Supreme Court of New Jersey

DOCKET NO. 082209

STATE OF NEW JERSEY,	:	Criminal Action
Plaintiff-Respondent,	:	On Leave to Appeal Granted from an Interlocutory Order of the
v.	:	Superior Court of New Jersey, Appellate Division.
ROBERT ANDREWS,	:	
		Sat Below:
Defendant-Appellant.	:	Hon. Joseph L. Yanotti, P.J.A.D., Hon. Garry S. Rothstadt, J.A.D., Hon. Arnold L. Natali, Jr., J.A.D.

BRIEF AND APPENDIX ON BEHALF OF
THE ATTORNEY GENERAL OF NEW JERSEY
AMICUS CURIAE

GURBIR S. GREWAL
ATTORNEY GENERAL OF NEW JERSEY
AMICUS CURIAE
RICHARD J. HUGHES JUSTICE COMPLEX
TRENTON, NEW JERSEY 08625

LILA B. LEONARD - ATTY NO. 110242014
DEPUTY ATTORNEY GENERAL
DIVISION OF CRIMINAL JUSTICE
APPELLATE BUREAU
P.O. BOX 086
TRENTON, NEW JERSEY 08625
(609) 376-2400
leonardl@njdcj.org

OF COUNSEL AND ON THE BRIEF

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

RULES

CONSTITUTIONAL PROVISIONS

TABLE OF CITATIONS

AGa – Attorney General's appendix
Db – Defendant's brief in support of motion
1T - Transcript of Grand Jury Hearing, dated April 28, 2016
2T – Transcript of Grand Jury Hearing, dated May 26, 2016
3T - Transcript of Motion, dated April 21, 2017

TABLE TO APPENDIX

PRELIMINARY STATEMENT

In this matter of first impression, this Court is asked to determine the correct focus of the foregone-conclusion doctrine in the realm of compelled decryption. In other words, this Court is asked to determine under what circumstances the State can compel a defendant to enter passcodes into computer devices that have been lawfully seized and are the subject of valid search warrants. A review of caselaw from the few jurisdictions that have addressed this issue reveals that the correct question is not whether the State can show with reasonable particularity the specific evidence it seeks, but whether the defendant knows the passcodes to the devices.

There is a palpable difference between asking someone to hand over documents and asking him to enter a passcode into a passcode-protected or encrypted computer device storing those documents. Encryption is nothing more than a way to disguise or hide computer files. Decryption is thus akin to simply lifting the disguise. The State does not seek to compel defendant to put his text messages or call logs — the evidence that the State ultimately seeks — into the hands of the police; it instead merely asks this Court to allow the State to compel defendant to unlock the phones using his passcodes. In doing so, the State will finally be able to execute the search warrant dated July 7, 2015, and lawfully search the relevant applications of defendant's phones.

The State obtained the warrant after learning that

defendant, a sheriff's officer, used his position to help a friend thwart an investigation into a narcotics-trafficking operation. After alerting the friend that the State was employing a wiretap for the investigation, defendant also advised the friend to reset his phone. Doing so cleared all of the phone's data, and now defendant refuses to enter his passcodes into his own phones to allow the police to execute the search warrant.

The foregone-conclusion doctrine focuses on the act the State seeks to compel, which in this case is the act of entering passcodes into defendant's phones. Here, the Appellate Division correctly analyzed the foregone-conclusion doctrine and rightly held that the State's valid search warrants give the State a superior right to possession of the passcodes, because the State has evidence showing that defendant knows the passcodes to the phones and used the phones to engage in criminal activity before surrendering them.

The devices in question are iPhones. Such phones are equipped with technology that allows a user to unlock them with a fingerprint or facial-recognition software. And it is well established that such biometrics are not testimonial. It would thus lead to inconsistent results if defendants could be compelled to unlock devices using biometrics but not with passcodes. Whether a person unlocks a phone with a fingerprint, facial recognition, or a passcode, the result is the same. Regardless of the method, the user has unlocked the phone.

