NACDL FOURTH AMENDMENT CENTER

COMPELLED DECRYPTION PRIMER

NOVEMBER 2025

The Supreme Court recognized in *Riley v. California* that cell phones are unlike other types of physical objects.[1] 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. Law enforcement can gain access to devices via consent or digital extraction tools such as Cellebrite and Graykey. But when those methods fail, the question remains: can law enforcement compel someone to produce their passcode? Can they compel an individual to provide their fingerprint or other biometrics 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 issue.

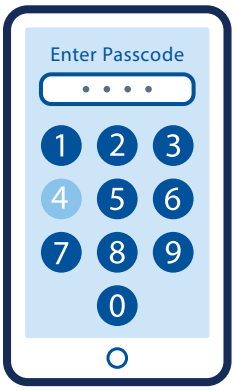
The majority of Americans now own several devices that are encrypted until unlocked by a passcode or biometric mechanism. A passcode can be a secret number, pattern, or alphanumeric password.[2] Biometric locks may use a fingerprint or face scan.[3] These locks serve to make a device's contents inaccessible and unreadable until unlocked and decrypted by an authorized user. Modern cell phones are most commonly locked and encrypted, although it is possible for a device to be locked with unencrypted data.

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." The first two requirements are often obviously met, so the key question becomes whether compelled decryption is testimonial.

Is Compelling Decryption "Testimonial"?

There is wide variance in the case law on this subject. Courts, state and federal, have split on nearly every aspect of this question—including whether biometric decryption is testimonial, whether having to verbally provide a password is testimonial, and whether either is testimonial but falls within a permissible exception. Importantly, there are three Supreme Court cases cited most frequently as the foundations for Fifth Amendment analysis on this issue; one or more will appear in most decisions to address the subject. First, the dissent in *Doe v. United States*[4] is often cited for the analogy that one may be forced to surrender the "key to a strongbox" but not compelled to reveal the "combination to his wall safe—by word or deed," because the latter requires revealing the "contents of the mind." In *Fisher v. United States*,[5] involving tax preparation documents held by an accountant, the Court distinguished compelled testimony from an "act of production" and introduced the "foregone conclusion" exception, discussed below. Finally, *United States v. Hubbell*[6] found that even the production of documents can be testimonial if doing so would convey information about their existence, authenticity, or custody that is unknown to the government.

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," analogous to compelling production of the combination to a wall safe.[7] The Eleventh Circuit considered this issue in *In Re Grand Jury Subpoena Duces Tecum*[8] regarding the decryption of digital hard drives, and held that being forced to turn over the passcodes would require using "the contents of one's mind" and is therefore testimonial. The court stated that the client's "knowledge of the existence and location of potentially incriminating files," his "possession, control, and access to the encrypted portions… and his capability to decrypt the files" would be "tantamount to testimony."[9] Other courts have followed suit.[10]

Biometric Locks

The case law on biometric decryption is mixed. Although some courts have found biometric keys are not testimonial, others have reasoned that they violate the Fifth Amendment. The most recent federal appellate court to consider the issue was the D.C. Circuit in *United States v. Brown*,[11] where the court found that biometric (fingerprint) decryption was testimonial under the Fifth Amendment, departing from other courts that have tended to view "physical traits" such as fingerprints and mugshots as non-testimonial.[12] The Ninth Circuit,[13] by contrast, found that biometric decryption was not testimonial because it does not require revealing contents from one's mind. Defense counsel should note that decrypting data is inherently testimonial because it requires an act of "translation" and therefore, a communicative act. On modern iPhones, encryption keys are inextricably linked with users' passcodes, meaning that the passcode is a foundational part of the encryption and decryption process.[14] In other words, the passcode is a big part of the secret "key" necessary to unencrypt or decode the information the device contains.

Is it a "Foregone Conclusion"?

