© meenkulathiamma | AdobeStock

Defending Device Decryption Cases

In the last seven years, the U.S. Supreme Court has issued a trinity of new Fourth Amendment decisions designed to protect privacy rights in the digital age.[1] Two of those opinions, *Riley v. California* and *Carpenter v. United States*, involve modern cellphones, establishing a privacy interest in both the data they contain and the location data they create through third-party service providers.[2] But the Court has not yet had occasion to consider an important corollary: Can the government compel someone to unlock and decrypt a phone or digital device? This is fundamentally a Fifth Amendment question, implicating the right against self-incrimination, but as a practical matter, it may be the surest guarantee of privacy rights. It is also a largely unresolved question that merits the close attention of defense attorneys and rights advocates alike.

When the government has a warrant to search a device that it cannot readily access or decrypt, it may turn to the courts and attempt to compel the device's purported owner to enter or produce the decryption key — typically a passcode, fingerprint, or faceprint. Whether or under what circumstances courts have such authority is a relatively new question, but it is arising with increasing frequency now that encryption has become a standard feature on smartphones.

Case law on "compelled decryption" is frustratingly sparse, however. And the decisions that do exist deploy a variety of standards and have created a divide between federal and state courts around the country. Some cases, for example, treat passcodes differently from biometric keys, while more recent decisions view them as functionally equivalent. Likewise, some courts have set a low bar for invoking Fifth Amendment exceptions, such as the "foregone conclusion" doctrine, while others apply higher standards in the wake of recent Supreme Court guidance. This article will address the technology behind encryption, describe the current state of the law, and suggest strategies for any lawyer seeking to challenge a compelled decryption order.

Background: Device Encryption Today

Encryption uses a mathematical algorithm to encode data in a way that makes it incomprehensible and unreadable until decrypted with an authorized key.[3] An encryption algorithm takes information that can be read by humans, or "plaintext," and converts it into unintelligible characters, or "ciphertext."[4] When the authorized key is entered, the algorithm transforms the ciphertext back into useable, readable form. Without the key, encrypted data stored on a device appears to be random, and it is impossible to tell whether a file contains relevant data or nothing at all.[5] Decryption keys may be numeric or alphanumeric passcodes, or they may be biometric identifiers, like a fingerprint or faceprint.

BY MICHAEL PRICE AND ZACH SIMONETTI

Guessing a passcode can take a prohibitively long time, depending on its length and complexity.[6] Biometric features are similarly difficult to guess,[7] although it is possible to replicate or steal them.[8] Additional security measures present on devices may limit the number of incorrect entries before the device locks down or deletes data.[9] Consequently, the government is often keen to obtain the key, whatever the form.

It is important to recognize, however, that there is a significant difference between unlocking and decrypting devices; the terms are not synonymous. For example, early iPhones could be "locked," but they did not encrypt the data inside, making it possible to read user contents by bypassing the lock. It was not until 2008 that iPhone users had the option to encrypt their devices, making the data not just inaccessible, but also impossible to understand without the proper passcode.[10] In 2014, Apple released a new operating system ("iOS 8"), which provided encryption by default,[11] a feature included on every subsequent iteration. Apple also issues regular operating system updates that strengthen protections and defeat workarounds.[12] Default encryption, protected by a password or biometric key, is now a standard feature of Android devices as well.[13]

The Supreme Court has recognized that mobile phones are "a pervasive and insistent part of daily life."[14] Further, cellphones are particularly unique, because they "faithfully follow[]" their owners "beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales."[15] They also hold sensitive private documents, pictures, videos, or data on usage of the device, including apps and web browsing history. Encryption keeps this sensitive information private. Even if someone steals the device, the thief will not be able to access or read it without the decryption key.

This article addresses only whether individuals can be compelled to decrypt their devices, not the larger debate over requiring "backdoors" for law enforcement to access encrypted data.[16] But in litigating compelled decryption cases, the government's technological capabilities matter. If it has the ability to decrypt, or could reasonably acquire the technology to do so, then compelled decryption should be impermissible given the constitutional rights at stake.

Encryption is as essential to privacy and free speech rights as are locks and envelopes.[17] Encryption facilitates free speech, and it has become part of everyday functions like financial transactions and digital communications.[18] It allows for the safe discussion of ideas among human rights advocates, attorneys and clients, doctors and patients, journalists, and members of vulnerable groups.[19] Indeed, the American Bar Association recommends encrypting communications about confidential or sensitive information and encrypting devices where client information is stored.[20] Encryption should not be seen as an indication of wrongdoing nor as an insurmountable hurdle for law enforcement to overcome in most cases.[21] In fact, there may be no need to compel decryption at all, and any lawyer facing a compelled decryption order should stress the government's alternatives and fight for the future of privacy.

The Fifth Amendment and Compelled Decryption

Courts have only begun to grapple with compelled decryption cases,[22] and the cases do not fit a neat pattern, although many follow a similar trajectory: the government, seeking to search an encrypted smartphone or computer, asks a court to compel the device owner to either enter or provide the decryption key or render the device in a decrypted state.[23] The decryption order may be issued independently or included in a search warrant.[24] This is where the privilege against self-incrimination comes in.

The Fifth Amendment states, in relevant part, that "no person … shall be compelled in any criminal case to be a witness against himself. …"[25] While the Supreme Court has not ruled on compelled decryption specifically, the general rule is that the privilege applies if what the government wants is (1) compelled, (2) incriminating, and (3) testimonial.[26] The "compelled" and "incriminating" prongs are often easily satisfied. Compulsion exists where there is a court order, warrant or subpoena,[27] as is often the situation in compelled decryption cases.[28] Providing information that is inculpatory, or that could lead to the discovery of inculpatory evidence, qualifies as "self-incriminating."[29] Thus, decrypting a device that the government claims to contain incriminating evidence would easily fulfil the second element, as may the act of decryption itself. What is "testimonial," however, is the first major point of disagreement in the existing case law on compelled decryption.[30]

What Is Testimonial?