Defendants cannot be allowed to use the Fifth Amendment as a weapon against what is authorized under the Fourth Amendment.

The Attorney General thus asks this Court to follow the rule recently adopted by the Appellate Division and the most recent rulings of our sister states: defendant should be compelled to enter his passcode where, as here, the State can show it is a "foregone conclusion" that defendant knows the passcodes to his devices.

STATEMENT OF PROCEDURAL HISTORY AND FACTS

The Attorney General relies on the procedural history and facts as set forth in the Appellate Division opinion.

LEGAL ARGUMENT

POINT I

DEFENDANTS CANNOT BE PERMITTED TO DEFEAT THE EXECUTION OF SEARCH WARRANTS SIMPLY BY PASSCODE-PROTECTING COMPUTER DEVICES.

Defendants should not be allowed to stand in the way of the execution of a valid search warrant simply by putting a passcode between the police and the evidence they are lawfully authorized to seize and search. The Third Circuit and a handful of our sister states have recently addressed the issue of compelled decryption of computer devices. The growing consensus is that defendants must either tell police their passcodes or decrypt their devices themselves if the State can show that the defendant knows the passcodes; they cannot claim Fifth Amendment protections as a way to hide evidence to which the State is legally entitled.

Here, defendant was an officer with the Essex County Sheriff's Office (ECSO) who had been leaking information to Quincy Lowery, the target of a narcotics-trafficking investigation. (AGa2). After the police arrested Lowery on June 30, 2015, he told the police that defendant had helped him conceal his drug-trafficking activities. (AGa3). Defendant warned Lowery that police had obtained a wiretap order for his phone, and suggested that Lowery look to see if a GPS tracker had been put on his Jeep. (AGa3).

Upon arrest, Lowery consented to a search of his phone.

(AGa4). He told investigators defendant had usually offered his help in person or by using the FaceTime video chat application, and that their text messages were limited to arranging meetings. (AGa4).

The night of Lowery's arrest, the ECSO Internal Affairs Department asked defendant to surrender his two iPhones. (AGa4). Defendant surrendered the phones, but refused to consent to a search of them. (AGa4). The ECSO held the phones pending a search-warrant application, which the Honorable Ronald D. Wigler, P.J. Crim., granted on July 7, 2015. (AGa25 to 46).

In January 2017, the State filed a motion to compel defendant to disclose the passcodes to unlock his phones. (AGa5). In support of the motion, the State submitted call records for Lowery's phone, which showed that defendant and Lowery had exchanged 187 phone calls during the month before Lowery's arrest. (AGa5). Lowery's phone records also revealed a series of text messages with defendant. (AGa5).

But on defendant's advice, Lowery had reset his phone about a month before his arrest, so the police were unable to access any prior messages. (AGa5). The only way to obtain the text messages and information about the length of the phone calls between Lowery and defendant was thus for defendant to unlock his phones. (AGa5). The trial judge granted the State's motion to compel the passcodes, and the Appellate Division correctly affirmed that order because it was a foregone conclusion that defendant knew the passcodes. See (AGa6 to 7, 24).

A. Defendant must turn over his passcodes because they exist, are in his possession or control, and are authentic.

The Fifth Amendment states, "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." U.S. Const. amend. V. This privilege is not included in the New Jersey Constitution, but it has been incorporated into our common law and rules of evidence. State v. Hartley, 103 N.J. 252, 260 (1986); see N.J.R.E. 501-503. This privilege "protects a person only against being incriminated by his own compelled testimonial communications." Doe v. United States, 487 U.S. 201, 207 (1988) (quoting Fisher v. United States, 425 U.S. 391, 401 (1976)).

"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). To be testimonial, "an accused's communication must itself, explicitly or implicitly, relate to a factual assertion or disclose information," such as an admission that the revealed evidence indeed exists, is in the accused's possession or control, and is authentic. Doe, 487 U.S. at 209-10. But when "the existence, custody, and authenticity of evidence" "adds little or nothing to the sum total of the [State]'s information,'" the information provided is a "foregone conclusion." Apple MacPro Comput., 851 F.3d 238, 247 (3d Cir. 2017) (quoting Fisher, 425 U.S. at 411).

