The Micro-Hornbook on the Fifth Amendment and Encryption

DAN TERZIAN*

The DOJ calls encryption a "zone of lawlessness."[1] Others call it an "[e]scape from [t]yranny."[2] Opinions on encryption clearly diverge. But this micro-hornbook isn't about opinions. It's about the law—on what happens when the government has the right to search digital data (perhaps through a search warrant), but can't because the data is password protected and encrypted. Can the government, without violating the Fifth Amendment, force a phone's owner[3] to (a) produce the phone's password or (b) produce the decrypted phone (i.e., force her first to enter the password and then to produce the phone)? The first question's answer is easy; the second's answer is hard; and this micro-hornbook sketches the answers for both.

---

* Associate, Duane Morris LLP; Dan@danterzian.com.

1. Jason Koebler, *Tor and Encryption Have Created a 'Zone of Lawlessness,' Justice Department Says*, VICE (Jan. 27, 2015, 1:35 PM), http://motherboard.vice.com/read/tor-and-encryption-have-created-a-zone-of-lawlessness-justice-department-says [http://perma.cc/TV2F-9EQY].

2. Dude-Lebowski, Comment to *Tor and Encryption Have Created a 'Zone of Lawlessness,' Justice Department Says*, REDDIT (Jan. 28, 2015, 8:42 AM), https://www.reddit.com/r/Bitcoin/comments/2tyck4/tor_and_encryption_have_created_a_zone_of/co3gn71 [http://perma.cc/E9UK-99ZU].

3. This micro-hornbook does not address whether the government can force the phone's *manufacturer* to produce the password or decrypted phone. That question poses no Fifth Amendment issues because there is no danger of self-incrimination and because the Self-Incrimination Clause does not apply to corporations. United States v. White, 322 U. S. 694, 698–701 (1944). For an objective primer on that question, see Orin Kerr, *Preliminary Thoughts on the Apple iPhone Order in the San Bernardino Case: Part 2, the All Writs Act*, WASH. POST (Feb. 19, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/02/19/preliminary-thoughts-on-the-apple-iphone-order-in-the-san-bernardino-case-part-2-the-all-writs-act/ [http://perma.cc/C6WQ-PAG8].

I. FORCING PRODUCTION OF THE PASSWORD?

Whether the government can force a person to divulge her password depends on the password's type.

Unquestionably, the government can force people to produce biometric passwords like fingerprints. The Fifth Amendment does not protect against forced physical acts, such as the taking of fingerprint or voice samples, or even forcing a person "to make a particular gesture."[4] For this reason, a Virginia trial court reached the unremarkable conclusion that there is no cellphone exception to the Fifth Amendment.[5] So if you use a fingerprint to unlock your phone, the government's right to take fingerprint samples potentially allows it to access your phone.[6] Whether it *actually* allows the government to access your phone depends on the circumstances, as a fingerprint won't unlock an iPhone that's gone untouched for more than 48 hours.[7]

Almost as certainly, the government can't force you to produce a password.[8] The touchstone doctrine here stems from an oft-repeated line

---

4. Schmerber v. California, 384 U.S. 757, 764 (1966) (recognizing that "real or physical evidence" can be compelled and that "both federal and state courts have usually held that [the privilege] offers no protection against compulsion to submit to fingerprinting"); *see also* United States v. Hubbell, 530 U.S. 27, 34–35 (2000) ("[E]ven though the act may provide incriminating evidence, a criminal suspect may be compelled to put on a shirt, to provide a blood sample or handwriting exemplar, or to make a recording of his voice." (footnotes omitted)); United States v. Hook, 471 F.3d 766, 773–74 (7th Cir. 2006) ("[T]he taking of blood samples or fingerprints is not testimonial evidence and as such is not protected by the Fifth Amendment."); Williams v. Schario, 93 F.3d 527, 529 (8th Cir. 1996); Doe v. United States, 487 U.S. 201, 219 (1988) (Stevens, J., dissenting) ("Fingerprints, blood samples, voice exemplars, handwriting specimens, or other items of physical evidence may be extracted from a defendant against his will."); John E. D. Larkin, *Compelled Production of Encrypted Data*, 14 VAND. J. ENT. & TECH. L. 253, 270 (2012).

5. *See* Virginia v. Baust, No. CR14-1439, 2014 WL 6709960, at *3 (Va. Cir. Ct. Oct. 28, 2014).

6. *Id.*

7. *See About Touch ID Security on iPhone and iPad*, APPLE, http://support.apple.com/en-us/HT5949 [http://perma.cc/JF8Q-9EUE] (last visited Jan. 30, 2015) (fingerprint alone insufficient to unlock iPhone when "more than 48 hours have elapsed from the last time" the phone was unlocked).

