New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
JUNE 9, 2021

WHITE-COLLAR CRIME

Hey SIRI, Does the Fifth Amendment Protect My Passcode?

When law enforcement seeks to compel a subject to provide a passcode to allow them to rummage through a cellphone, courts have not spoken with a unified voice. On May 12th, the Supreme Court declined to wade in, seemingly guaranteeing that continued uncertainty on this critical issue will continue to bedevil criminal practitioners. Robert J. Anello and Richard F. Albert discuss the issue in this edition of their White-Collar Crime column.

By **Robert J. Anello**

And **Richard F. Albert**

Cellphones regularly have posed perplexing issues to courts struggling to apply our constitutional rights to this ubiquitous and overwhelmingly important modern technology. The already thorny area of how the Fifth Amendment reaches conduct short of an individual actually speaking to the police or taking the witness stand has proven no exception. The right against self-incrimination generally covers potentially incriminatory testimonial communications—assertions of fact deriving from the person's mind—and not demands to produce something that already exists. Unless, as is typically the case, the very act of producing that thing implicitly communicates incriminatory information.

When law enforcement seeks to compel a subject to provide a passcode to allow them to rummage through a cellphone, courts have not spoken with a unified voice. Some, including New Jersey's highest court, have arrived at the dubious conclusion that requiring an individual to communicate cellphone passcodes to the government does not warrant Fifth Amendment protection. According to such courts, the passcodes themselves are of minimal testimonial value, and therefore can be compelled if their existence, possession and authentication are "foregone conclusions." This rationale improperly extends a narrowly drawn exception in Fifth Amendment "act of production" doctrine to encompass nearly every person who owns a cellphone. Critics of that analysis cite to Justice Stevens' metaphor that the government can require you to surrender the key to a locked safe but cannot force you to say its combination to argue that requiring a person to disclose their passcode is a testimonial act that cannot be compelled. Commentators had hoped that a certiorari petition filed in *Andrews v. New Jersey*, no. 20-937, would provide an opportunity for the Supreme Court to clarify the law and reject the New Jersey Supreme Court's expansive view. On May 12, 2021, however, the Supreme Court declined to wade in, seemingly guaranteeing that continued uncertainty on this critical issue will continue to bedevil criminal practitioners.

The Fifth Amendment Act of Production Doctrine

The Supreme Court's Fifth Amendment jurisprudence provides that testimonial communications occur when a person makes a factual assertion or discloses information that derives from the person's own mind. Typically, actions that do not require an individual to make a factual assertion are nontestimonial and therefore are not protected by the Fifth Amendment. For instance, the Fifth Amendment does not bar the compelled production of a person's voice, blood or handwriting samples. Similarly, the Supreme Court has held that authorities can require an individual to sign a consent directive allowing the government to access the person's foreign bank accounts without violating the Fifth Amendment.

The Supreme Court established the modern analytical framework for the application of Fifth Amendment self-incrimination doctrine to demands for existing documents and things

ROBERT J. ANELLO *and* RICHARD F. ALBERT *are partners at Morvillo Abramowitz Grand Iason & Anello, P.C.* RYAN MCMENAMIN, *an associate at the firm, assisted in the preparation of this article.*

in *Fisher v. United States*, 425 U.S. 391 (1976), a case involving a document subpoena. The court held that although the contents of pre-existing documents typically are not subject to Fifth Amendment protection, the very "act of production" of documents could take on a testimonial character, and implicitly communicate incriminatory statements. For example, if a witness is required to produce a particular letter or bank statement, the content of the document is not protected, but the witness's producing it pursuant to a subpoena is an implicit assertion that the document exists, that it is authentic, and it is in the witness's possession. As *Fisher* explained and subsequent Supreme Court decisions have held, the Fifth Amendment right against self-incrimination protects the witness against being forced to make those implicit assertions through the "act of production," and thus (subject to exceptions for, among other things, the records of collective entities) protects the witness from being required to produce the document. As the court held in *Fisher*, however, a narrow exception to the protection of the "act of production" doctrine exists where the information revealed by the compelled act is a "foregone conclusion"—in other words, the government can already establish the document's existence, authenticity and possession, and therefore it does not communicate anything of value to the government that it does not already know.

A Potential New Application of Act of Production Doctrine: Decryption

When law enforcement cannot access a device due to its encryption, a law enforcement demand to direct the owner of the device to disclose its password implicates the Fifth Amendment. With few exceptions, courts generally have agreed that disclosing a passcode to the government amounts to a testimonial act because the communication is a factual assertion, at the very least, that the person knows the password. Courts have disagreed, however, as to whether the act of production doctrine's foregone conclusion exception applies to compelled decryption. Some courts have held that the foregone conclusion exception applies when the government can independently show that the suspect knows the password. Other courts have ruled the exception is wholly inapplicable outside the context of a subpoena for preexisting documents.

As the law stands today, whether you are entitled to the Fifth Amendment's protections depends heavily on which state or federal jurisdiction you are located. In Massachusetts, the state's highest court has ruled that law enforcement can make you unlock your phone if they can show that you own the phone. In Indiana, by contrast, law enforcement cannot make you unlock your phone unless investigators can show they already know the incriminating evidence that is on the phone. In Florida, conflicting decisions have been issued by different appellate districts within the state. Similarly, in the federal system, the Northern District of California has ruled that disclosing a cellphone passcode is always testimonial, like reciting the safe combination referenced by Justice Stevens, triggering the self-incrimination clause—and the Fourth Circuit Court of Appeals has suggested that law enforcement can require someone to enter a phone's passcode without violating the Fifth Amendment.

