Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

Catch Me If You Scan: Constitutionality of Compelled Decryption Divides the Courts

March 6, 2020

In the digital age, courts have been tasked with determining how longstanding constitutional protections for criminal suspects and defendants apply to new forms of technology like smartphones that are portable, nearly ubiquitous, and increasingly capable of revealing extremely intimate details of their owners' lives. Many court cases and legal commentators have focused on when law enforcement searches of electronic devices are permissible under the Fourth Amendment. That Amendment protects against unreasonable "searches and seizures" by the government, and in recent cases such as *Riley v. California* and *Carpenter v. United States*, the Supreme Court has recognized that a search of digital information associated with a mobile device often requires a warrant supported by probable cause to be considered "reasonable" under the Fourth Amendment.

Obtaining a warrant to search a smartphone or other electronic, data-containing device does not guarantee that law enforcement can access the device's data, however, as such devices "can be and often are encrypted." And decryption frequently requires entering a password or, increasingly, using a biometric identifier such as a fingerprint or facial scan. When a warrant is obtained to search a protected device, the question becomes whether a suspect or ostensible owner of the device can be compelled to furnish the password or biometric identifier needed to access the device's data. Courts in recent years have had to grapple with whether compulsion in such cases would violate the Fifth Amendment's Self Incrimination Clause, which provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself[.]" Courts have reached conflicting conclusions as to whether and when the compelled decryption of a password- or biometric-identifier-protected device runs afoul of the Fifth Amendment. And perhaps counterintuitively, the trend appears to favor recognizing more constitutional protection for password-protected devices than for devices protected by a biometric identifier. This Sidebar provides an overview of the Self Incrimination Clause and relevant case law; surveys some recent cases addressing the Fifth Amendment's application to compelled decryption of password- and biometric-identifier-protected electronic devices; and concludes with some considerations for Congress.

Fifth Amendment: Overview of Pertinent Principles

For the Fifth Amendment privilege against compelled self-incrimination to apply, what the government is compelling must (among other things) be considered "testimonial," meaning that the compelled

Congressional Research Service
https://crsreports.congress.gov
LSB10416

individual must use "'the contents of his own mind' to explicitly or implicitly communicate some statement of fact." Generally, then, the government may not compel a criminal suspect to make an incriminating *communication*. The privilege does not, however, ordinarily "protect a suspect from being compelled . . . to produce 'real or physical evidence.'" For example, the government may force a suspect to give a blood sample or a handwriting exemplar, stand in a lineup, or even provide a voice exemplar, because, although these acts certainly can furnish incriminating information, they do not require the suspect to "disclose any knowledge he might have" or "speak his guilt."

Nevertheless, the Supreme Court has recognized that certain acts can be testimonial, and thus covered by the Fifth Amendment, where the acts "implicitly communicate 'statements of fact.'" Most notably, the Court has indicated that although the Fifth Amendment does not protect voluntarily created incriminating documents themselves, "the act of producing documents in response to a subpoena may have a compelled testimonial aspect" of its own because in segregating and producing the documents sought, "the witness would admit that the papers existed, were in his possession or control, and were authentic." The Court analogized identifying documents responsive to a subpoena to "telling an inquisitor the combination to a wall safe" (which would presumably require use of "the contents of [one's] own mind" and thus could be testimonial) rather than "being forced to surrender the key to a strongbox" (which apparently would not).

Yet if the government can show that it *already knows* of the existence and the suspect's possession of the documents at issue—i.e., that these matters are a "foregone conclusion" and thus that the factual assertions implicit in the act of production add "little or nothing to the sum total of the Government's information"—then "no Fifth Amendment right is touched because the 'question is not of testimony but of surrender.'" As an example, in *Fisher v. United States*, the Supreme Court applied this so-called "foregone conclusion" exception to determine that the Fifth Amendment did not protect taxpayers from having to produce certain tax documents their accountants had prepared, as the government already knew from the accountants that the papers existed and were in the taxpayers' possession.