8. I say "almost" because there is an argument that, if the password is physically recorded somewhere, the government can subpoena the production of that password. Phillip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171, 195; Dan Terzian, *The Fifth Amendment, Encryption, and the Forgotten State Interest*, 61 UCLA L. REV. DISCOURSE 298, 305 n.34 (2014). But, as a practical matter, the govern-

of Supreme Court dicta: The government can "force[] [someone] to surrender a key to a strongbox containing incriminating documents," but it can't force him "to reveal the combination to [a] wall safe."[9] Because a password is essentially a combination, several courts have held that the government can't force you to produce your password.[10]

II. FORCING PRODUCTION OF THE DECRYPTED PHONE?

The next, and more difficult, question is whether the government can force you to enter the password, which decrypts your phone. There is no right answer here, and you can argue it constitutional or not—unless you're in the Eleventh Circuit or Massachusetts. The former's litigants are bound by the rule that forced decryption is not constitutional, and the latter probably the opposite.[11]

The arguments trace three fronts: the key-combination dicta just discussed; forced decryption's physicality; and the foregone conclusion exception.

---

ment probably won't know if the password is physically recorded. So, even though the government can theoretically subpoena the written password, the subpoena won't yield anything if (when) the defendant responds that there is no written password.

9. *Doe*, 487 U.S. at 210 n.9 (internal brackets and quotation marks omitted); *see also Hubbell*, 530 U.S. at 43; United States v. Green, 272 F.3d 748, 763 n.10 (5th Cir. 2001); United States v. Kirschner, 823 F. Supp. 2d 665, 668–69 (E.D. Mich. 2010).

10. *Kirschner*, 823 F. Supp. 2d at 668–69; *In re* Boucher, No. 2:06–mj–91, 2007 WL 4246473, at *3–4 (D. Vt. Nov. 29, 2007), *overruled in part on other grounds*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009); *Baust*, No. CR14-1439, 2014 WL 6709960, at *3; *see also In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1345–46 (11th Cir. 2012); SEC Civil Action v. Huang, No. 15-cv-269, 2015 U.S. Dist. LEXIS 127853, at *3–7 (E.D. Pa. Sept. 23, 2015).

11. *Compare In re Grand Jury Subpoena*, 670 F.3d at 1346–47, 1349 & n.28 (requiring "knowledge as to the *files* on the hard drives" and as to "what . . . was hidden behind the encrypted wall"), *with* Commonwealth v. Gelfgatt, 11 N.E.3d 605, 615–16 (Mass. 2014) (finding a foregone conclusion where the government knew the defendant owned and operated the encrypted computer), *and id.* at 620–21 (Lenk, J., dissenting) (arguing that a foregone conclusion requires knowledge of "a certain file").

Obviously, one can still argue against these rules in the Eleventh Circuit and Massachusetts, but obtaining a favorable result would likely require reaching the Supreme Court.

A. THE KEY-COMBINATION DICTA

The first front stems from the dicta instructing that a key's production can be compelled but a combination's cannot.[12] Some courts have extended this dicta to forced decryption. Most notably, the Eleventh Circuit held that forced decryption—which requires the respondent "to *use* a decryption password"—"is most certainly more akin to requiring the production of a combination because both demand the use of the contents of the mind."[13]

Yet this extension is questionable. For one thing, the referenced dicta concerns producing a safe's unlocking mechanisms; it's not about producing a safe's contents, which is what forced decryption seeks. For another, safes and encryption differ markedly: the government can always crack a safe; rarely can it crack encryption.[14] This chasm could persuade a court to disregard the dicta, or at least to apply it less mechanistically.[15]

B. FORCED DECRYPTION'S PHYSICALITY

The second front is forced decryption's physicality. The government can compel you to perform physical acts, like providing handwriting or voice samples.[16] This includes producing a safe's key, assuming the above dicta is binding.

But what about forcing you to enter a password? Is this a compellable physical act? Three courts have answered no.[17] In their view, forcing a person to use a password to decrypt a hard drive is not a physical act because it forces the person to "use the contents of his mind."[18] Also prevalent in these courts' reasoning is the key-combination dicta already dis-

---

12. *See Hubbell*, 530 U.S. at 43; *Doe*, 487 U.S. at 210 n.9; Reitinger, *supra* note 8, at 203 & n.133.

13. *In re Grand Jury Subpoena*, 670 F.3d at 1346 (emphasis added); *see also In re Boucher*, 2007 WL 4246473, at *4; *Baust*, 2014 WL 6709960, at *3.

14. *See, e.g.*, Terzian, *supra* note 8, at 309–10.

15. *See, e.g.*, Dan Terzian, *Forced Decryption as Equilibrium—Why It's Constitutional and How* Riley *Matters*, 109 NW. U. L. REV. ONLINE 56, 60–63 (2014); *see also* Riley v. California, 134 S. Ct. 2473 (2014) (enacting Fourth Amendment rules specific to cellphone searches incident to arrest).

