to his cell phone invades this "sphere of privacy" because he has private information stored on his phone concerns the scope of the search warrant and is more properly addressed under the Fourth Amendment, which defendant has not raised and is not before this Court.

otherwise a document, chattel or other thing under his control if some other person or a corporation or other association has a superior right to the possession of the thing ordered to be produced;

(c) no person has a privilege to refuse to disclose any matter which the statutes or regulations governing his office, activity, occupation, profession or calling, or governing the corporation or association of which he is an officer, agent or employee, require him to record or report or disclose except to the extent that such statutes or regulations provide that the matter to be recorded, reported or disclosed shall be privileged or confidential;

(d) subject to the same limitations on evidence affecting credibility as apply to any other witness, the accused in a criminal action or a party in a civil action who voluntarily testifies in the action upon the merits does not have the privilege to refuse to disclose in that action, any matter relevant to any issue therein.

As the Appellate Division found, exception (b) applies to the circumstances in this case. The New Jersey statutory and evidentiary privileges developed from the Boyd[18] body of case law, which recognized a privacy interest in a defendant's personal papers, prior to Fisher narrowing this interest in 1976. Boyd found that a valid search warrant gave the government a "superior proprietary interest" in the documents or other property it sought as evidence. Fisher, 425 U.S. at 406 (citing Boyd, 116 U.S. at 623-24) ("[T]he Government may not, consistent with the Fourth Amendment, seize a person's documents or other property as evidence unless it can claim a proprietary

[18] Boyd v. United States, 116 U.S. 616 (1886).

interest in the property superior to that of the person from whom the property is obtained.").

Although Boyd's holding that the Fourth Amendment applied to subpoenas duces tecum in the same manner that it applies to search warrants is no longer good law after Fisher, Fisher did not affect the holding that a valid search warrant confers a superior proprietary interest on the government to evidence it seeks under the search warrant.

As such, this Court should affirm the Appellate Division's holding that the defendant is not shielded from providing access to his text messages and call log with his co-conspirator because the search warrant, which defendant is not contesting the validity of, confers a superior proprietary interest in the evidence that allows its disclosure under state evidentiary and statutory law.

POINT V

Alternatively, if the Court does find that the defendant's passcode is subject to greater protection under state law than is available under the Fifth Amendment, the Court can increase the showing the State must make under the "foregone conclusion" exception to comport with this more stringent protection. And if it does, the burden is met in this case.

Federally, the Government is required to make the showing under the foregone conclusion exception with "reasonable particularity." Hubbell, 167 F.3d at 579. Some courts have accepted the "reasonable particularity" standard in cases

involving locked devices, including the Third Circuit. Apple MacPro Computer, 851 F.3d 238, 247 (2017). Our Appellate Division adopted the federal standard in this case. State v. Andrews, 457 N.J. Super. 14, 22-23 (App. Div. 2018). However, some states have chosen to escalate the standard the government must meet beyond the federal standard. For example, the Northern District of California has articulated a "clear and convincing evidence" standard. United States v. Spencer, U.S. Dist. Ct., No. 17-cr-00259-CRB-1, 2018 WL 1964588 (N.D. Ca. Apr. 26, 2018).

Massachusetts has taken the protection even further and requires the government to prove defendant's knowledge of the passcode beyond a reasonable doubt. Jones, 117 N.E.3d at 713. However, Massachusetts adopted this standard because their state analogue to the Fifth Amendment differs in its wording from its Constitutional counterpart. Id. at 713-14. While the Fifth Amendment protects a person from being compelled to be a witness against himself, Massachusetts state law is far broader and protects a citizen from being compelled to "furnish evidence" against himself. Ibid. (quoting Mass. Const. pt. 1, art. XII.). This wording is a critical difference from New Jersey jurisprudence, which derives from the common law and concerns evidence of an extremely private nature.

Accordingly, the same could be done here if this Court decides that New Jersey's common law, statutory, and evidentiary privileges afford greater protection to defendant's passcode than the Fifth Amendment. This Court can follow in the lead of other states and increase the showing the government must make under the "foregone conclusion" doctrine to comport with this increased protection. Regardless of the burden, the State has proven all prongs of the "foregone conclusion" doctrine in this case, and so the Appellate Division's judgment must be affirmed.

Conclusion

This Court should affirm the Appellate Division's judgment, compelling defendant to provide his iPhone passcode so that the devices can be searched subject to a valid search warrant, as doing so does not violate the defendant's Fifth Amendment privilege against self-incrimination.

Respectfully submitted,

THEODORE N. STEPHENS II
ACTING ESSEX COUNTY PROSECUTOR
ATTORNEY FOR PLAINTIFF-RESPONDENT

Frank J. Ducoat – No. 000322007
Special Deputy Attorney General/
Acting Assistant Prosecutor
Director, Appellate Section
Of Counsel

Caroline C. Galda
No. 271662018
Special Deputy Attorney General/
Acting Assistant Prosecutor
Appellate Section
On the Brief

Filed: August 30, 2019