Application of Fifth Amendment to Compelled Decryption

Recently, numerous federal and state courts have grappled with how the above principles apply to compelled (1) entry of a password or passcode to unlock an electronic device, and (2) use of a biometric identifier such as a fingerprint or face-scan to do the same.

Passwords and Passcodes

Courts have mostly, though not entirely, agreed that unlocking a phone or other data-containing device with a password or passcode is a testimonial act under the Fifth Amendment, as such an act "demand[s] the use of the contents of the mind" and carries an implicit assertion of certain statements of fact. Courts and commentators have disagreed, however, on the precise nature of those implied statements of fact, which has resulted in conflicting views on what the government must actually know (i.e., what information is a "foregone conclusion") to overcome a Fifth Amendment objection.

At one end of the spectrum, some courts have taken the position that "the only fact conveyed by compelling a defendant to enter the password to an encrypted electronic device is that the defendant knows the password and can therefore access the device," or some variation of that fact. Thus, according to these courts, what the government must establish to overcome a Fifth Amendment objection is merely "that the suspect's knowledge of the passcode is a foregone conclusion, not that the contents of the device are a foregone conclusion." For example, one state appellate court upheld an order requiring a defendant to enter a passcode to unlock his smartphone because he had previously unlocked the phone in front of law enforcement. The court reasoned that the "implicit facts" at issue—"the existence of the passcode, its possession or control by [the defendant], and the passcode's authenticity"—were thus "already known" to the government and a foregone conclusion. Under this view, the Fifth Amendment appears to pose a

relatively limited information-access barrier, as the circumstances in which an encrypted device is seized may often suffice to conclude that the person under compulsion can decrypt the device.

However, some other courts have instead looked to whether the government has independent knowledge of the device's *contents*. Analogizing to the context of physical document production in which the Supreme Court announced the relevant Fifth Amendment concepts, these courts have required the government to show with "reasonable particularity" its knowledge that specific files or data are contained on the device. In support, these courts have theorized that "when it comes to data locked behind a passcode wall, the object of the foregone conclusion exception is not the password itself, but the data the [government] seeks behind the passcode wall." Accordingly, this view appears to regard the testimonial assertions implicit in compelled decryption as including that the decrypting "person possesses, perhaps knowingly, the files on the device." One Florida appellate court, for instance, quashed a trial court order requiring a minor to provide a smartphone passcode and iTunes password, as the government failed "to identify any specific file locations or even name particular files that it [sought]." This approach may impose a more formidable barrier to compelled decryption of electronic devices, as it bars the government from accessing such devices unless it can point to particular documents it needs that are on the device to be searched.

The only federal appellate court to address directly the Fifth Amendment implications of compelled decryption using a password appears to have required the government to show both that the suspect knew the passwords at issue and that particular content would be found following decryption. In a 2012 decision, the Eleventh Circuit held that the foregone conclusion exception did not support a subpoena requiring a suspect to produce the decrypted contents of password-protected hard drives. In so doing, the court recognized that "the decryption and production would be tantamount to testimony by [the suspect] of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; and of his capability to decrypt the files." And because nothing indicated that the government knew "whether any files exist and are located on the hard drive" or knew "with reasonable particularity that [the suspect] is even capable of accessing the encrypted portions of the drives," the court concluded that the implicit testimony at issue was not a foregone conclusion. However, another federal appellate court subsequently questioned the Eleventh Circuit's focus on the government's knowledge of the content on an encrypted device, noting in dicta that "a very sound argument can be made" that the proper focus is "limited to the question" of the suspect's "knowledge of the password itself."

