SUPERIOR COURT OF NEW JERSEY
APPELLATE DIVISION
DOCKET NO. A-4971-17T4

STATE OF NEW JERSEY,

Plaintiff-Respondent/
Cross-Appellant,

v.

ROBERT G. WHITE,

Defendant-Appellant/
Cross-Respondent.

———————————————

Argued April 9, 2019 – Decided June 5, 2019

Before Judges Yannotti and Rothstadt.

On appeal from Superior Court of New Jersey, Law Division, Morris County, Indictment No. 10-17-0636.

Paul E. Zager argued the cause for appellant/cross-respondent (Palumbo, Renaud & De Appolonio, attorneys; Jeff Thakker, of counsel and on the briefs; Anthony N. Palumbo, on the briefs).

Lila B. Leonard, Deputy Attorney General, argued the cause for respondent/cross-appellant (Gurbir S.

Grewal, Attorney General, attorney; Lila B. Leonard, of counsel and on the brief).

PER CURIAM

In March 2017, law enforcement officers executed a search warrant at defendant's residence in Morristown and seized certain computer devices. The court had granted the State's application for the warrant based on information that child pornography was being shared on the internet through devices at defendant's home. The officers could not gain access to two computer hard drives and a computer tower, which were encrypted.

The State thereafter filed a motion to compel defendant to produce the passcodes for, or otherwise decrypt, the devices. Defendant opposed the motion, arguing that the compelled disclosure violated his right against self-incrimination under the Fifth Amendment to the United States Constitution and New Jersey law. He also argued that the State's motion was an improper attempt to obtain discovery and not permitted by the court rules.

The trial court conducted an evidentiary hearing on the State's motion, and thereafter entered an order dated May 25, 2018, which granted the State's motion as to the hard drives, but denied the motion with regard to the computer tower. We thereafter granted defendant's motion for leave to appeal, and the State filed a cross-appeal pursuant to Rule 2:3-4(a). For the reasons stated herein, we

affirm on defendant's appeal, reverse on the State's cross-appeal, and remand the matter to the trial court for further proceedings.

I.

The record discloses the following. In September 2016, the Division of Criminal Justice (DCJ) in the State's Department of Law and Public Safety began investigating individuals who were suspected of sharing images of child pornography on the internet. During the investigation, Detective Laura Hurley discovered an Internet Protocol (IP) address[1] that was offering to share such images with others by utilizing peer-to-peer file sharing networks. Hurley used BitTorrent software and downloaded thirty-eight images of child pornography from the IP address. DCJ's investigators traced the IP address to defendant's home.

In January 2017, detectives from the Bayonne Police Department (BPD) began a separate investigation using similar investigative software to identify an IP address that was being used to share images of child pornography with other users on the internet. The BPD detectives downloaded hundreds of such images

[1] An IP address is an identifying number assigned to an internet subscriber by the subscriber's service provider. State v. Reid, 194 N.J. 386, 389 (2008).

from this IP address, twenty-four of which depicted child pornography. The detectives also traced the IP address to defendant's residence.

The DCJ learned that the BPD was investigating the same IP address and they merged their investigations. The BDP provided Hurley with a disk that contained files the BDP had downloaded from the IP address. On March 10, 2017, the court issued a warrant, which authorized the DCJ to search defendant's home in Morristown and "seize evidence pertaining to" crimes related to the "distribution and possession of child pornography."

The warrant stated that the investigators could search and seize "[a]ny and all computers, computer systems, computer programs, computer software, computer hardware, including central processing units, external storage units, flash drives, . . . hard disk drives/units, . . . documentation, passwords and data security devices . . . ." The warrant also stated that the investigators could "conduct a forensic examination performed by any qualified examiner, whether sworn law enforcement or civilian, on scene and later in a recognized laboratory environment on all items until such examination is complete."

On March 17, 2017, the DCJ executed the warrant and searched defendant's home. Defendant was home at the time and remained downstairs while the investigators searched his home. The DCJ seized a number of devices

from defendant's second-floor office, including a Lenovo P500 laptop, an Asus computer tower, two external hard drives, a universal serial bus (USB) thumb drive, and other peripheral devices.

At the scene, DCJ Detective Kevin Madore attempted to access the contents of the seized devices. The laptop was logged on, so Madore was able to access its contents. To preserve the laptop's data, Madore performed a forensic "preview" of the laptop's files and created reports detailing his preliminary findings. Madore later completed a "Forensic Analysis Report."

In his report, Madore stated that the two external hard drives and the computer tower were encrypted and therefore "could not be read." He found, however, that the laptop's hard drive contained eighty-two images of suspected child pornography. He noted that the laptop was registered to an e-mail address with defendant's name.