Even if the act of decryption is testimonial, there is one final hurdle to overcome: the "foregone conclusion" exception.[15] In general, the exception applies to otherwise testimonial acts if the implicit facts conveyed would be a "foregone conclusion" that "adds little or nothing to the sum total of the government's information."[16] But there is a persistent split over how to apply this legal standard to digital devices. Does the government need to know exactly what files they are going to find? Or do they just need to show that someone knows the passcode to their own phone? Some courts have required the government to particularly identify the data they expect to find, while others have effectively lowered this bar based on lesser findings that passwords are "self-authenticating," that the government "established that the passcodes exist," and that the "cellphones were in [the client's] possession when seized and that he owned and operated the cellphones, establishing his knowledge of the passcodes and that the passcodes enable access to the cellphones."[17] Courts have applied one of two tests depending on whether they believe the object of the foregone conclusion exception ought to relate to the specific files on the device or to the passcode itself:

> **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.[18] 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:** A few courts have rejected the Eleventh Circuit's "reasonable particularity" test. In *United States v. Spencer,* for example, the court instead required "clear and convincing evidence" that the defendant could unlock his phone.[19] 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 their own phone, a low bar to clear in most cases.[20]

Defense counsel should argue that the "foregone conclusion" exception should only apply if the government can show it knows the location, existence, and authenticity of the purported digital *files* with reasonable particularity.[21] In other words, the exception should only apply if police can show that they already know that the files exist, that they're located on a particular device, and that the client is capable of accessing that data and unlocking/decrypting it.[22] Only in that situation would compelling decryption "add[] little or nothing to the sum total of the government's information."[23] For example, in holding that the "foregone conclusion" doctrine did not apply, the Eleventh Circuit faulted the government for failing to show "with reasonable particularity…its belief that encrypted files exist on the drives, that Doe has access to those files, or that he is capable of decrypting the files."[24]

The Foregone Conclusion Exception Should Not Apply

It is important to recognize that the Supreme Court has never applied the foregone conclusion exception beyond paper business documents, indicating an unwillingness to do so where more private and personal documents, like a diary, are at issue.[25] It is therefore essential to challenge whether the doctrine applies at all in the compelled decryption context. The Supreme Court has repeatedly emphasized that cell phones are not like ordinary closed containers or physical objects.[26] 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 the rule does not apply in the context of digital devices, just as the Court declined to apply the search-incident-to-arrest rule in *Riley v. California* and the longstanding "third-party doctrine" in *Carpenter v. United States.* [27] Further, counsel should preempt the rationale that passwords meet the foregone conclusion standard via possession, knowledge, and authentication because "[d]irectly providing a passcode to law enforcement is not an 'act.' It is a statement."[28] As testimonial statements, the foregone conclusion analysis should not apply to produced passwords.

OTHER ARGUMENTS TO CONSIDER

Is Compelled Decryption Necessary or Appropriate?

When an individual does not provide a passcode to decrypt a device, the government may invoke the All Writs Act or state equivalent for a court order to compel decryption "in aid of" a valid search warrant.[29] 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. Law enforcement can likely break into a device without compelling decryption in most circumstances. 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 an individual to provide a passcode for their encrypted device or compelling a company to assist in the search of a device. An order compelling an individual to decrypt a device is not "necessary or appropriate" if the government has other viable means of getting in.

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.

Is the Search Warrant Overbroad or Lacking Particularity?

It is always useful to consider Fourth Amendment overbreadth or particularity challenges, as detailed in related resources.[30] For example, 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*,[31] 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.[32]

Border Searches

If an individual is entering the United States, their ability to assert privacy interests in their digital information depends heavily on their immigration status. Additionally, the border falls within an exceptional area wherein the government's stated interest in national security 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 "Device Searches at the Border: A Criminal Defense Lawyer's Primer (April 2025)."[33]

CASE LIST

Compelling A Passcode Is Testimonial:

- *In Re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335 (11th Cir. 2012)
- *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)
- *Commonwealth v. Davis*, 656 Pa. 213, 235 (Pa. 2019)
- *SEC v. Bonan Huang*, 2015 WL 5611644 (E.D. Pa. 2015)
- *United States v. Schvartsman*, 722 F.Supp.3d 276, 315-324 (S.D.N.Y. Mar. 20, 2024) (compelling a password can be testimonial and incriminating, not a foregone conclusion, but found voluntarily disclosed/not compelled in this case)
- *United States v. Gogic*, No. 22-CR-493, 2025 WL 836493 at *4-6 (E.D.N.Y. Mar. 17, 2025) (password is testimonial, does not fall within foregone conclusion exception, not compelled in this case)
- *State v. Valdez*, 552 P.3d 159 (Utah 2023) (providing a password is testimonial but difference between having to say the password vs. putting it in yourself and handing it to them unlocked, act-of-production analysis does not apply (no foregone conclusion))
- *Seo v. State*, 148 N.E. 3d 952, 957-958 (Ind. 2020) (compelled unlocking (having to surrender an unlocked phone) implicitly communicates facts, to become nontestimonial the State must establish that it already knows these facts)