The Fifth Amendment does not prohibit the compelled production of all incriminating evidence, only evidence that is "testimonial."[31] Thus, for example, it not testimonial to compel "fingerprinting, photographing or measurements, to write or speak identification, to appear in court, to stand, to assume a stance, to walk, or to make a particular gesture" because no "testimonial capacities" of the mind were used by the defendant.[32] The Supreme Court has said that the touchstone is whether someone must "disclose the contents of his own mind,"[33] contrasting an order to produce the combination to a wall safe and an order to surrender the key to a strongbox.[34] But even with this guidance, "the line between testimonial and non-testimonial communications under the Fifth Amendment is not crystal clear."[35]

Furthermore, although analogizing to a safe combination is useful to show the mental process involved in recalling and entering a passcode, it is also important to caution against oversimplification. Like many attempts to compare the digital and the physical worlds, the safe analogy has some intuitive appeal, but it only tells part of the story.[36] Entering the passcode on an iPhone, for example, not only "unlocks" the device, like opening a safe, but it also decrypts the data stored on the device, translating it from gibberish back into intelligible content. It would be as if a suspect were not only compelled to enter the combination to a wall safe, but also had to explain or translate any documents inside for the benefit of government investigators.[37] On modern iPhones, the functions are inextricably linked — the passcode helps generate the encryption cypher. Technically speaking, a passcode "provides entropy for certain encryption keys," so "the stronger the user passcode is, the stronger the encryption key becomes."[38] In short, a passcode not only unlocks the device, but also makes use of the contents of the suspect's mind to translate the data for the government, making it an intrinsically testimonial act.[39]

The Supreme Court has held that the definition of "testimonial" extends beyond oral communications to include certain communicative acts as well. For

example, in *United States v. Hubbell* the Court recognized that "the act of producing documents in response to a subpoena may have a compelled testimonial aspect."[40] The Justices found that compelling the production of 11 categories of documents in response to a subpoena was testimonial because it would effectively "admit the papers existed, were in [the subject's] possession or control, and were authentic."[41] Similarly, in the context of digital devices, the act of decryption is likely to demonstrate access to the device as well as knowledge, possession, and control of its contents.[42] For example, *In re Grand Jury* tracked the reasoning in *Hubbell,* finding that compelling the defendant to use his password to decrypt a device was testimonial because it demanded the "use of the contents of the mind" and implied factual statements like control, possession, and authenticity of the purported evidence.[43]

Despite seemingly widespread recognition that decryption may be an act of production, strong disagreement exists about when, if ever, that act is sufficiently testimonial for Fifth Amendment purposes. Some courts treat compelling a passcode as testimonial, analogizing it to producing the combination for a wall safe; others do not. Some courts treat biometric keys as equivalent to passcodes; others liken them to taking a fingerprint or mug shot. Consequently, successfully asserting the privilege against self-incrimination may hinge on the type of lock and key used, as discussed next.

Numeric or Alphanumeric Passcodes

The Eleventh and Third Circuits are the only federal courts of appeals to have ruled on compelled decryption, and both found that the compulsion of an alphanumeric or numeric passcode is potentially testimonial.[44] In 2012, the Eleventh Circuit reasoned that entering a passcode requires an individual to use his mental processes.[45] The defendant was being compelled to produce unencrypted files, not simply the passcode, but the court held that doing so required the defendant to use his password and was testimonial because it demands both "the use of the contents of the mind, and the production is accompanied by the implied factual statements … that could prove to be incriminatory."[46]

State and federal district courts have adopted similar reasoning. In *G.A.Q.L. v. State,* a Florida court found the production of a device's password to be testimonial because it "probes into the contents of an individual's mind and therefore implicates the Fifth Amendment."[47] Likewise, in *United Sates v. Kirschner*, a Michigan federal court found that the government could not force the defendant to "divulge through his mental processes his password."[48]

In one instance, a Florida state court found that compelling a passcode is not testimonial because complying does not use sufficient mental energy.[49] In *State v. Stahl*, the court reasoned that for the Fifth Amendment to apply, the contents of the defendant's mind must be "extensive[ly] use[d]" when responding to a subpoena.[50] The court did not elaborate on what "extensively" means, but applying *Stahl*'s reasoning could lead to potentially absurd results. Would a passcode of four numeric digits receive less protection than an alphanumeric passcode 25 characters long? Further, *Stahl* found that the act of providing the passcode would not acknowledge that the phone contained incriminating evidence,[51] but failed to recognize that doing so would communicates one's control over and previous use of the device.

Most recently, however, a third Florida appeals court opted to follow *G.A.Q.L* and the Eleventh Circuit instead of *Sthal*.[52] In *State v. Pollard,* the court reasoned that, "Forcing a defendant to disclose a password, whether by speaking it, writing it down, or physically entering it into a cellphone, compels information from that person's mind and thereby falls within the core of what constitutes a testimonial disclosure."[53]

Biometric Decryption Keys

When Apple released the iPhone 5S in 2013, it had a new security feature — the option to use a "Touch ID" fingerprint recognition sensor to unlock and decrypt the device.[54] Touch ID marked the first widespread use of biometric decryption keys, but they are now a standard feature on many modern smartphones. Most recently, Apple introduced "Face ID," which uses facial recognition to generate a Face ID key that can act in place of a traditional alphanumeric code or Touch ID lock.[55] These developments are relatively new, so cases involving biometric locks have only begun to work their way through the courts. Nonetheless, there is already a split in the law, as some recent opinions have started to equate passcodes and biometric keys.

