NACDL
FOURTH
AMENDMENT
CENTER

Compelled Decryption Primer

The Supreme Court recognized in *Riley v. California* that cell phones are unlike other types of physical objects. 134 S.Ct. 2473 (2014). Instead, the Court held, they are minicomputers that contain the most intimate details of life. Due to their immense storage capacity, combined with the many distinct types of private data they contain, the Court held that the Fourth Amendment requires law enforcement to get a warrant to search a cell phone, even incident to arrest.

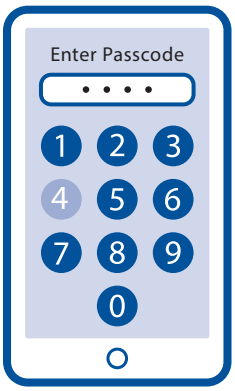
But if a device is locked or encrypted, can law enforcement compel a suspect to unlock or decrypt it? This primer outlines the state of the law on compelled decryption and offers a guide for defense lawyers on this important emerging issue.

The majority of Americans now own several devices that are encrypted until unlocked by a passcode or biometric mechanism. A passcode can be a secret number, pattern, or alphanumeric password. Biometric locks may use a fingerprint or face scan. These locks serve to make their contents inaccessible and unreadable until unlocked and decrypted by an authorized user.

While the lawfulness of a device search is a Fourth Amendment issue, the Fifth Amendment privilege against self-incrimination is the central safeguard against compelled decryption. To successfully assert this right, the act of decryption must be compelled, incriminating, and "testimonial." While the first two requirements are often easily met, the key question is whether decryption is testimonial.

Is Compelling Decryption "Testimonial"?

The act of decrypting a device may be "testimonial" under the Fifth Amendment if it explicitly or implicitly conveys the fact that certain data exists or is in the possession, custody, or control of an individual. *See In Re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335 (11th Cir. 2012). Such an "act of production" may itself be incriminating or effectively concede the "existence, possession and control, and authenticity" of potentially incriminating evidence on a device. *Id.* at 1343. This analysis often hinges on the type of lock employed.



Numeric or Alphanumeric Locks: Courts have generally found that compelling individuals to provide their numeric or alphanumeric passcode is potentially testimonial under the Fifth Amendment, as it forces the defendant to reveal "the contents of his own mind." *In Re Grand Jury Subpoena Duces Tecum* 670 F.3d at 1345; *see also U.S. v. Apple MacPro Computer,* 851 F.3d 238 (3d Cir. 2017). It is analogous to compelling production of the combination to a wall safe, which is testimonial, as opposed to surrendering the key to a strongbox, which is not. *See Doe v. U.S.*, 487 U.S. 201, 220 (1988). However, even if a court finds that providing the passcode is "testimonial," it may still fall under the "foregone conclusion" exception, which is addressed on the next page.

Biometric Locks: Some courts have found nothing testimonial under the Fifth Amendment about compelling the production of biometric keys, such as a fingerprint, similar to tests that gather physical evidence. *See, e.g., State v. Diamond,* 905 N.W.2d 870 (Minn. 2018); *Matter of Search of [Redacted] Washington, D.C.*, 317 F. Supp. 3d 523 (D.D.C. 2018); *Commonwealth v. Baust,* 89 Va. Cir. 267 (Va. Cir. Ct. 2014). Recently, however, others have begun to hold that compelling the production of a biometric key is just as testimonial as a numeric one. *See Matter of Residence in Oakland, California*, 354 F. Supp. 3d 1010, 1016 (N.D. Cal. 2019); *In Re Application for a Search Warrant*, 236 F. Supp. 3d 1066 (N.D. Ill. 2017). From this perspective, "biometric features serve the same purpose of a passcode, which is to secure the owner's content, pragmatically rendering them functionally equivalent." 354 F. Supp. 3d at 1015.

Is it a "Foregone Conclusion"?