'Andrews v. New Jersey'

In August 2020, the New Jersey Supreme Court weighed in on the debate. The case arose from an official misconduct investigation of Robert Andrews, a former Essex County Sheriff's Officer. In the course of an Essex County narcotics investigation directed at Quincy Lowery, Lowery informed detectives that Andrews, a friend from Lowery's motorcycle club, had been providing Lowery with confidential information about the investigation. Andrews told him various ways to avoid detection by law enforcement and instructed Lowery on how to locate tracking devices hidden in his car and how to determine whether certain license plates numbers belonged to law enforcement. The state eventually obtained warrants for cellphone numbers corresponding to both Lowery and Andrews. The warrants showed over one hundred calls and text messages between the two over a period of six weeks. Andrews ultimately was indicted for official misconduct, hindering apprehension and obstruction of justice.

Following the seizure of Andrews's cellphones, the state determined that Apple's encryption measures made access to the devices impossible. Prosecutors moved for an order compelling Andrews to disclose the passcodes. He opposed, claiming that forcing him to disclose the passcodes violated his right against self-incrimination.

New Jersey's lower courts rejected Andrew's argument and the New Jersey Supreme Court affirmed in a 4 to 3 decision, holding that although a compelled passcode disclosure amounted to a testimonial act under the Fifth Amendment, the disclosure fell within the "foregone conclusion" exception. In analyzing whether the disclosure was testimonial, the majority invoked Justice Stevens' metaphor and found that revealing a cellphone passcode was analogous to the combination of a safe and not a key because the required facts—the passcodes—were kept in Andrews's mind. The court ruled that nevertheless, cellphone passcodes are without independent evidentiary

significance, and found that providing a passcode was subject to the "foregone conclusion" exception derived from case law applying the act of production doctrine. Because the state already demonstrated that the defendant owned and operated the cellphones associated with the passcodes, the court reasoned that the foregone conclusion exception applied.

Justice LaVecchia dissented, arguing that the majority opinion violated a core principle that the Fifth Amendment protects the government from compelling someone to provide their inner-held thoughts in order to assist in one's prosecution. The majority had disregarded that the Supreme Court had never applied "foregone conclusion" analysis beyond the implicit assertion of fact deriving from the physical act of producing a document pursuant to a subpoena. The dissent asserted that the foregone conclusion doctrine has nothing to do with the government's compulsion of pure testimony, and thus being compelled to disclose a cellphone passcode violates the Fifth Amendment.

Courts Are Forgoing the Foregone Conclusion Exception

The Supreme Court has thus far resisted the chance to provide guidance in this area. In 2020, the court denied a petition appealed from the Pennsylvania Supreme Court, which concluded on facts nearly identical to *Andrew*s that an individual could not be compelled to disclose a cellphone passcode. Twenty-one states urged the Supreme Court to grant certiorari in an amicus brief filed in support of that petition, stating that the resolution of the matter could affect nearly every criminal case.

This year, commentators had hoped that the Supreme Court would grant the *Andrews* petition to clarify the law and obviate the absurd result that an individual's constitutional rights depend on which side of the Delaware River he or she stands. Moreover, the state supreme court decisions that have come out on opposing sides of this issue generally have been decided by thin majorities with robust dissents. In opposing a grant of certiorari, the state of New Jersey, for its part, argued that overturning the decision below would cause wrongdoers to intentionally disable biometric accessibility to their devices (and make them password-only) in order to render their contents unavailable to law enforcement. Despite the weighty concerns at play, the Supreme Court denied certiorari.

State supreme court decisions issued since Andrews filed his certiorari petition nevertheless suggest the tide is turning against the use of the foregone conclusion exception to compel password disclosures. In January 2021, the Supreme Court of Oregon held on state constitutional grounds that compelling an individual to unlock a cellphone with a passcode violated the right against self-incrimination. In *State v. Pittman*, the defendant twice entered the wrong passcode into her phone after the police presented her with a lawful order to unlock the phone. The trial court found her in contempt and sentenced her to thirty days in jail before the Oregon Supreme Court reversed.

Most recently, on Feb. 11, 2021, the Utah Supreme Court in *State v. Valdez* declined to apply the foregone conclusion exception to law enforcement's failed attempt to require a suspect to disclose his cellphone passcode. After obtaining a warrant to search Valdez's phone, police officers asked him for his passcodes and explained that they would destroy his phone if he refused. Valdez refused and told the officers they could destroy the phone. At trial, the prosecutors argued that the jury should infer that the phone had incriminatory content based on Valdez's refusal. The court ruled that the state's comment that Valdez's refusal supported an inference of guilt was reversible error. Like the dissent in *Andrews*, the Utah Supreme Court found that the foregone conclusion doctrine was ill-suited for analyzing the compelled communication of a person's cellphone passcode.

Conclusion

The Supreme Court's denial of the *Andrews* petition disappointed those who yearned for a unified approach to an issue that has fractured the lower courts. As a host of courts have now properly concluded, however, the narrow "foregone conclusion" exception to the implicit testimonial aspects of producing existing documents provides no valid basis for compelling all cellphone owners to explicitly testify to their cellphone password.

Over seven years ago, in applying the Fourth Amendment's warrant requirement to cell phones, the Supreme Court observed that "cell phones are such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley v. California*, 573 U.S. 373, 385 (2014). This year regrettably we will not benefit from the Supreme Court's views on how the Fifth Amendment applies to cellphone passcodes, but these devices' near-anatomical role in our lives makes it unlikely that this constitutional quandary will soon go away.