The Fifth Amendment does not "independently proscribe the

compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a testimonial communication that is incriminating." Commonwealth v. Gelfgatt, 11 N.E.3d 605, 612 (Mass. 2014) (emphasis added) (citing Fisher, 425 U.S. at 408). In other words, the Fifth Amendment protects against "compelled self-incrimination, not the disclosure of private information." Fisher, 425 U.S. at 401. Indeed, the United States Supreme Court has determined that allowing the Fifth Amendment to serve as a "general protector of privacy" would "completely loose [it] from the moorings of its language," because "privacy" is not mentioned in the Fifth Amendment. Ibid. Privacy is instead "addressed in the Fourth Amendment." Ibid.

New Jersey's "common law privilege against self-incrimination protects the individual's right '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, 378 U.S. 52, 55 (1964)). Under certain circumstances, it "affords greater protection to an individual than that accorded under the federal privilege." State v. A.G.D., 178 N.J. 56, 67 (2003) (citation omitted). Our courts determine if evidence falls within that sphere of personal privacy by examining the "nature of the evidence." Guarino, 104 N.J. at 231-32 (quoting Couch v. United States, 409 U.S. 322, 350 (1973) (Marshall, J., dissenting)). For documents, this Court has held that courts must look to the document's contents,

rather than reviewing the testimonial compulsion involved in its production, to determine whether evidence "lies within [a] sphere of personal privacy." Id. at 232.

But documents are different from passcodes. The Appellate Division thus correctly declined to hold "greater protections against self-incrimination than those provided by the Fifth Amendment" in the context of compelled decryption. (AGa22). And the factors set forth in Justice Handler's concurring opinion in State v. Hunt support this decision. See 91 N.J. 338, 364-67 (1982) (Handler, J., concurring). Indeed, Justice Handler's concurrence stands as the standard for Constitutional divergence in New Jersey. See, e.g., State v. Muhammad, 145 N.J. 23, 41 (1996) (applying Hunt criteria to victim rights under New Jersey Constitution).

As set forth by Justice Handler, the following seven factors should be considered when determining whether our State Constitution should diverge from cognate provisions in the Federal Constitution: (1) textual language; (2) legislative history; (3) pre-existing state law; (4) structural differences between the federal and state Constitutions; (5) matters of particular state interest or local concern; (6) state traditions; and (7) public attitudes. Ibid.

Explaining the need for specific criteria, Justice Handler saw "a danger . . . in state courts turning uncritically to their state constitutions for convenient solutions to problems not readily or obviously found elsewhere." Hunt, 91 N.J. at 361

(Handler, J., concurring). "Moreover, while a natural monolithic system is not contemplated, some consistency and uniformity between the state and federal governments in certain areas of judicial administration is desirable." Id. at 362-63. After detailing the meaning of each factor, Justice Handler stated: "The explication of standards such as these demonstrates that the discovery of unique individual rights in a state constitution does not spring from pure intuition but, rather, from a process that is reasonable and reasoned." Id. at 367.

Application of the Hunt factors reveals no basis to diverge from the Fifth Amendment and provide greater protections in the context of compelled decryption. The right against self-incrimination comes from the common law and the Rules of Evidence, not the text of the state Constitution. And as the Appellate Division correctly recognized, the Rules of Evidence and our statute prohibit a defendant from refusing to obey court orders. See (AGa22); N.J.S.A. 2A:84A-19; N.J.R.E. 503. In identical language, the statute and evidence rule provide 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. Ibid. One of those exceptions provides:

> (b) no person has the privilege to refuse to obey an order made by a court to produce for

> use as evidence or 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[.]
>
> [N.J.S.A. 2A:84A-19(b); N.J.R.E. 503(b).]