Madore also found that the serial number of one of the encrypted external hard drives appeared on the laptop's hard drive, which indicated that the external hard drive had at some point been connected to the laptop. In addition, the laptop contained a link to a "tor browser," which Madore explained is "primarily used to gain access to the dark web" and help maintain the user's anonymity while browsing on the internet. Madore noted that the "tor browser" contained

a "bookmark" to a page titled "The Pedophile's Handbook," which is an internet publication that provides adults suggestions on having sex with minors.

After the search, the DCJ detectives arrested defendant and charged him with second-degree endangering the welfare of a child by distributing child pornography, in violation of N.J.S.A. 2C:24-4(b)(5)(a)(i), and third-degree endangering the welfare of a child by possessing, viewing or controlling child pornography, in violation of N.J.S.A. 2C:24-4(b)(5)(b).

On August 27, 2017, the State filed a motion to compel defendant "to provide the passcodes necessary to decrypt" the two external hard drives and the computer tower. As we noted previously, defendant opposed the motion. The trial court thereafter held an evidentiary hearing on the motion.

At the hearing, the State presented testimony from Hurley and Madore regarding the DCJ's investigation and the execution of the search warrant. Hurley testified that when DCJ conducted the search, she read defendant his Miranda[2] rights and asked defendant for the passcodes to access the encrypted devices. Defendant told Hurley he knew the passcodes for the devices, but he refused to disclose them because "he did not want [the police] looking through his stuff." Madore testified about the information he obtained from the devices,

[2] Miranda v. Arizona, 384 U.S. 436 (1966).

and his inability to gain access to the encrypted external hard drives and tower. The State also presented testimony from Detective Ryan Foley of the Somerset County Prosecutor's Office, who explained various technical terms for the court.

On May 25, 2018, the trial court filed a written opinion in which it concluded that defendant's act of producing the passcodes to decrypt the devices is a testimonial communication for purposes of the Fifth Amendment privilege against self-incrimination. The court noted, however, that the "foregone conclusion" principle is a recognized exception to the Fifth Amendment privilege. Quoting Fisher v. United States, 425 U.S. 391, 411 (1976), the court stated the act of production does not violate the Fifth Amendment privilege against self-incrimination if the facts communicated by the act of production "add[] little or nothing to the sum total of the [g]overnment's information."

The court held that the facts that would be communicated by defendant's act of decryption of the hard drives are a "foregone conclusion" that would not violate the Fifth Amendment privilege against self-incrimination. The court stated that the State had established that it "knows of the existence and location of child pornography files on the hard drives, and knows of defendant's custody, control and access to the devices." The court also found that compelled

production of the passcodes to the hard drives would not violate defendant's privilege against self-incrimination under New Jersey's common law.

The court held, however, that the State had not presented sufficient evidence to satisfy the "foregone conclusion" exception with regard to the computer tower. The court found that the State had not shown that it has "knowledge of the existence and location of child pornography on the tower." The court also found that the State had not shown defendant had exclusive possession or control of the tower, since the forensic examination revealed there were three "user profiles" associated with the tower.

The court memorialized its decision in an order dated May 25, 2018, which granted the State's motion to compel production of the passcodes to the external hard drives, but denied the motion with regard to the computer tower. This appeal and the State's cross-appeal followed.

On appeal, defendant argues:

> [POINT I]
> THE STATE EXECUTED THE WARRANT AND FILED ITS CHARGES, AND [DEFENDANT'S] DISCOVERY OBLIGATIONS AT THAT JUNCTURE (IF ANY) WERE GOVERNED BY THE COURT RULES; THE STATE LACKED LEGAL GROUNDS FOR FILING A MOTION TO COMPEL DISCLOSURE FROM [DEFENDANT].

[POINT II]
THE DETECTIVES' ASSUMPTIONS ABOUT WHAT THE LAPTOP'S VIRTUAL DRIVES[] ONCE CONTAINED (AND THEIR ASSUMPTIONS ABOUT THE ASSOCIATION OF THE TOSHIBA HARD DRIVES WITH THE VIRTUAL DRIVES) DID NOT MAKE THE CONTENT OF THE HARD DRIVES A "FOREGONE CONCLUSION"; THE COMPELLED DISCLOSURE WAS (AND IS) IN VIOLATION OF [DEFENDANT'S] FIFTH AMENDMENT RIGHTS.

[POINT III]
PASSWORD DISCLOSURE SHOULD BE ALSO EXCLUDED IN THE CONTEXT OF NEW JERSEY'S SELF-INCRIMINATION/PRIVACY PRIVILEGE.