Compelling Biometric Decryption Is Testimonial:

- *People v. Manganiello,* 2025 NY Slip. Op. 03873 (Jun. 27, 2025)
- *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)
- *United States v. Brown*, 125 F.4th 1186, 1202-1203 (D.C. Cir. 2025)

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)
- *Matter of Search Warrant v. Barrera*, 415 F.Supp.3d 832, 839-841 (N.D. Ill. 2019)
- *United States v. Eldarir*, 681 F. Supp. 3d 43 (E.D.N.Y. 2023)
- *In re Search Warrant As to the Residence of Mike Crowe*, 437 F. Supp. 3d 515 (W.D. Va. 2020)
- *United States v. Payne*, 99 F.4th 496, 511-513 (9th Cir. 2024)

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 (Mass. 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*, 851F.3d 238 (3d Cir. 2017)
- *Commonwealth v. Gelfgatt*, 468 Mass. 512 (Mass 2014)
- *Pollard v. State*, 287 So.3d 649, 662 (Fla. Dist. Ct. App. 2019)
- *United States v. Smith*, 706 F.Supp.3d 404 (S.D.N.Y. Dec. 13, 2023)
- *People v. Sneed*, 230 N.E.3d 97, 118 (Ill. 2023)
- *State v. Andrews*, 243 N.J. 447, 480-481 (N.J. 2020)

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).
- *State v. Pittman*, 367 Or. 498, 525 (Or. 2020) (Supreme Court of Oregon case, U.S. v. Payne 9th Circuit case ruled differently) (order compelling someone to unlock a cell phone is valid with (1) warrant for search and seizure of the phone; (2) gov. already knows the information that unlocking the phone would communicate, (3) gov. can't use the act of opening the phone against the individual, only to access the contents)
- *United States v. Sanchez*, 3344 F.Supp.3d 1284, 1300 (N.D. Ga. Sept. 12, 2018) (being forced to give passcode is compelled self-incrimination under 5A, evidence from phone is fruit of the poisonous tree)

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).
- Aubrey Zimmerling, Actions Speak Louder Than Words: Compelled Biometric Decryption is a Testimonial Act, 100 WASH. U. L. REV. 827 (2023)

NOTES

1. 573 U.S. 373 (2014).
2. *See Use a Passcode With Your iPhone, iPad, or iPod Touch,* Apple, https://perma.cc/3YYB-H32S (Last accessed Oct. 2025). *See also Set Screen Lock on An Android Device,* Google Support, https://perma.cc/TS84-5P3E (Last accessed Oct. 2025).
3. *See List of All Fingerprint Scanner Enabled Smartphones,* WebCUSP, https://perma.cc/V9D5-VV2R (last accessed Oct. 2025); *see also List of All Eye Scanner (Iris, Retna Recognition Smartphones),* WebCUSP, https://perma.cc/D286-V59V (last accessed Oct. 2025); Lynn La, *10 Best Phones With Facial Recognition,* CNET, (Aug. 22, 2018), https://perma.cc/H25N-R66J.
4. 487 U.S. 201, 219 (1988).
5. 425 U.S. 391, 411 (1976).
6. 530 U.S. 27, 32 (2000).
7. *See Doe v. U.S.*, 487 U.S. 201, 220 (1988).
8. 670 F.3d 1335 (11th Cir. 2012).
9. *Id.* at 1346.
10. *See United States v. Gogic*, No. 22-CR-493, 2025 WL 836493 at *4-6 (E.D.N.Y. Mar. 17, 2025); *United States v. Schvartsman*, 722 F.Supp.3d 276, 315-324 (S.D.N.Y. Mar. 20, 2024); *State v. Valdez*, 552 P.3d 159 (2023); *Seo v. State*, 148 N.E. 3d 952, 957-958 (2020); *Commonwealth v. Davis,* 656 Pa.213 (2019); *United States v. Apple MacPro Computer,* 851 F.3d 238 (3rd Cir. 2017).
11. 125 F.4th 1186, 1202-1203 (D.C. Cir. 2025).
12. *See People v. Manganiello,* 2025 NY Slip. Op. 03873 (Jun. 27, 2025); *Matter of Residence in Oakland, California*, 354 F. Supp. 3d 1010 (N.D. Cal. 2019); *In Re Application for a Search Warrant*, 236 F. Supp. 3d 1066 (N.D. Ill. 2017).
13. *United States v. Payne*, 99 F.4th 496, 511-513 (9th Cir. 2024).
14. Apple, Inc., *iCloud data security overview*, https://perma.cc/L9EX-HG4R (last accessed Oct. 2025).
15. *See Fisher,* 425 U.S. at 411; *Hubbell,* 530 U.S. at 27.
16. *Fisher,* 425 U.S. at 411.
17. *See State v. Andrews*, 243 N.J. 447, 480 (2020); *Seo v. State*, 148 N.E. 3d 952 (2020); *Pollard v. State*, 287 So.3d 649 (2019).