In other words, defendant cannot defeat the search warrant by refusing to enter his passcodes, as expressly stated in the exceptions to our statutory right against self-incrimination.

The last three policy-based Hunt factors all weigh against diverging as well. In this case, defendant is a law enforcement officer who used his position of power to help a criminal conceal his drug-trafficking activities. And more generally, this issue is relevant to all computer-crime investigations, such as child-pornography cases. It would be devastating to law enforcement and the public at large if avoiding prosecution for crimes such as manufacturing child pornography were as easy as passcode-protecting a computer. Certainly, public attitudes in New Jersey favor a stricter reading of the right against self-incrimination under the particular circumstances presented here, i.e., a corrupt law enforcement official. Thus, in applying the foregone-conclusion doctrine to the issue of compelled decryption here, the Appellate Division correctly declined to extend "greater protections against self-incrimination than those provided by the Fifth Amendment" under these circumstances. See (AGa22).

Cases such as Fisher and Hubbell also illustrate that the

Appellate Division correctly applied the foregone-conclusion analysis here. In Fisher, the Internal Revenue Service summoned two defendants to produce documents related to their taxes. 425 U.S. at 394-95. Both defendants declined, asserting Fifth Amendment privilege. Ibid. While the Supreme Court was concerned that the act of producing the papers admitted to the existence of the papers, the Court ultimately found that, because the papers had been prepared by accountants, "[t]he existence and location of the papers [we]re a foregone conclusion" such that the taxpayer could "add[] little or nothing to the sum total of the Government's information by conceding that he in fact ha[d] the papers." Id. at 411. Thus, the question was "not of testimony but of surrender," and "no constitutional rights [we]re touched." Ibid. (quoting In re Harris, 221 U.S. 274, 279 (1911).

Likewise, in Hubbell, the defendant was compelled to produce physical, subpoenaed documents, and in doing so, admitted to the very existence of those documents. 530 U.S. at 43. The Government had granted derivative use immunity to Hubbell, and the Supreme Court determined it was "abundantly clear" that the act of producing the subpoenaed documents led to his indictment. Ibid. The Court also found that Hubbell had "ma[d]e extensive use of 'the contents of his own mind' in identifying the hundreds of documents responsive to the requests in the subpoena." Id. at 43. The Court ultimately concluded that the constitutional privilege against self-incrimination

protected Hubbell, the target of a grand jury investigation, "from being compelled to answer questions designed to elicit information about the existence of sources of potentially incriminating evidence." Ibid. In other words, because the Government sought specific documents in a subpoena, the Government was precluded from using those documents against the defendant when he ultimately produced them.

This Court has previously required a defendant to produce evidence sought by the State, despite the defendant's assertion of his right against self-incrimination. In Guarino, a grand jury issued a subpoena duces tecum, directing Guarino to produce contracts for the sale of real estate, a cash-receipts journal, and payment coupons. 104 N.J. at 221. When Guarino refused to produce the documents, asserting his Fifth Amendment privilege, this Court looked to the nature of the documents sought by the State to determine whether they were protected by the privilege against self-incrimination. Id. at 231-32. Because the documents were business records, and not personal records, this Court held that they were not privileged. Id. at 228-29, 235.

As the Appellate Division correctly held here, the act of disclosing the passcodes would not convey any implicit factual assertions about the existence or authenticity of data from the devices. (AGa9). The fact that defendant knows his passcodes adds "little or nothing to the sum total of the [State's] information." (AGa10) (quoting Fisher, 425 U.S. at 411). The panel acknowledged that by producing the passcodes, defendant

would be "making an implicit statement of fact that the iPhone passcodes [we]re within his 'possession or control.'" (AGa10) (citing Doe, 487 U.S. at 209). Nevertheless, the panel held that "these testimonial aspects of the passcodes [we]re a 'foregone conclusion'" because the State had established, and defendant had not disputed, that he "exercised possession, custody, or control over these devices." (AGa10) (citing Fisher, 425 U.S. at 411). And one can easily draw a rational inference that a person knows the passcode to his or her own phone.