Many of the first courts to consider the issue found that there is nothing testimonial about producing a fingerprint for the purpose of unlocking and decrypting a device, citing the lack of mental processes involved.[56] In 2014, for example, a Virginia state court held that a passcode is testimonial for Fifth Amendment purposes, but found that a fingerprint does not implicate a defendant's Fifth Amendment privilege against self-incrimination.[57] The Supreme Court of Minnesota reached a similar conclusion in *State v. Diamond* in 2018, struggling to determine the testimonial nature of a fingerprint in this context.[58] Ultimately, the *Diamond* court decided that taking a fingerprint to unlock a cellphone was non-testimonial because unlocking a device is "not evidence of [the] mind's thought process."[59] And just last year, in *Matter of Search of [Redacted] Washington, District of Columbia*, the government obtained a warrant to search a location and compel anyone present to unlock any digital devices seized using biometric features.[60] The court ruled that compelled decryption using the fingerprint sensor is akin to the compelled production of other physical characteristics that are generally not testimonial, like voice and handwriting exemplars, as they do not reveal the contents of the subject's mind.[61]

More recently, however, some courts have begun to find biometric decryption to be testimonial. In *Matter of Residence in Oakland, California,* the court denied a warrant application, similar to the one in Washington, D.C., that would have authorized police to use the fingerprints of any resident at the premises to unlock any electronic devices discovered.[62] The court reasoned that biometric keys "serve the same purpose of a passcode … rendering them functionally equivalent."[63] Just like a passcode, the act of biometric decryption "concedes that the phone was in the possession and control of the suspect, and authenticates ownership or access to the phone and all of its digital contents."[64] This act authenticates the device's contents, the court continued, in a way that "far exceeds the 'physical evidence' created when a suspect submits to fingerprinting."[65]

A district court in Illinois came to a similar conclusion in 2017.[66] The court felt that by successfully unlocking the device with a fingerprint, the "suspect is testifying that he or she has accessed the phone before … and that he or she currently has some level of control over or relatively significant

connection to the phone and its contents."[67] And in May 2019, an Idaho district court embraced the Illinois opinion, finding a warrant that compelled the production of the defendant's fingerprint to unlock his Google Pixel smartphone to be unconstitutional under the Fifth Amendment.[68] The Idaho court reasoned that "the government seeks evidence that the individual's fingerprint unlocks the phone not simply to access its contents but also to establish the individual's possession and control of the phone and knowledge of its contents."[69] Significantly, the Idaho court also found a Fourth Amendment violation as a result of the Fifth Amendment violation, holding that "because the compelled use of the individual's fingerprints violates the Fifth Amendment, the search and seizure would not be reasonable under the Fourth Amendment."[70]

The California, Illinois, and Idaho cases highlight how some courts are coming to understand the testimonial significance of unlocking and decrypting a device with a fingerprint.

The widening split on biometric decryption underscores the importance of understanding how encryption operates as well as the difficulty of applying old doctrines to the digital world.

While it is a physical characteristic, a fingerprint that successfully unlocks a device communicates a plethora of information to law enforcement, including a deep familiarity with the basic functions of the device. Indeed, before setting up Touch ID or Face ID the user must create a numeric or alphanumeric passcode for the device.[71] While biometric keys can be alternatives for unlocking the device, a passcode is still required when restarting an Apple device or changing passcode settings, linking a fingerprint to knowledge of the passcode.[72] This is an indication of significant control over device functions like updates and restarts, as well as any purchases made using fingerprint verification. Thus, the successful use of a biometric key communicates control over the device, showing that the individual set it up and created a passcode that is vital to the device's most basic functions.

The widening split on biometric decryption underscores the importance of understanding how encryption operates in practice as well as the difficulty of applying old doctrines to the digital world. New advances in technology will continue to complicate the analysis and reveal the limitations of simple analogies to the physical world.

The Foregone Conclusion Exception

Even if compelling a passcode or biometric key is potentially testimonial, some courts have invoked the "foregone conclusion" doctrine to conclude that there is no Fifth Amendment violation.[73] First articulated by the Supreme Court in *Fisher v. United States,* the doctrine works as an exception to the privilege against self-incrimination, applicable when the existence and location of particular documents are a "foregone conclusion" and the testimony adds "little or nothing to the sum total of the government's information by conceding that he in fact has the papers."[74] In *Fisher,* decided in 1976, the government sought to compel a defendant to produce accounting documents in the possession of his attorney.[75] The Court found that the act of production could not be considered testimonial because the government knew both the contents and location of the tax documents, making it a question "not of testimony but of surrender."[76]

It is important to emphasize, however, that the Supreme Court has never applied the foregone conclusion doctrine in the compelled decryption context. Indeed, it has never applied the exception to anything other than paper business documents. Rather, the *Fisher* Court explicitly cautioned against applying it to more obviously private information, like a personal diary.[77] An order to compel such materials might present "[s]pecial problems of privacy," the Court explained, or implicate First Amendment values that were not involved in *Fisher*.[78]

Thus, any challenge to a decryption order should begin by arguing that the foregone conclusion doctrine simply does not apply to digital devices, in keeping with the Court's warning in *Fisher* as well as the Justices' recent and repeated recognition that cellphones are not like ordinary closed containers or physical objects.[79] In *Riley v. California*, decided in 2014, the Court declined to apply the longstanding search-incident-to-arrest rule to cellphones, citing their capacity to contain the "privacies of life."[80] And in *Carpenter v. United States*, decided in 2018, the Court declined to apply the so-called "third-party doctrine" to historical cellphone location information, recognizing once again that, at least for Fourth Amendment purposes, digital is different.[81] 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 in *Fisher*. Counsel should therefore be sure to argue that the foregone conclusion doctrine should not apply to device decryption, just as the Court declined to apply the old rules in *Riley* and *Carpenter*.

Assuming, however, that the foregone conclusion doctrine applies generally to digital devices, the question is how. Once again, courts are split. The Eleventh Circuit employs the "reasonable particularity" test from *In Re Grand Jury Subpoena*, which requires the government to show with reasonable particularly that the evidence it seeks exists, is in a specific location, and is authentic.[82] In that case, the government failed to show it knew the location of the data, and government forensic examiners admitted that they could not say with certainty that any information existed on the seized devices at all.[83] Thus, the Eleventh Circuit held that the foregone conclusion exception did not apply to production of the defendant's passcode.