Even if the act of decryption is potentially testimonial, it may not violate the Fifth Amendment if the implicit facts conveyed by doing so would be a "foregone conclusion" that "adds little or nothing to the sum total of the government's information." *U.S. v. Hubbell*, 530 U.S. 27, 45 (2000). As a general rule, the "foregone conclusion" exception applies if the government can show it knows the location, existence, and authenticity of the purported evidence with reasonable particularity. *Id*. at 27. But the Supreme Court has never applied the exception beyond business documents, indicating an unwillingness to do so where more private and personal documents, like a diary, are at issue. *Fisher v. U.S.*, 425 U.S. 391, 401 & n.7 (1976) (citing *U.S. v. Bennet*, 409 F.2d 888, 897 (2d Cir. 1969)). It is therefore essential to challenge whether the doctrine applies at all in the digital context. The Court has repeatedly emphasized that cell phones are not like ordinary closed containers or physical objects. *See Riley*, 134 S. Ct. at 2491 ("[A] cell phone search would typically expose to the government far more than the most exhaustive search of a house"); *Carpenter* v. U.S., 138 S.Ct. 2206, 2220 (2018) (requiring a warrant for historical cell phone location information). Indeed, the breadth and depth of private information contained in modern electronic devices simply did not exist when the Court established the foregone conclusion rule. Defense counsel should argue that it does not apply in the context of digital devices, just as the Court declined to apply the search-incident-to-arrest rule in *Riley* and the longstanding "third-party doctrine" in *Carpenter*.

In the alternative, the critical question is whether the government already knows of the existence and location of relevant files and can show that the client can access them. *In Re Grand Jury Subpoena Duces Tecum*, 670 F.3d at 1346. Lower courts are currently split on the test for deciding this question in the context of digital devices. Each of the tests is addressed below:

Reasonable Particularity Test: The Eleventh Circuit has held that the foregone conclusion rule applies only if the government can show with "reasonable particularity" that the purported evidence exists, is in a certain location, and is authentic. By contrast, the rule does not apply if the government is unable to identify specific files or data that investigators expect to find. *See In Re Grand Jury Subpoena* 670 F.3d at 1346; *see also Apple MacPro Computer*, 851 F.3d at 248-49 (applying Eleventh Circuit's test, but finding a foregone conclusion where a family member saw the defendant navigate to child pornography on the encrypted device). This is a high bar to meet, consistent with the high degree of constitutional protection that the Supreme Court has afforded to modern cell phones.

Clear & Convincing Evidence Test: Some courts have rejected the Eleventh Circuit's "reasonable particularity" test. In *U.S. v. Spencer,* for example, the court instead required "clear and convincing evidence" that the defendant could unlock his phone. No. 17 CR 259, 2018 WL 1964588 (N.D. Cal. Apr. 26, 2018). This test shifts the goalposts in a way that is exceedingly unfavorable to the defense. Rather than needing to show that the files exist, are on the device, and are authentic, the *Spencer* court requires the government to show only that an individual can unlock his own phone, a low bar to clear in most cases.

Other Potential Legal Arguments

Is Compelled Decryption Necessary or Appropriate?

When a suspect does not provide a passcode to decrypt a device, the government may invoke the All Writs Act for a court order to compel decryption "in aid of" a valid search warrant. *See U.S. v. Apple MacPro Computer,* 851 F.3d at 241-42. But, if the government has the technical capability to decrypt the device itself, or can reasonably acquire that ability, then an order compelling decryption is improper.

As private companies develop technologies that allow the government to unlock and decrypt devices, the government should be required to disclose any methods known or reasonably available to it that could be used instead of ordering a suspect to provide a passcode for an encrypted device or compelling a company to assist in the search of a device. An All Writs Act order compelling the suspect to decrypt a device is not "necessary or appropriate" if the government has other viable means of getting in.

Is the Search Warrant Overbroad?

When presented with a warrant to search a device locked by a biometric key, make sure to check that the warrant describes the device to be searched, files expected to be found, and specific individuals law enforcement seek to compel to provide a biometric key. In *In Re Application for a Search Warrant*, 236 F. Supp. 3d 1066 (N.D. Ill. 2017), the court found that the search warrant application lacked enough detailed information about the devices to be searched, and residents of the premises to be searched. The magistrate judge found that, in this case, the use of a fingerprint to unlock a device would be testimonial because it would communicate that the individual had accessed the device before and had control over its contents. *Id.* at 1073*; see also In the Matter of the Search of a Residence in Oakland, California,* No. 4-19-70053, 2019 WL 176937, at *3-5 (N.D. Cal. Jan. 10, 2019) (finding that the warrant's language was overbroad, and that the use of a fingerprint to unlock the device was testimonial for Fifth Amendment purposes).

State Jurisdictional Challenges

State courts may lack jurisdiction to issue a compelled decryption order if there is no state law granting judges such authority. While state law may authorize courts to compel the production of evidence in certain circumstances, device decryption is likely not one of them, indicating that the legislature did not intend to vest courts with this power. Federal courts have the general authority to compel the production of evidence "in aid of their respective jurisdictions" under the All Writs Act, 28 U.S.C.A. § 1651, but similar provisions may not exist in state law. Consequently, any decryption order issued by a state court may be vulnerable to jurisdictional challenges as well as constitutional ones.