Requiring defendant to provide his passcodes is a matter of surrender, not testimony. See Fisher, 425 U.S. at 410. Defendant must enter his passcode into his phones, which the State seized and is authorized to search under a valid search warrant. He does not have to tell anyone his passcode – he can enter it directly without ever uttering it. Defendant's act of producing his passcodes does not admit the presence of text messages or information about phone calls with Lowery. Nor does it admit that defendant himself sent or read the text messages or engaged in the phone calls. It merely admits that defendant has the ability to unlock his phone. And the State has already agreed not to use evidence that defendant entered his passcodes against him in its case-in-chief. Thus, defendant's right against self-incrimination remains intact.

The panel also found that the State described with "reasonable particularity" the specific evidence it sought to

compel, "which is the passcodes to the phones." (AGa10). Thus, the panel properly focused on the passcodes, not the State's knowledge of the content on the phones, in its foregone-conclusion analysis. (AGa10). And while defendant had argued that the State was unaware of "all of the possible contents" of the phones, the panel correctly found that this was "immaterial because the order requires defendant to disclose the passcodes, not the contents of the phones unlocked by those passcodes." (AGa10) (citing Fisher, 425 U.S. at 409). This makes plain sense, as the act compelled of the defendant is the act of entering his passcodes; he is not asked to show the investigators the text messages between him and the target, nor is he asked to show them his recent calls in his call log.

Cases such as Apple MacPro Computer highlight the tangible difference between compelling specific documents and merely unlocking a device where those documents may or may not be stored. See 851 F.3d at 248 n.7. The Third Circuit noted that the correct focus of the foregone-conclusion doctrine in the context of compelled decryption is whether the defendant knows the passcode, not whether the State knows the contents of the devices. Ibid.

The court was constrained to a plain-error analysis there, but explained, "a very sound argument can be made that the 'foregone conclusion' doctrine properly focuses on whether the Government already knows the testimony that is implicit in the act of production." Ibid. Thus, "the fact known to the

Government that is implicit in the act of providing the password for the devices is 'I, John Doe know the password for these devices.'" Ibid. But, since the District Court had not committed plain error in finding that the Government established that it knew the contents of the encrypted hard drives, the court did not decide "that the inquiry c[ould] be limited to the question of whether Doe's knowledge of the password itself [wa]s sufficient to support application of the foregone conclusion doctrine." Ibid.

Similarly, in State v. Stahl, the District Court of Appeal of Florida, Second District, emphasized that the information sought by the State, was "the passcode to Stahl's iPhone," and not the content of the phone itself. 206 So.3d 124, 133 (Fla. Dist. Ct. App. 2016). The court pointed out that the State had a warrant to search the device, based on probable cause that it had been used in the commission of video voyeurism. Ibid. The court specifically noted that "the State ha[d] not asked Stahl to produce the photographs or videos on the phone." Ibid. The court found that, "[b]y providing the passcode, Stahl would not be acknowledging that the phone contains evidence of video voyeurism." Id. at 134 (citing Doe, 487 U.S. at 215). The court explained further that, because the phone had been seized under the authority of a search warrant, "the source of evidence had already been uncovered." Ibid. Thus, providing the passcode would not "'betray any knowledge [Stahl] may have [had] about the circumstances of the offenses' for which he [wa]s

charged." Ibid. (citing Doe, 487 U.S. at 201, 215).

In conducting its foregone-conclusion analysis, the Stahl court explained, "the relevant question is whether the State has established that it knows with reasonable particularity that the passcode exists, is within the accused's possession or control, and is authentic." Id. at 136. The court determined that "the question is not the State's knowledge of the contents of the phone; the State has not requested the contents of the phone or the photos or videos" stored on the phone. Stahl, 206 So.3d at 136.