This is a highly fact-specific test, as illustrated by the Third Circuit in 2017. In *United States v. Apple MacPro Computer*, the Third Circuit applied the reasonable particularity standard from the Eleventh Circuit, but it came to the opposite result on the facts. Unlike the Eleventh Circuit, the facts indicated that the defendant's sister watched him decrypt his computer to show her videos of child pornography on the computer in question.[84] As a result, the Third Circuit found that the government already knew with reasonable particularity that the evidence existed on the encrypted device, and that the defendant had custody and control over it, making the act of decryption a foregone conclusion.[85] By contrast, in Florida the *Pollard* court applied the same test but found that the evidentiary record was "too thin"

for the foregone conclusion exception to apply.[86] The court reasoned that "unless the state can describe with reasonable particularity the information it seeks to access on a specific cellphone, an attempt to seek all communication data and images amount[s] to a mere fishing expedition."[87]

Some courts have taken a markedly different approach, rejecting the Eleventh Circuit's reasonable particularity test and requiring the government to show only that an individual is able to unlock and decrypt his device.[88] In *United States v. Spencer*, for example, a California district court reasoned that because the government was asking the defendant to turn over entire decrypted devices, and not particular files, the government "need only show it is a foregone conclusion that [the defendant] has the ability to decrypt the device" by "clear and convincing evidence."[89] The *Spencer* decision contends that the Eleventh Circuit's test is faulty, as it would make it too difficult for the government to compel a password from a defendant.[90]

At least one state court has adopted a similar framework for the foregone conclusion in the decryption context.[91] In *Commonwealth v. Jones*, the Supreme Judicial Court of Massachusetts crafted a slightly stricter version of *Spencer*'s "clear and convincing" test, upping the standard to "beyond a reasonable doubt" that the defendant can unlock and decrypt the device.[92] By doing so, the court said it hoped to reduce the "risk of incorrectly imputing knowledge to those defendants who truly do not know the password."[93] But even this standard risks reducing the Fifth Amendment to a mere formality.[94]

The reality is that people generally know the passcode to their own cellphones and computers, making it trivial to prove in many cases, either by "clear and convincing" evidence or "beyond a reasonable doubt." As a result, the rules in *Spencer* and *Jones* effectively shift the goal posts far up the field from *Fisher*, *Hubble*, and the "reasonable particularity" test employed by the Eleventh and Third Circuits. Whereas the Eleventh Circuit would require the government to "describe with reasonable particularity" the files it seeks to access, *Spencer* and *Jones* simply require showing that people know the passcode to their phones. In effect, this is no test at all, and counsel should argue it is not the correct test to use, assuming the foregone conclusion doctrine applies.

Is Compelled Decryption Necessary or Appropriate?

Federal courts have the authority to compel production of evidence under the All Writs Act,[95] which may include a decryption order in aid of a valid search warrant where "necessary or appropriate."[96] But what is "necessary or appropriate" in the context of compelled decryption is an open question. Generally speaking, the government must have no other adequate means of relief to which it is indisputably entitled.[97] Thus, assuming the government has a right to the decrypted contents of a device, it still may not compel a defendant to decrypt it if law enforcement has the technological capability to do so as well.[98]

The government's technical capabilities currently depend on the services of two private companies, Cellebrite and GrayShift, which are in the midst of a digital arms race with device manufacturers like Apple.[99] These companies boast the ability to unlock and decrypt any cellphone on the market today despite continuing efforts to keep them out.[100] While the most advanced tools can be expensive for law enforcement to use or acquire,[101] it is usually feasible for the government to do so, and counsel should be wary of any assertions to the contrary.[102] Older devices are far less expensive to unlock, and well worth the cost to preserve Fifth Amendment rights in the digital age. In sum, an order compelling decryption is not "necessary or appropriate" if the government has other viable means of decrypting the device.

Challenging State Court Jurisdiction

Whereas federal courts may invoke the All Writs Act, state courts may lack any analogous statutory authority. Some state provisions may permit courts to compel the production of certain types of physical evidence, but as discussed, passcodes and biometric keys are a far cry from mere physical evidence.[103] Consequently, some state courts may lack the jurisdiction to issue a compelled decryption order altogether. Counsel in state cases should therefore be sure to ascertain whether local courts have the authority to issue decryption orders in the first instance.

Conclusion

In this digital age, when the private and intimate details of daily life are recorded in intricate detail, and the complexity of digital devices makes it difficult to apply old analogies, the patchwork of standards in the compelled decryption context illustrates how difficult it can be to figure out how new technologies should be viewed under the Constitution. Fingerprint-based decryption keys became a standard smartphone feature before most courts had a chance to consider the Fifth Amendment implications of compelling a numeric passcode. And while courts began to grapple with fingerprint keys, Apple replaced them with Face ID.[104] Some courts have appreciated the constitutional significance of these developments more than others, but despite these bright spots, attorneys must be diligent to prevent technologic advances from undercutting the Fourth and Fifth Amendments.

Editor's Note: It is essential for criminal defense attorneys to stay up to date on the latest technological advances and legal strategies for challenging the government when it seeks to gain access to a client's digital device. NACDL's Fourth Amendment Center provides *pro bono* litigation assistance to defense attorneys for building the strongest legal arguments to prevent the government from diminishing privacy rights in digital devices. A three-page primer and case list on compelled decryption are also available on NACDL's website.[105]

Notes

1. *Carpenter v. United States,* 138 S. Ct. 2206 (2018); *Riley v. California,* 573 U.S. 373 (2014); *United States v. Jones*, 565 U.S. 400 (2012).

2. *Riley,* 573 U.S. 373 (holding that the warrantless search and seizure of a cellphone and its digital contents during an arrest is unconstitutional); *Carpenter,* 138 S. Ct. 2206 (holding that a warrant is required before compelling a wireless carrier to turn over more than six days of a subscriber's historical cell site location information).

3. *See* Kevin Stine & Quynh Dang, *Encryption Basics,* National Institute of Standards and Technology, (May 2, 2011), https://www.nist.gov/publications/encryption-basics; *See also* Nicholas G. McDonald, *Past Present, and Future Methods of Cryptography and Data Encryption,* Department of Electrical and Computer Engineering, University of Utah (last accessed May 9, 2019), https://pubweb.eng.utah.edu/~nmcdonal/Tutorials/EncryptionResearchReview.pdf.

