Police Prosecutor Update

Issue No. 336
June 2020

SEARCH AND SEIZURE
COMPELLING CELL PHONE PASSWORD

On June 23, 2020, the Indiana Supreme Court issued its decision in Seo v. State, ___ N.E.3d ___ (Ind. 2020), vacating the decision in Seo v. State, 109 N.E.3d 418 (Ind. Ct. App. 2018), which was reviewed in the September, 2018, edition of the Police Prosecutor Update. Seo reported to law enforcement that she had been raped. As part of the investigation, she allowed the detective to open her encrypted smart phone (she decrypted it for him) and download its contents. After reviewing the contents of the forensic download, the detective determined that the rape investigation was no longer appropriate and, instead, recommended charges against Seo for stalking and harassing D.S. D.S. had received up to 30 calls and text messages from Seo every day from her cell phone number. Ultimately, he received calls from numerous different cell phone numbers, although the calls and messages appeared to be linked and to come from Seo. The detective suspected Seo was using a third party application to disguise the origin of her calls and messages by making it appear that they originated from different cell phone numbers.

Seo was charged with intimidation, theft and harassment and arrested. When she was arrested, she possessed the same smart phone that the detective had examined. She admitted the phone was hers, and it was seized as evidence. A few days later, Seo was charged with 13 counts of invasion of privacy, alleging she had violated a protective order prohibiting her from contacting D.S. The same day, the police obtained a warrant to search Seo's smart phone. Because the phone was locked, the court also ordered Seo "be compelled to unlock (via biometric fingerprint passcode, password or otherwise)" the phone or be subject to contempt of court. Through counsel, Seo informed the court that she would not comply with the order to unlock the phone. After a hearing, the court issued an order finding Seo in contempt. The court specifically found, "The act of unlocking the phone does not rise to the level of testimonial self-incrimination that is protected by the Fifth Amendment of the United States Constitution or by Article 1, Section 14 of the Indiana Constitution." Seo filed a motion to stay the court's order pending appeal, which the court granted. On appeal Seo argued that the court's order compelling her to unlock the phone violated the Fifth Amendment guarantee against self-incrimination.

The Indiana Court of Appeals found, "Because compelling Seo to unlock her phone compels her to literally recreate the information the State is seeking, we consider this recreation of digital information to be more testimonial in nature than the mere production of paper documents." Therefore, the Court found the trial court's order compelled her to incriminate herself in violation of the Fifth Amendment. On transfer, the Supreme Court found, "The compelled production of an unlocked smartphone is testimonial and entitled to Fifth Amendment protection— unless the State demonstrates the foregone conclusion exception applies." For the foregone conclusion exception to apply, the State must show that it already knows this information: (1) the suspect knows the password; (2) the files on the device exist; and (3) the suspect possesses those files. A "suspect surrendering an unlocked smartphone implicitly communicates, at a minimum, three things: (1) the suspect knows the password; (2) the files on the device exist; and (3)

the suspect possessed those files. And, unless the State can show it already knows this information, the communicative aspects of the production fall within the Fifth Amendment's protection."

In deciding that the state had not met the foregone conclusion exception, the Court stated, "Even if we assume the State has shown that Seo knows the password to her smartphone, the State has failed to demonstrate that any particular files on the device exist or that she possessed those files." Therefore, because the act of producing an unlocked cell phone would give the state access to information that it does not already know, requiring Seo to produce her password violates the Fifth Amendment's privilege against compelled self-incrimination. The trial court's contempt finding was, therefore, reversed.

In conclusion, a defendant cannot be compelled to provide the pass-code to open her cell-phone even if the state can demonstrate that it already knows that she knows the passcode. But what about opening it with her fingerprint? Fingerprints are considered non-testimonial. Could the state compel the defendant to open her phone if it can show that, in addition to knowing her passcode, it knows the files exist on her phone and she is in in possession of them? The Court does not answer either of those questions directly, but it instead expresses its doubts as to whether the foregone conclusion exception can ever apply to digital devices. "The limited, and questionable, application of the foregone conclusion exception also cautions against extending it further." Cell phones contain much more information than the specific files a police investigator would typically look for. "[C]ompelling the production of an unlocked smartphone gives the government access to everything on the device, not just those files it can identify with 'reasonable particularity.'"

While this language is troubling, it does not mean that law enforcement cannot get a warrant to search for evidence contained within a cellular telephone. It simply means that law enforcement cannot compel a suspect to give up the equivalent of the combination to the safe. Law enforcement will have to figure out a digital version of a blow torch to break into a device.

.