Likewise, the Superior Court of Pennsylvania recently determined that the act of producing a password is not testimonial. Commonwealth v. Davis, 176 A.3d 869, 876 (Pa. Super. Ct. 2017), appeal granted, 195 A.3d 557 (Pa. 2018). The court rejected Davis's argument that compelled disclosure of his passcode was "tantamount to his testifying to the existence and location of potentially incriminating computer files." Id. at 875. The court instead emphasized that the Commonwealth had shown it "kn[ew] with reasonable particularity that the passcode exist[ed], [wa]s within the accused's possession or control, and [wa]s authentic." Ibid. (emphasis omitted) (quoting Stahl, 206 So.3d at 136). The computer seized from Davis's residence was encrypted with TrueCrypt software, and thus required a sixty-four-character passcode to bypass. Id. at 876. Davis had admitted he was the sole user of the computer and that he knew the passcode, but refused to turn it over. Ibid. Finally, the

court found that "technology is self-authenticating." Ibid. (quoting Stahl, 206 So.3d at 136). "Namely, if [the] encrypted computer is accessible once its password has been entered, it is clearly authentic." Ibid. The court thus concluded that Davis's act of providing the passcode "was not testimonial in nature and his Fifth Amendment right against self-incrimination would not be violated." Ibid. (emphasis added).[1]

Here, the State is not asking defendant to print the documents and images from his computer devices, forward them in an email, or direct investigators to information stored on his phones. He simply must enter his passcodes so that the police can finally execute the court-ordered search warrant dated July 7, 2015.

The State can show that defendant knows his passcodes, because he owned, possessed, and used the phones, so his knowledge of the passcodes would not be tantamount to admitting he knew the content stored on them. People often know the passcodes to their spouse's, children's, or even friends' phones or computers. Simply because one can access devices belonging to other people does not mean they have any idea what is stored on them, or what has been searched using the devices. In

[1] The court also recognized there was a "high probability that child pornography exist[ed] on said computer," given that it was used to share child pornography on a peer-to-peer network. Davis, 176 A.3d at 876. But the legal analysis focused on whether Davis knew the passcode to the computer, not on its content.

unlocking his phones, defendant will admit only that he knows the passcodes. That is all. That is why the proper focus of the foregone-conclusion doctrine is whether defendant knows his passcodes, not whether the State can show that the particular evidence it seeks exists on a particular device.

This Court should thus affirm the Appellate Division's opinion, and order that defendant must either unlock his phones or give his passcodes to the police.

B. The State has shown with reasonable particularity that evidence of defendant's interference with a narcotics-trafficking investigation exists on his iPhones.

As set forth above, the correct focus of the foregone-conclusion doctrine is whether the State can show that defendant knows his passcodes. That is the standard generally adopted by the courts that have recently considered this issue. But in the alternative, defendant should be compelled to unlock his phones because the State has also established he used his phones to communicate with Lowery, the target of a narcotics-trafficking investigation, and that he tipped off Lowery to the investigation using those phones. Although Lowery had recently deleted the data from his phone, data from Lowery's phone and phone records revealed a month's worth of text messages and phone calls between defendant and Lowery. Thus, the State has established with reasonable particularity the data it seeks to recover.

The early cases on the foregone-conclusion doctrine in the

realm of compelled decryption focused on whether the State could show with "reasonable particularity" that the evidence could be found the particular computer device. See United States v. Doe, 670 F.3d 1335, 1346-47 (11th Cir. 2012) (concluding that "[n]othing in the record" revealed "whether any files exist and are located on the hard drives" where the Government requested production of the contents of the hard drives, not passcodes). But see United States v. Fricosu, 841 F. Supp. 2d 1232 (D. Colo. 2012) (holding Fifth Amendment not implicated where there was little question Government knew of files' existence and location, and Government proved suspect had ownership or access; Government's lack of knowledge of "the specific content of any specific documents [was] not a barrier to production").