4. Aloni Cohen & Sunoo Park, *Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries,* 32 Harv. J.L. & Tech 169 (2018).

5. *Id.* at 179 (While one could be looking at a chest and insist that the subject turn over the key, the chest "is

instead a solid block of wood carved to look like a chest — and so could not possibly contain anything at all.").

6. The longer a passcode, and more complex its make-up, the longer it will take to crack by brute force. On average, it would take 12 years to crack a 10-digit password. *See* Lorenzo Franceschi-Bicchierai, *Stop Using 6-Digit iPhone Passcodes,* Motherboard (Apr. 16, 2018 4:56 PM), https://www.vice.com/en_us/article/59jq8a/how-to-make-a-secure-iphone-passcode-6-digits.

7. Nilesah A. Lal et al., *A Review of Authentication Methods,* 5 Int'l J. Sci. & Tech. Res. 246 (2016) (discussing the pros and cons of different authentication methods).

8. Kaveh Waddell, *When Fingerprints Are as Easy to Steal as Passwords,* The Atlantic (Mar. 24,2017), https://www.theatlantic.com/technology/archive/2017/03/new-biometrics/520695.

9. Avery Hartmans, *There's a Scary iPhone Feature That Erases All Your Data After Too Many Password Attempts — Here's Why You Should Turn It on Anyway,* Business Insider (Dec. 16, 2018, 3;10 PM), https://www.businessinsider.com/iphone-security-failed-passcode-attempts-2018-6.

10. Elizabeth Weise, *What Does It Mean That a Phone Is Encrypted?* USA Today (Feb. 20, 2016) https://www.usatoday.com/story/tech/news/2016/02/20/phone-encryption-iphone-apple-qa/80623208/.

11. Kevin Poulsen, *Apple's iPhone Encryption Is a Godsend, Even If Cops Hate It,* Wired (Oct. 10, 2014) https://www.wired.com/2014/10/golden-key.

12. *See Apple Security Updates,* Apple Support, https://support.apple.com/en-us/HT201222.

13. Android devices will often recommend file-based encryption that allows different files to be encrypted with different keys that can be unlocked independently. Android 5.0 and above support full-disk encryption, but it is not the default method of encryption. *See* https://source.android.com/security/encryption; *see also* https://support.google.com/pixelphone/answer/2844831?hl=en.

14. *Riley*, 573 U.S. 373 at 385 (2014). More than 95 percent of Americans now own a cellphone of some kind, and more than 75 percent of Americans own smartphones. *See* Mobile Fact Sheet, Pew Research Center (Feb. 5, 2018), https://www.pewinternet.org/fact-sheet/mobile.

15. *Carpenter,* 138 S. Ct. 2206, at 2218 (2018).

16. *See, e.g.,* Office of the Inspector General, *A Special Inquiry Regarding the Accuracy of FBI Statements Concerning Its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attacks Investigation,* Mar. 2018, https://oig.justice.gov/reports/2018/o1803.pdf; Nate Cardozo & Andrew Crocker, *The FBI Could Have Gotten Into the San Bernardino Shooter's iPhone, but Leadership Didn't Say That,* Electronic Frontier Foundation (April 2, 2018), https://www.eff.org/deeplinks/2018/04/fbi-could-have-gotten-san-bernardino-shooters-iphone-leadership-didnt-say; Amie Stepanovich & Michael Karanicolas, *Why an Encryption Backdoor for Just the 'Good Guys' Won't Work,* Just Security (Mar. 2, 2018), https://www.justsecurity.org/53316/criminalize-security-criminals-secure.

17. *Encryption: A Matter of Human Rights,* Amnesty Int'l (Mar. 2016), https://www.amnestyusa.org/wp-content/uploads/2017/04/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf.

18. Andi Thompson, *The Human Rights Benefits of Encryption,* New America Open Technology Institute blog post, (Mar. 2, 2015), https://www.newamerica.org/oti/blog/the-human-rights-benefits-of-encryption/.

19. Emma Llanso, *UN Report: Encryption and Anonymity Tools Essential to Expression Online,* Center for Democracy & Technology (June 17, 2015), https://cdt.org/blog/un-report-encryption-and-anonymity-tools-essential-to-free-expression-online.

20. American Bar Association, *Securing Communication of Protected Client Information,* Formal Opinion 477 (May 4, 2017), https://www.americanbar.org/content/dam/aba/images/abanews/FormalOpinion477.pdf.

21. Devlin Barrett, *FBI Repeatedly Overstated Encryption Threat Figures to Congress, Public,* Wash. Post (May 22, 2018), https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html.

22. The earliest reported decryption cases begin with *United States v. Pearson,* 1:04-CR-340, 2006 WL 8442594 at* 3 (N.D. N.Y. May. 24, 2006) (compelling the defendant to produce "all passwords, keys, and/or log-ins used to encrypt any and all files") and *In re Boucher,* No. 2:06-mj-91, 2007 WL 4246473 (D. Vt. Nov. 29, 2007), *appeal granted, decision rev'd*, No. 2:06-MJ-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009) (finding that the defendant could not be compelled to provide the password to his encrypted computer) which was later appealed and reversed.

23. *United States v. Kirschner,* 23 F. Supp. 2d 665, 666 (E.D. Mich. 2010) (reveal the password); *In re Grand Jury Subpoena,* 670 F.3d 1335 (11th Cir. 2012) (defendant compelled to produce the decrypted contents); *Commonwealth v. Gelfgatt*, 11 N.E.3d 605 (Mass. 2014) (compelling defendant to enter the password to unlock

and decrypt his device); *see also* Aloni Cohen & Sunoo Park, *Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries,* 32 Harv. J.L. & Tech 169 (2018).