18. *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).

19. No. 17 CR 259, 2018 WL 1964588 (N.D. Cal. April 26, 2018) (unreported).

20. *See also United States v. Cheng,* No. 4:20 CR 455, 2022 WL 112025 (S.D. Tex. Jan. 12, 2022) (unreported).

21. *See Hubbell,* 530 U.S. at 27; *see also State v. Andrews*, 243 N.J. 447, 480 (2020); *Seo v. State*, 148 N.E. 3d 952 (2020); *Pollard v. State*, 287 So.3d 649 (2019).

22. *See Commonwealth v. Davis*, 656 Pa. 213 (2019) (holding that a password can never fall within the foregone conclusion exception because it is information from one's mind).

23. *Fisher,* 425 U.S. at 411.

24. *In Re Grand Jury Subpoena*, 670 F.3d at 1349.

25. *Fisher,* 425 U.S. at 401 & n.7 (1976) (citing *U.S. v. Bennet*, 409 F.2d 888, 897 (2d Cir. 1969); *see also G.A.Q.L. v. State*, 257 So.3d 1058, 1063 (Fla. Dist. Ct. App. Oct. 24, 2018) (discussing why the foregone conclusion exception cannot apply to a password); *Commonwealth v. Davis*, 656 Pa. 213 (2019) (password cannot fit within foregone conclusion exception).

26. *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).

27. *Id.*

28. *State v. Valdez* 552 P.3d at 170.

29. *See U.S. v. Apple MacPro Computer,* 851 F.3d at 241-42.

30. *See e.g.,* NACDL Geofence Primer (2022), available at https://www.nacdl.org/Document/Geofence-Primer.

31. 236 F. Supp. 3d 1066 (N.D. Ill. 2017).

32. *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).

33. Available at: https://www.nacdl.org/Document/BorderSearchPrimer.

About the National Association of Criminal Defense Lawyers (NACDL)

The National Association of Criminal Defense Lawyers (NACDL) envisions a society where all individuals receive fair, rational, and humane treatment within the criminal legal system.

NACDL's mission is to serve as a leader, alongside diverse coalitions, in identifying and reforming flaws and inequities in the criminal legal system, and redressing systemic racism, and ensuring that its members and others in the criminal defense bar are fully equipped to serve all accused persons at the highest level.

About the NACDL Foundation for Criminal Justice (NFCJ)

NACDL's Fourth Amendment Center is supported by contributions made to the NACDL Foundation for Criminal Justice (NFCJ), a 501(c)(3) charity. The mission of the NFCJ is to preserve and promote the core values of America's justice system guaranteed by the Constitution — among them due process, freedom from unreasonable search and seizure, fair sentencing and effective assistance of counsel — by educating the public and the legal profession to the role of these rights and values in a free society.

How to Support Our Work

You can support our mission and enhance your career by becoming a member of the NACDL or by making a tax-deductible donation to the NFCJ. Learn more by visiting **NACDL.org/Landing/JoinNow** or **NFCJ.org/support**.

About the Fourth Amendment Center

NACDL's Fourth Amendment Center offers direct assistance to defense lawyers handling cases involving new surveillance tools, technologies and tactics that infringe on the constitutional rights of people in America.

The Center is available to help members of the defense bar in bringing new Fourth Amendment challenges. To request assistance or additional information, contact **4AC@nacdl.org**.

NACDL FOURTH AMENDMENT CENTER

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