In response to defendant's arguments, and in support of its cross-appeal, the State argues:

[POINT I]
BECAUSE DEFENDANT ADMITTED HE KNOWS THE PASSWORDS TO HIS ELECTRONIC DEVICES, THIS COURT SHOULD [AFFIRM THE TRIAL COURT'S ORDER COMPELLING] DEFENDANT TO USE THOSE PASSWORDS TO DECRYPT ALL OF HIS DEVICES.

[POINT II]
IT IS A FOREGONE CONCLUSION THAT DEFENDANT POSSESSES CHILD PORNOGRAPHY ON HIS LAPTOP AND HARD DRIVES.

[POINT III]
THE SEARCH WARRANT, DATED MARCH 10, 2017, AUTHORIZED THE STATE TO SEIZE AND

SEARCH DEFENDANT'S ENCRYPTED HARD DRIVES.

II.

The trial court filed its opinion and order on the State's motion before this court decided State v. Andrews, 457 N.J. Super. 14 (App. Div. 2018), leave to appeal granted, __ N.J. __ (2019). In Andrews, the defendant appealed from an order, which required him to disclose personal identification numbers and passcodes for his iPhones. Id. at 18. The defendant argued that the compelled disclosure of this information violated his right against self-incrimination under the Fifth Amendment, and the protections afforded against self-incrimination under New Jersey law. Ibid.

We rejected the defendant's arguments and affirmed the order requiring disclosure of the passcodes. Id. at 18. In our opinion, we noted that the Fifth Amendment privilege against self-incrimination applies to verbal and written communications as well as to the production of documents because "[t]he act of product[ion]" may communicate incriminating statements. Id. at 22 (alteration in original) (quoting Fisher, 425 U.S. at 410).

We noted, however, that the "foregone conclusion" principle is an exception to the "act of production" doctrine. Ibid. (citing Fisher, 425 U.S. at 411). We stated that the exception applies when the State establishes with

"reasonable particularity" (1) that it has "knowledge of the existence of the evidence demanded"; (2) that defendant has "possession and control of that evidence"; and (3) that the evidence is authentic. Id. at 22-23 (citing United States v. Hubbell, 530 U.S. 27, 30, 40-41 (2000)). We stated that "when an accused implicitly admits the existence and possession of evidence, the accused has 'add[ed] little or nothing to the sum total' of the information the government has, and the information provided is a 'foregone conclusion.'" Id. at 23 (alteration in original) (quoting Fisher, 425 U.S. at 411).

We held that the "foregone conclusion" exception applied to the compelled disclosure of the defendant's passcodes. Id. at 23-24. We determined that the testimonial aspects of the act of producing the passcodes are a "foregone conclusion" because the State had established that the defendant "exercised possession, custody, or control" of the phones, and the fact that defendant knows the passcodes "adds little or nothing to the sum total of the [g]overnment's information." Id. at 24 (quoting Fisher, 425 U.S. at 411).

We stated that the act of disclosing the passcodes did "not convey any implicit factual assertions about the 'existence' or 'authenticity' of the data on the device[s]." Id. at 23. We also stated that the State had described with "reasonable particularity" the evidence it was seeking, "which is the passcodes

to the phones." Id. at 24. We observed that the defendant had argued that the State had not shown that it knew of the possible contents on the devices, but held that this was immaterial because the court had ordered the defendant to disclose the passcodes, not the contents of the phones unlocked by those passcodes. Id. at 23.

Here, the trial court determined that for the "foregone conclusion" exception to apply, the State had to establish, among other things, that it had sufficient knowledge of the existence and location of child pornography files on the hard drives and tower. Under Andrews, however, the State need only show with "reasonable particularity" the knowledge of the existence of the evidence, that defendant has possession and control of that evidence, and that the evidence is authentic. Id. at 22-23.

The evidence that the State sought in this case is the passcodes, not the contents of the external hard drives or computer tower. As we explained in Andrews, the facts implicitly conveyed by the act of disclosing the passcodes are that the defendant knows the passcodes, and that the defendant had possession, custody, and control of the devices encrypted with those passcodes. Ibid.

Moreover, in the opinion, the trial court commented that the State had to prove defendant had exclusive possession of the tower. The court noted there were two other user profiles for the tower. However, in Andrews, we did not state that the "foregone conclusion" exception would only apply if the defendant has exclusive possession and control of the encrypted devices. The State has to prove defendant has possession and control of the encrypted devices, not exclusive possession and control.

Therefore, for the reasons stated in Andrews, we conclude the trial court correctly determined that the "foregone conclusion" exception applied to the passwords to the external hard drives, but erred by finding that the exception did not apply to the computer tower. We conclude the State presented sufficient evidence for the application of the exception to all three devices.

III.