24. Cases in which the warrant allowed for the compulsion of passwords or biometric keys include *In Re Application for a Search Warrant*, 236 F. Supp. 3d 1066 (N.D. Ill. 2017); *Matter of Search of [Redacted] Washington, D.C.*, 317 F. Supp. 3d 523 (D.D.C. 2018). Cases in which the defendant was ordered to produce the passcode or decrypted contents include *United States v. Apple MacPro Computer*, 851 F.3d 238 (3d Cir. 2017); *United States v. Spencer,* No. 17-cr-00259-CRB-1 (N.D. Cal. April 26, 2018); and *United States v. Friscosu,* 841 F. Supp. 2d 1232 (D. Colo. 2012).

25. U.S. Const. amend. V.

26. *Hiibel v. Sixth Judicial Dist. Court of Nevada, Humbolt County,* 542 U.S. 177 (2004). *See also United States v. Hubbell,* 530 U.S. 27 (2000).

27. *See Matter of Search of [Redacted] Washington, D.C.,* 317 F. Supp. 3d at 534 ("In that sense, the government's warrant was obviously compulsive."); *Commonwealth v. Baust,* 89 Va. Cir. 267, 2014 WL 10355635 at *2 (Va. Cir Ct. 2014) ("Additionally, there is no question that a motion to compel is compulsive and the production of the passcode or fingerprint would be incriminating."): *see also Hubbell*, 530 U.S. at 36-37 (finding that a subpoena to produce 11 categories of documents was compelled and testimonial under the privilege against self-incrimination).

28. Compulsion also exists in the context of an interrogation where "the free will of the witness was overborne" and the information is not given voluntarily. *See United States v. Washington*, 431 U.S. 181, 188 (1997); *United States v. Maffei,* No. 18-CR-00174-YGR-1, 2019 WL 1864712, at *6 (N.D. Cal. Apr. 25, 2019) (offering a robust analysis of the compulsion and self-incriminating elements in an interrogation context).

29. *Id.* at *5; *Hubbell,* 530 U.S. at 37-38 (quoting *Hoffman v. United States*, 341 U.S. 479, 486 (1951)).

30. That is to say, the definition of "testimonial" has not been clearly defined by the Supreme Court in the context of technological advances like encryption and decryption keys.

31. *Fisher v. United States,* 425 U.S. 391 (1976).

32. *Schmerber v. California,* 384 U.S. 757, 764 (1966).

33. *Curcio v. United States,* 354 U.S. 118 (1957).

34. *Doe v. United States,* 487 U.S. 201, 210 n.9 (1988).

35. Matter of Search of [Redacted] Washington, D.C., 317 F. Supp. 3d 523, 535 (D.D.C. 2018).

36. *See, e.g.,* Jeffrey Kiok, *Missing the Metaphor: Compulsory Decryption and the Fifth Amendment*, 24 B.U. Pub. Int. L.J. 53, 77 (2015).

37. Additionally, when the entire device is encrypted, it is impossible to distinguish user-created data from blank space. See Cohen & Park, *supra* note 4. To carry the analogy further, without the additional step of decryption, investigators would be unable to determine if the safe contained documents of importance, irrelevant information, or nothing at all. *See generally* Jeffrey Kiok, *Missing the Metaphor: Compulsory Decryption and the Fifth Amendment*, 24 B.U. Pub. Int. L.J. 53, 57-59 (2015).

38. Apple, Inc., iOS Security (Nov. 2018) at 18, https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf (last accessed May 17, 2019).

39. *See* Brief of Electronic Frontier Foundation, American Civil Liberties Union, and ACLU of the District of Columbia as Amici Curiae in Support of the Appellee, *United States v. Mitchell II*, 76 M.J. 413 (C.A.A.F. 2017).

40. 530 U.S. 27, 36 (2000).

41. *Id.*

42. *See In Re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335 (11th Cir. 2012) (reasoning that "production would be tantamount to testimony by Doe 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"); *see also In Re Application for a Search Warrant*, 236 F. Supp. 3d 1066 (N.D. Ill. 2017) (finding that "[w]ith a touch of a finger, a suspect is testifying that he or she has accessed the phone before, at a minimum, to set up the fingerprint password capabilities, and that he or she currently has some level of control over or relatively significant connection to the phone and its contents.").

43. 670 F.3d 1335, 1345-46 (11th Cir. 2012).

44. The Third Circuit mainly punted on explicitly deciding the testimonial nature of the passcode. Noting that the magistrate judge found that the Fifth Amendment may be implicated by the defendant's decryption of the devices, the court instead focused on whether the magistrate court had correctly applied the foregone conclusion rule. While implicitly adopting the Eleventh Circuit's test for the foregone conclusion exception, the Third Circuit came to a different conclusion reasoning that "[u]nlike *In Re Grand Jury Subpoena,* the government has provided evidence to show both that files exist on the encrypted portions of the devices and that [defendant] can access them." *United States v. Apple MacPro Computer,* 851 F.3d 238, 248 (3d Cir. 2017).

45. *In Re Grand Jury Subpoena Duces Tecum,* 670 F.3d 1335 (11th Cir. 2012).

46. *Id.* at 1346 (referencing aspects like control, authenticity, and previous access to the device that is inferred if one can open the device with a password).

47. 257 So. 3d 1058, 1061 (Fla. Dist. Ct. App. Oct. 24, 2018).

48. 823 F. Supp. 2d 665, 666 (E.D. Mich. 2010).

49. *See State v. Stahl*, 206 So. 3d 124 (Fla. Dist. Ct. App. 2016).

50. *Id.* at 133-34 (*citing Hubbell,* 530 U.S. at 28. It is important to note that in the language cited from *Hubbell,* the Court was not promulgating a standard for determining what is testimonial, but was critiquing the government's argument that the defendant's granted immunity did not preclude the government from using produced documents because its possession of the documents was the "fruit only of a simple physical act — the act of producing the documents.").

51. *Id.* at 134.

52. *Pollard v. State*, No.1D18-4572, 2019 WL 2528776, at *1 (Fla. Dist. Ct. App. June 20, 2019).

53. *Id.* at *2.

54. *Apple Announces iPhone 5s — The Most Forward-Thinking Smartphone in the World,* Apple Newsroom (Sept. 10, 2013), https://www.apple.com/newsroom/2013/09/10Apple-Announces-iPhone-5s-The-Most-Forward-Thinking-Smartphone-in-the-World.