In Gelfgatt, the Supreme Judicial Court of Massachusetts likewise followed the reasoning of Fisher, which dealt with physical documents rather than passcodes. Gelfgatt, 11 N.E.3d at 614. Gelfgatt had used his computer to illegally divert funds to himself that were intended to pay off large mortgage loans. Id. at 609. Digital forensic examiners found file names on his computer that implicated him in the crime, and Gelfgatt admitted, "'[e]verything is encrypted and no one is going to get to it.'" Ibid.

The court found that Gelfgatt had already incriminated himself through that statement, and that law enforcement knew he had been using his computers to engage in the real-estate activity in question. Id. at 615-16. Thus, the court found

that the facts that would be conveyed by Gelfgatt through his act of decryption, namely "his ownership and control of the computers and their contents, knowledge of the fact of encryption, and knowledge of the encryption key," were "already known to the government, and thus, [we]re a 'foregone conclusion.'" Id. at 615.

Constrained to a plain-error analysis in Apple MacPro Computer, the Third Circuit upheld a magistrate judge's order compelling decryption of encrypted devices because forensic examiners found child pornography on defendant's decrypted computer, as well as data indicating that defendant had downloaded thousands of files of child pornography. 851 F.3d at 243. But as shown in subpoint a. above, the court noted that this was the incorrect focus of the doctrine. And the more recent cases have diverged from this focus of the analysis, and have shifted toward whether a defendant knows the passcodes that the State seeks.

Here, even if this Court focuses on the State's knowledge of the contents of defendant's call logs and text messages, defendant must be compelled to unlock his phones. It is a foregone conclusion that the phones contain evidence that defendant communicated with Lowery to thwart a narcotics-trafficking investigation and that defendant owned, possessed, and controlled the phones before the State seized them. The State knows that defendant spoke with Lowery on the phone 187 times in the thirty days leading up to Lowery's arrest, and that

they sent several text messages back and forth to each other. (3T6-5 to 7-14). Because Lowery reset his phone on June 20, 2015, the State cannot obtain any further information without searching defendant's phones. See (3T6-4 to 5; AGa5). But the State has shown it is a foregone conclusion that the evidence exists on defendant's phones. Defendant thus must enter his passcodes to allow the State to execute the search warrant it duly obtained nearly four years ago.[2]

C. This case will have lasting implications on all computer-based criminal investigations.

With advancing technologies, the Gelfgatt standard of requiring the State to show with reasonable particularity the specific content it seeks to discover on a computer device will soon become impossible to meet. See 11 N.E. 605. Encryption software is ever advancing, and "can render [a computer drive] completely opaque to law enforcement" without a passcode. David W. Opderbeck, The Skeleton in the Harddrive: Encryption and the

[2] Relatedly, a person who "hinders, obstructs or impedes the effectuation of a judicial order," such as a search warrant, is guilty of fourth-degree contempt. N.J.S.A. 2C:29-9(a); see, e.g., State v. Hemenway, 454 N.J. Super. 303, 329 (App. Div.), certif. granted, 236 N.J. 42 (2018) (finding that "defendant's failure to comply with the police officers' direct instruction to allow them entry into his residence to execute a facially valid TRO and search warrant gave the officers probable cause to arrest defendant" for contempt). Likewise, if defendant continues to defy the search warrant by refusing to enter his passcodes, he risks being adjudged in contempt of court and getting "committed to the county jail until such time as he purges himself of contempt" by providing or entering the passcodes. See In re Addonizio, 53 N.J. 107, 114 (1968); N.J.S.A. 2A:81-17.3.

Fifth Amendment, 70 Fla. L. Rev. 883, 886 (2018). Thus, "[d]espite the sophistication of law enforcement, . . . forensic laboratories cannot crack robust disk encryption." Ibid.

The outcome of this case will implicate thousands of cases where the State seeks passcodes to cellphones as well as computer devices, and will thus have a substantial impact on all computer-crime investigations, such as child-pornography cases. For example, if the State learns that a person has offered to share child pornography over the internet, the State can obtain a search warrant to seize and search that suspect's computer and computer storage devices. In such a situation, the State may be able to show that the suspect offered to share child-pornography files on a file-sharing network, and may easily obtain a search warrant to search the suspect's computers to investigate the scope of the evidence. But without compelled decryption, a search warrant for an encrypted device is utterly useless.