On appeal, defendant argues that the evidence presented at the hearing does not support the trial court's finding that he acknowledged he knew the passcodes to the external hard drives and the computer tower. Defendant asserts that, when Hurley questioned him at the time of the search, she asked if he knew the password for his "computer." Defendant asserts that Hurley asked him about a password for "one unspecified computer," not any other devices.

Defendant's argument is not supported by the record. At the hearing, Hurley was asked if she requested defendant to provide the password to his "computers" and she replied, "Yes, I did." She further testified that defendant would not provide "his password" because "he did not want" the detectives "looking through his stuff." The trial court did not err by interpreting defendant's statements to be an acknowledgement that he knew the passwords to all of his computer devices, including the external hard drives and the computer tower.

Defendant also suggests that Hurley elicited his statements about the passcodes in violation of his rights under Miranda. At the hearing, defendant objected to Hurley's testimony on the ground that the court had not yet conducted a Miranda hearing. The court decided to take testimony on whether defendant was informed of his rights under Miranda, and whether he had waived those rights.

Hurley then testified that she read defendant his Miranda rights, and he did not invoke those rights. Hurley further testified that the detectives did not arrest defendant before she questioned him about the passwords. She also said that she did not threaten defendant or make any promises to induce him to make the statements about the passcodes.

In its opinion, the trial court found the testimony established that Hurley read defendant his Miranda rights before he made his statements. The court found there was no evidence of compulsion and defendant was not under arrest at the time he made his statements. We must defer to the trial court's findings of facts where, as here, they are "supported by sufficient credible evidence in the record." State v. Brown, 216 N.J. 508, 538 (2014) (quoting State v. Elders, 192 N.J. 224, 246 (2007)).

Defendant further argues that the State did not present sufficient evidence to show with "reasonable particularity" that there were images of child pornography on defendant's two external hard drives. As we noted previously, under Andrews, the focus of the analysis for application of the "foregone conclusion" exception is the facts implicitly conveyed by the disclosure of the passcodes, not the content of the devices encrypted with those passcodes. Andrews, 457 N.J. Super. at 24. Therefore, we need not address defendant's argument.

IV.

Defendant further argues that the trial court's order compelling him to produce the passcodes or otherwise decrypt the external hard drives violates his right against self-incrimination under New Jersey law. As noted, the trial court

rejected defendant's contention that the State's common law privilege against self-incrimination precludes the court from requiring defendant to provide his passcodes or otherwise decrypt the external hard drives.

The court stated that New Jersey's right against self-incrimination did not employ the decryption of defendant's devices. The court noted that defendant may generally have a right "to a private enclave where he may lead a private life," but he does not have the right to a "private enclave" replete "with images of child exploitation."

We agree with the trial court's analysis, which applies not only to the external hard drives, but also to the computer tower. We reject defendant's argument that the court's order violates his privilege against self-incrimination under New Jersey law substantially for the reasons stated in Andrews. Id. at 30-34.

V.

Defendant further argues that our court rules do not authorize the State to seek an order compelling him to produce the passcodes or otherwise decrypt the external hard drives and computer tower. He contends that by seeking to compel him to produce the passcodes months after it seized the devices, the State is improperly engaging in discovery, rather than the actions to execute the search

warrant. Defendant's arguments lack sufficient merit to warrant discussion. R. 2:11-3(e)(2).

We note, however, that in this case, the DCJ obtained a search warrant, which authorized it to search for and seize evidence of child pornography in defendant's home, including computers, computer hardware, hard drives, computer storage media, and peripheral devices. The warrant also authorized the DCJ to conduct forensic examination "on scene and later in a recognized laboratory environment on all items until such examination is complete."

As explained previously, in executing the warrant, the DCJ found and seized defendant's encrypted external hard drives and computer tower. Defendant admitted he owned the devices and knew the passcodes, but refused to provide the passwords or decrypt the devices. The State thereafter moved to compel decryption. In doing so, the State was not engaged in discovery. It was seeking information that would allow it to complete the forensic examination of the devices seized, which was specifically authorized by the warrant.

The record shows that the State sought the passcodes so that it could complete the search authorized by the warrant. The State was not attempting to conduct a "new and separate search" and its effort to complete the search was "reasonable under the totality of the circumstances." State v. Hai Kim Nguyen,

419 N.J. Super. 413, 427 (App. Div. 2011) (quoting State v. Finesmith, 406 N.J. Super. 510, 519 (App. Div. 2009), and United States v. Keszthelyi, 308 F.3d 557, 569 (6th Cir. 2002)).

Accordingly, we affirm on defendant's appeal, reverse on the State's cross-appeal, and remand the matter for further proceedings consistent with this opinion. We do not retain jurisdiction.