55. *Use Face ID on Your iPhone or iPad Pro,* Apple Support, https://support.apple.com/en-us/HT208109.

56. *See, e.g., Commonwealth v. Baust*, 89 Va. Cir. 267, 2014 WL 10355635 (Va. Cir. Ct. 2014); *State v. Diamond*, 905 N.W.2d 870, 878 (Minn. 2018) (holding that "because the compelled act merely demonstrated [defendants] physical characteristics and did not communicate assertation of fact from [defendants] mind" there was no testimonial communication protected by the Fifth Amendment.); *United States v. Maffei*, No. 18CR00174, 2019 WL 1864712, at *5 (N.D. Cal. 2019) (holding that a passcode is testimonial, but a fingerprint is non-testimonial).

57. *Baust*, 2014 WL 10355635 at *4.

58. *State v. Diamond*, 905 N.W.2d 870 (Minn. 2018). The court noted a distinction between the testimonial production of documents and the non-testimonial compulsion of physical acts, but said that "the act here — providing the police a fingerprint to unlock a cellphone — does not

fit neatly into either category." *Id.* at 875-76.

59. *Id.* at 875.

60. *Matter of Search of [Redacted] Washington*, D.C., 317 F. Supp. 3d 523 (D.D.C. 2018) (more specifically, the government sought authorization to "compel biometric features of an individual believed to have perpetrated the alleged offenses under investigation in connection with any biometric recognition sensor-enabled digital device.").

61. *Id.* at 536. Citing *Gilbert v. California,* 388 U.S. 218 (1967) (holding that a handwriting exemplar is non-testimonial); *United States v. Wade,* 388 U.S. 218 (1967) (holding use of voice exemplar in lineup non-testimonial).

62. *Matter of Residence in Oakland*, California, 354 F. Supp. 3d 1010, 1013 (N.D. Cal. 2019).

63. *Id.* at 1015.

64. *Id.* at 1016.

65. *Id.*

66. *In Re Application for a Search Warrant*, 236 F. Supp. 3d 1066 (N.D. Ill. 2017).

67. *Id.* at 1073. The district court also specifically took issue with the lack of particularity in the warrant, which did not identify the devices to be seized, in violation of the Fourth Amendment's particularity requirement. *Id.* at 1067.

68. *In the Matter of the Search of a White Google Pixel 3 XL Cellphone,* No. 1:19-mj-10441, 2019 WL 2082709, at *1 (D. Idaho May 8, 2019).

69. *Id.* at *4.

70. *Id.* at *1.

71. *See Set up Face ID,* Apple Support, https://support.apple.com/en-us/HT208109; *Set up Touch ID,* Apple Support, https://support.apple.com/en-us/HT201371.

72. *Use a Passcode with Your iPhone, iPad, or iPod Touch,* Apple Support, https://support.apple.com/en-us/HT204060.

73. *See United States v. Apple MacPro Computer*, 851 F.3d 238 (3d Cir. 2017); *Commonwealth v. Jones*, 481 Mass. 540 (2019); *United States v. Spencer*, No. 17-cr-00259-CRB-1, 2018 WL 1964588 (N.D. Cal. April 26, 2018).

74. 425 U.S. 391, at 411 (1967); *Commonwealth v. Baust*, 89 Va. Cir. 267 (Va. Cir. Ct. 2014).

75. *Id.* at 391-92.

76. *Id.* at 411.

77. *Id.* 425 U.S. 391, 401 & n.7 (1976) (citing *United States v. Bennett*, 409 F.2d 888, 897 (2d Cir. 1969)).

78. *Id.*

79. See *Riley v. California*, 134 S. Ct. 2473, 2491 ("[A] cellphone search would typically expose to the government far more than the most exhaustive search of a house."); *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018) (requiring a warrant for historical cellphone location information).

80. *Riley*, 134 S. Ct. at 2495.

81. *Carpenter*, 138 S. Ct. at 2220; *see also* Michael Price, *Carpenter v. United States and the Future Fourth Amendment,* The Champion, June 2018, at 48; Michael Price & Bill Wolf, *Building on Carpenter: Six New Fourth Amendment Challenges Every Defense Lawyer Should Consider,* The Champion, Dec. 2018, at 20.

82. 670 F.3d at 1346 (After the grand jury sought to compel the password to a defendant's digital devices taken pursuant to a valid warrant, the defendant invoked his privilege against self-incrimination. The government failed to offer evidence that it knew what incrimination data, if any, were held on the devices it seized, thus failing to meet the foregone conclusion test.).

83. *Id.* at 1340.

84. *Apple MacPro Computer*, 851 F.3d 238, 242-243 (3d Cir. 2017).

85. *Id. See also In re Boucher,* No. 2:06-MJ-91, 2009 WL 424718 at *3-4 (The *Boucher* court held that the foregone conclusion exception applied. In that case a customs official viewed child pornography during the initial search of the defendant's computer in the presence of the defendant after he admitted the computer was his, but was later unable to access the desired files after shutting the computer because they were encrypted. The court found that the foregone conclusion exception applied because the border agent had viewed the pornographic material on the defendant's drive, and thus the questions of authentication and ownership were not at issue.).

86. *Pollard*, 2019 WL 2528776, at *5.

87. *Id.*

88. *See United States v. Spencer*, No. 17-cr-00259-CRB-1, 2018 WL 1964588 (N.D. Cal. April 26, 2018).

89. *Id.* at *2.

90. *Id.* ("[A] rule that the government can never compel decryption of a password-protected device would lead to absurd results.").

91. *See Commonwealth v. Jones*, 481 Mass. 540 (2019) (holding that the government could compel the production of the defendant's password under the foregone conclusion test if the government could show beyond a reasonable doubt that the defendant knew the password.).

92. *Id.* at 551 The *Jones* Court decided that the foregone conclusion exception applied because the government was able to show that the defendant could unlock his devices based on his possession of the phone, his name on the phone's subscriber information, a witness's statements that she had contacted the defendant on the phone, and other "reasonable inferences" that the defendant knew the password to his device. *Id.* at 557-58.