A purveyor of child pornography cannot be allowed to escape prosecution simply because he is technologically savvy. Like the defendant in Davis, a defendant could easily install encryption software such as TrueCrypt, and protect his evidence with a sixty-four-character passcode. If this were the law, and a defendant were permitted to defeat a warrant simply by making his files unreadable or invisible without a passcode, child-pornography prosecutions will grind to a halt.

By way of comparison, a person could shoot and kill someone, and then put the gun in a passcode-protected safe. If

the State secured a search warrant, or articulated an applicable exception to the warrant requirement, the defendant would not be permitted to obstruct the State from retrieving the weapon by asserting his privilege against self-incrimination. A defendant cannot build a fortress around evidence of his crimes and prevent the State from executing valid searches. See State v. Rockford, 213 N.J. 424, 447 (2013) (permitting use of flash-bang devices during search-warrant executions of homes). Cf. State v. Fanelle, 385 N.J. Super. 518, 523-24, 527 (App. Div. 2006) (upholding no-knock warrant where physical layout of property, with tall fence and 100-foot driveway divided by passcode-protected gate, made safe entry impossible).

But executing a search warrant on an encrypted computer or phone presents additional issues that are unique to computer devices. While the police can physically drill into a safe to obtain the evidence to which it is entitled, drilling into a computer would obviously destroy the evidence. And decryption software — the metaphorical drill police can use to crack into a computer device — is effectively useless against robust encryption software.

Notably, iPhones made in the last few years are equipped with technology that allows users to unlock the phones using fingerprints and facial-recognition software. It is well established that such biometrics are not testimonial because "the person is not required to vouch for the truth or falsity of anything." State v. Cary, 49 N.J. 343, 348 (1967). It would

thus lead to inconsistent results if defendants could be compelled to unlock devices using biometrics but not with passcodes. Whether a person unlocks a phone with a fingerprint, facial recognition, or a passcode, the user has unlocked the phone. Defendants should not be allowed to weaponize the Fifth Amendment against what is permitted under the Fourth Amendment.

Finally, not only will the outcome of this case affect hypothetical future cases, it will also have a direct effect on this case, and the other members of the narcotics-trafficking ring arrested along with Lowery. Indeed, it is quite possible that the communications between defendant and Lowery contain exculpatory evidence related to the other defendants, and would thus be discoverable to them. See generally R. 3:13-3; Giglio v. United States, 405 U.S. 150 (1972); Brady v. Maryland, 373 U.S. 83 (1963). In cases such as these, co-defendants have as significant an interest in obtaining potentially exculpatory information as the State has in obtaining potentially incriminating information.

In short, there is no question that defendant owned and controlled the two iPhones. Thus, defendant providing the passcode or inputting the passcode to unlock the phones will not cause him any additional prejudice. The State has shown it is a foregone conclusion that he knows the passcodes to his phones, and that he used the phones to communicate with Lowery in an effort to undercut a narcotics-trafficking investigation.

CONCLUSION

For the foregoing reasons, the Attorney General urges this Court to affirm the Appellate Division's ruling that defendant must decrypt his iPhones under the theory that it is a foregone conclusion that defendant knows the passcodes to the devices.

Respectfully submitted,

GURBIR S. GREWAL
ATTORNEY GENERAL OF NEW JERSEY
AMICUS CURIAE

BY /s/ *Lila B. Leonard*
Lila B. Leonard
Deputy Attorney General
leonardl@njdcj.org

LILA B. LEONARD
DEPUTY ATTORNEY GENERAL
ATTORNEY NO. 110242014
DIVISION OF CRIMINAL JUSTICE
APPELLATE BUREAU

OF COUNSEL AND ON THE BRIEF

DATED: JULY 22, 2019