Finally, one state supreme court has entirely rejected the foregone conclusion exception's applicability in this context. In *Commonwealth v. Davis*, the Supreme Court of Pennsylvania took the view that "the foregone conclusion gloss" on the Fifth Amendment is "an extremely limited exception" that the Supreme Court has only ever applied to the "unique category" of "specific existing business or financial records." And unlike that category "or demands for physical evidence such as blood, or handwriting or voice exemplars, information in one's mind to 'unlock the safe' to potentially incriminating information does not easily fall within [the foregone conclusion] exception." The court accordingly concluded that the exception is simply "inapplicable to compel the disclosure of a defendant's password to assist the [government] in gaining access to a computer."

Biometric Identifiers

Unlike compelled decryption using a password or passcode—which courts have generally recognized as testimonial (subject to the "foregone conclusion" exception)—several federal and state courts have determined that compelled decryption using a biometric identifier such as a fingerprint scan does not implicate the Fifth Amendment in the first instance. These courts have viewed compelled decryption using biometric identifiers as permissible *regardless* of what the government knows—or, indeed, whether

it knows anything at all—because merely exposing a physical feature to a locked electronic device does not require use of "the contents of [one's] own mind" to communicate a statement of fact.

For instance, an Illinois federal district court granted the government's request to require four residents of a home "to apply their fingers and thumbs (as chosen by government agents) to the fingerprint sensor on any Apple-made devices found . . . during [a] search." In the court's view, simply seizing "a physical characteristic" by selecting and applying fingers to a sensor would not "engage the thought process of any of the residents," meaning that "the person's performance of the compelled act is not an act of communication by that person" for Fifth Amendment purposes. In reaching its conclusion, the court relied on the aforementioned metaphor of obtaining a key versus a combination to a physical safe. According to the court, while forcing disclosure of a safe's combination would require "obtaining information from a person's mind" and thus implicate the Fifth Amendment, requiring the surrender of a physical key to that safe would not. As such, the court concluded that "a person generally cannot be compelled to disclose the passcode [to an encrypted device] (like the safe's combination) but can be compelled to provide the fingerprint (like the key to the safe)."

However, other courts have rejected the combination/key analogy as undeveloped dicta from a Supreme Court footnote, concluding instead that there is "no meaningful distinction between unlocking a device with a password and unlocking [it] . . . with a biometric feature" and thus that compelled application of a biometric identifier amounts to a testimonial assertion of fact. For these courts, then, the relevant question becomes whether to apply the "foregone conclusion" exception previously discussed.

Considerations for Congress

The applicability the Fifth Amendment to compelled decryption of electronic devices is by no means settled, as evidenced by the conflicting approaches and outcomes in cases across the country, as well as the petitions that have been granted or are pending before multiple state supreme courts. While the U.S. Supreme Court has previously declined to review decisions addressing compelled decryption via passcodes and biometric identifiers, it may ultimately choose to weigh in to reconcile increasingly divergent judicial views. At least one court has called on Congress to set a national standard, arguing that "the legislature is better positioned to balance the interests of law enforcement and privacy interests." That said, though Congress generally may impose statutory requirements that exceed the minimum standards established by the Constitution (and there have been proposals addressing compelled decryption in particular contexts introduced in this Congress), it is always possible that an intervening constitutional interpretation by the Supreme Court could supersede statutory procedures.

Conversely, should Congress seek to ensure that encryption does not pose an obstacle to law enforcement, one commentator has argued that Congress could establish specific and severe criminal penalties for refusing to decrypt a device like a smartphone. However, authority for such an enactment would still depend on whether the Fifth Amendment restricts compelled decryption, as Congress may not legislate away constitutional protections. As such, legislative and investigative efforts may alternatively focus on mandates directed to *technology companies* that manufacture devices with encryption capabilities or control encrypted data, although such a focus could raise distinct issues. In any event, under current law, federal courts may hold those who fail to obey lawful orders in contempt, meaning that suspects who refuse to unlock electronic devices may already be subject to punishment in jurisdictions where a Fifth Amendment objection is untenable. Compelled testimony is also authorized where the person compelled is given immunity.

Author Information

Michael A. Foster
Legislative Attorney

Disclaimer