93. *Id.* at 555.

94. *See* Michael Price & Zach Simonetti, *Split Over Compelled Decryption Deepens with Massachusetts Case,* Just Security (Apr. 30, 2019), https://www.justsecurity.org/63827/split-over-compelled-decryption-deepens-with-massachusetts-case.

95. All Writs Act, 28 U.S.C.A. § 1651 (West). The All Writs Act allows federal courts to issue "all writs necessary or appropriate in aid of their respective jurisdiction." In *Spencer*, for example, the government applied for an order under the All Writs Act. 2018 WL 1964588 at *1.

96. *See, e.g., Apple MacPro Computer,* 851 F.3d 238, 245 (3d Cir. 2017) (federal courts may issue an All Writs Act order as may be necessary or appropriate to effectuate and prevent the frustration of orders it has issued previously in exercise of jurisdiction otherwise obtained); *see also Spencer,* 2018 WL 1964588 at *1; *United States v. Friscosu,* 841 F. Supp. 2d 1232 (D. Colo. 2012).

97. *United States v. New York Tel. Co.*, 434 U.S. 159, 161 (1977) (requiring the phone company to assist in installation of pen registers); *see also* § 51:208. Construction of "necessary or appropriate," 21A Fed. Proc., L. Ed. § 51:208.

98. Likewise, the government may not

(Continued on page 63)

(Continued from page 52)

have the right to compel a company like Apple to build a "backdoor" to its iPhone security features if other options are available to the government or within its reach. *See* Brief of *Amici Curiae*, *In the Matter of the Search of an Apple iPhone,* Counsel for *Amici Curiae* Electronic Frontier Foundation and 46 Technologists, Researchers, and Cryptographers, *In the Matter of the Search of an Apple iPhone,* No. 16-cm-0010-SP (C.D. Cal. Mar. 22, 2016).

99. *See, e.g.*, Thomas Brewster, *Apple Just Killed the 'GreyKey' iPhone Passcode Hack,* Forbes (Oct. 24, 2018), https://www.forbes.com/sites/thomasbrewster/2018/10/24/apple-just-killed-the-graykey-iphone-passcode-hack/#5301fe595318.

100. *See, e.g.,* Mikey Campbell, *GrayShift Claims It Defeated Apple's Forthcoming 'USB Restricted Mode' Security Feature,* Apple Insider (June 14, 2018), https://appleinsider.com/articles/18/06/14/grayshift-claims-it-defeated-apples-forthcoming-usb-restricted-mode-security-feature and Thomas Brewster, *The Feds Can Now (Probably) Unlock Every iPhone Model in Existence,* Forbes (Feb. 26, 2018), https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/#9b41da1667a0.

101. GrayShift offers a model of its GrayKey product for $30,000 that allows for unlimited iPhone unlocks and a version for $15,000 that permits 300 uses. https://www.forbes.com/sites/thomasbrewster/2018/03/05/apple-iphone-x-graykey-hack/#7683b3a2950f; Cellebrite UFED extraction models can range between $2,499 and $15,999 depending on the version desired. *See, e.g.*, Product Information: Cellebrite UFED Series, SC Magazine (Oct. 1, 2015), https://www.scmagazine.com/review/cellebrite-ufed-series.

102. In *Apple v. FBI*, the government sought to compel Apple to bypass its own encryption security features despite the fact that it was aware a private company, widely believed to be Cellebrite, was "90 percent of the way toward a solution" that had been in the works for many months. Office of the Inspector General, *A Special Inquiry Regarding the Accuracy of FBI Statements Concerning Its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attacks Investigation*, Mar. 2018, https://oig.justice.gov/reports/2018/o1803.pdf at 3. The government did not convey this information to the court, insisting that the FBI was unable to access the phone, as revealed in a subsequent investigation by the Inspector General for the Department of Justice. *Id.* After failing to compel Apple's compliance in court, the FBI purchased the necessary technology within a week, obtained access to the phone in question, and sought to vacate the Apple order. *Id.*

103. *See Riley,* 573 U.S. at 396-397; *Carpenter* 138 S. Ct. at 2222.

104. *See* Edgar Alvarez, *Apple's Face ID Replaces Touch ID on the iPhone X,* Engadget, https://www.engadget.com/2017/09/12/apple-face-id-iphone-x.

105. *Compelled Decryption Primer,* NACDL Fourth Amendment Center, *available at* https://www.nacdl.org/uploadedFiles/files/criminal_defense/fourth_amendment/CompelledDecryptionPrimer.pdf. ■

About the Authors

Michael Price is Senior Litigation Counsel for NACDL's Fourth Amendment Center, which provides defense trainings, resources, and direct legal assistance to preserve privacy rights in the digital age. He focuses on cutting-edge Fourth Amendment issues including the "third-party doctrine," location tracking, device searches, parallel construction, and government hacking.

Michael Price
NACDL
Washington, DC
202-465-7615
EMAIL mprice@nacdl.org
WEBSITE www.nacdl.org
TWITTER @NACDL

Zachary Simonetti served as NACDL's Fourth Amendment Legal Fellow.

Zachary Simonetti
Washington, DC
828-450-6062
EMAIL zsimonet@tulane.edu
TWITTER @zachsim1

The Champion®

The Champion® (ISSN 0744-9488) is published monthly, except for January/February and September/October, which are bimonthly, by the National Association of Criminal Defense Lawyers®, Inc. Printed in the United States of America. Basic subscription rate $65 per year when received as a benefit of NACDL membership. Non-member subscriptions are $100 annually in the U.S. or $125 if mailed outside the U.S. Periodicals postage paid at Washington, DC and additional mailing offices. Postmaster: Send address changes to *The Champion*®, 1660 L Street, NW, 12th Floor, Washington, DC 20036.

The Champion® is published in the interest of the members of the National Association of Criminal Defense Lawyers® to inform and educate the membership and to improve communication within the criminal defense community. See *www.nacdl.org* for details.