Border Searches

If an individual is entering the United States, the government's stated interest in national security at the border will often outweigh an individual's privacy rights. For more information on how your constitutional rights may be interpreted during a border search, please see NACDL's primer "Protecting Your Digital Devices at the Border," available at: **https://www.nacdl.org/bordersearches.**

Case List

Compelling A Passcode Is Testimonial:

- *In Re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335 (11th Cir. 2012).
- *Seo v. State*, 109 N.E.3d 418 (Ind. Ct. App.), transfer granted, opinion vacated, 119 N.E.3d 90 (Ind. 2018).
- *U.S. v Kirschner*, 823 F. Supp. 2d 665 (E.D. Mich. 2010).
- *G.A.Q.L. v. State*, 257 So.3d 1058 (Fla. Dist. Ct. App. Oct. 24, 2018).
- *SEC v. Bonan Huang*, 2015 WL 5611644 (E.D. Pa. 2015).

Compelling Biometric Decryption Is Testimonial:

- *In Re Application for a Search Warrant*, 236 F. Supp. 3d 1066 (N.D. Ill. 2017).
- *Matter of Residence in Oakland, California*, 354 F. Supp. 3d 1010 (N.D. Cal. 2019).

Biometric Decryption Is Not Testimonial:

- *State v. Diamond*, 905 N.W.2d 870 (Minn. 2018).
- *Matter of Search of [Redacted] Washington*, D.C., 317 F. Supp. 3d 523 (D.D.C. 2018).

Passcode Is Testimonial, But The Foregone Conclusion Applies:

- *U.S. v. Spencer*, No. 17-cr-00259-CRB-1, 2018 WL 1964588 (N.D. Cal. April 26, 2018).
- *Commonwealth v. Baust*, 89 Va. Cir. 267 (Va. Cir. Ct. 2014).
- *Commonwealth v. Jones*, 481 Mass. 540 (2019).
- *U.S. v. Friscosu*, 841 F. Supp. 2d 1232 (D. Colo. 2012).
- *State v. Stahl*, 206 So. 3d 124 (Fla. Dist. Ct. App. 2016).
- *U.S. v. Apple MacPro Computer*, 851 F.3d 238 (3d Cir. 2017).

Fifth Amendment Privilege Against Self-Incrimination Generally:

- *U.S. v. Hubbell*, 530 U.S. 27 (2000).
- *Fisher v. U.S.*, 425 U.S. 391 (1976).
- *U.S. v. Doe*, 465 U.S. 605 (1984).
- *Hoffman v. U.S.*, 341 U.S. 479 (1951).
- *Doe v. U.S.*, 487 U.S. 201, 220 (1988).
- *U.S. v. Patane*, 542 U.S. 630 (2004).

Other:

- *U.S. v. Djibo*, 151 F. Supp. 3d 297 (E.D. N.Y. 2015) (passcode suppressed as an un-Mirandized statement).
- *U.S. v. Gavegnano*, 305 Fed. App'x. 954 (4th Cir. 2009) (no expectation of privacy in a gov't-issued computer).

Additional Resources

- Stephanie Lacambra, *Defending Against the Digital Dragnet: Fighting Compelled Password Disclosure and Decryption,* Electronic Frontier Foundation, Oct. 31, 2017.
- Aloni Cohen and Sunoo Park, *Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries*, 32 HARV. J.L. & TECH. 169 (2018).
- Efren Lemus, *When Fingerprints Are Key: Reinstating Privacy to the Privilege Against Self-Incrimination in Light of Fingerprint Encryption in Smartphones,* 70 SMU L. REV. 533 (2017).
- Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices,* 87 FORDHAM L. REV. 203 (2018).
- Jason Wareham, *Cracking the Code: The Enigma of the Self-Incrimination Clause and Compulsory Decryption of Encrypted Media,* 1 GEO. L. TECH. REV. 247 (2017).
- Hanni Fakhoury, *A Combination or a Key? The Fifth Amendment and Privilege Against Compelled Decryption,* 9 DIGITAL EVIDENCE & ELECTRONIC SIGNATURE L. REV. 81 (2012).

For litigation assistance and other resources, contact 4AC@nacdl.org

NACDL FOURTH AMENDMENT CENTER