16. *See supra* note 4.

17. *In re Grand Jury Subpoena*, 670 F.3d 1335; *In re Boucher*, 2007 WL 4246473; *Baust*, 2014 WL 6709960.

18. *In re Grand Jury Subpoena*, 670 F.3d at 1346, 1349; *In re Boucher*, 2007 WL 4246473, at *4; *Baust*, 2014 WL 6709960, at *3.

cussed: "A password, like a combination, is in the suspect's mind, and is therefore testimonial . . . ."[19]

So far, no courts have answered differently. Yet nearly any court (save those in the Eleventh Circuit) could still decide the issue differently because they are not bound by the foregoing cases. And maybe courts should decide it differently because everything—even physical acts—requires minimally using your mind. You can't produce a key unless you remember where you put it. Prosecutors arguing physicality should also challenge these three courts' questionable approach of taking dicta on forcing people to *produce* unlocking mechanisms and then extending it to the issue of forcing people to *use* unlocking mechanisms (to produce the decrypted data itself).

C. THE FOREGONE CONCLUSION DOCTRINE

The final front is the "foregone conclusion" doctrine. Even if forced decryption is not a physical act, and even if forced decryption is more like producing a combination than a key, forced decryption is still constitutional if it falls within the foregone conclusion exception.

This exception permits the government to obtain documents that it already knows exist.[20] Courts applying the exception to subpoenas for de-

---

19. *In re Boucher*, 2007 WL 4246473, at *4; *see also In re Grand Jury Subpoena*, 670 F.3d at 1346; *Baust*, 2014 WL 6709960, at *3.

20. *See In re Grand Jury Subpoena*, 670 F.3d at 1344–46 ("Where the location, existence, and authenticity of the purported evidence is known with reasonable particularity, the contents of the individual's mind are not used against him, and therefore no Fifth Amendment protection is available." (footnote omitted)); United States v. Ponds, 454 F.3d 313, 319–20 (D.C. Cir. 2006); *In re* Grand Jury Subpoena, Dated April 18, 2003, 383 F.3d 905, 910 (9th Cir. 2004); Butcher v. Bailey, 753 F.2d 465, 469 (6th Cir. 1985); *see also* Fisher v. United States, 425 U.S. 391, 411–12 (1976); *In re* Grand Jury Subpoena Duces Tecum Dated October 29, 1992, 1 F.3d 87, 93 (2d Cir. 1993). Some cases have modified the requirement that the government know the document's location to require that the government know that the respondent possesses or controls the document. *See* United States v. Bright, 596 F.3d 683, 692 (9th Cir. 2010); *Ponds*, 454 F.3d at 324–25; *Butcher*, 753 F.2d at 469. Whatever the merits of this modification, it does not affect the analysis here. *See* Dan Terzian, *Forced Decryption as a Foregone Conclusion*, 6 CALIF. L. REV. CIRCUIT 27, 29 n.8 (2015).

The enterprising defense lawyer will note the existence of a good faith basis for arguing that the foregone conclusion doctrine is no longer good law or requires a more burdensome proof of knowledge. *See* Vivek Mohan & John Villasenor, *Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era*, 15 U. PA. J. CONST. L.

crypted hard drives have divided on a fundamental issue: what is the document that the government must know of? Is it a particular file, or is it instead the existence of the hard drive's contents generally?

Some courts require that the government know of "a certain file."[21] Other courts apparently require only that the government know of the potential for unencrypted files, even if it doesn't know the contents of those files because they're encrypted.[22] What's more, the government will always know this whenever it sees an iPhone's password prompt. Thus, the first group of courts allows forced decryption only in the rare instances where the government already knows what's on the hard drive, and the

---

HEIGHTENED SCRUTINY 11, 15–16 (2012) (arguing that the Circuit Courts' decisions are inconsistent with the Supreme Court's *Hubbell* decision).

21. *See In re Grand Jury Subpoena*, 670 F.3d at 1346–47, 1349 & n.28 (requiring "knowledge as to the *files* on the hard drives" and as to "what . . . was hidden behind the encrypted wall"); SEC v. Huang, No. 15-269, 2015 WL 5611644, at *4 (E.D. Pa. Sept. 23, 2015) (holding that a foregone conclusion does not exist because "the SEC has no evidence any documents it seeks are actually located on the [defendants'] work-issued smartphones"); *see also Baust*, 2014 WL 6709960, at *3 (requiring knowledge of the existence of an "unencrypted video recording" rather than of the unencrypted computer).

22. *See* United States v. Fricosu, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012) (stating that "[t]he fact that [the government] does not know the specific content of any specific documents is not a barrier to production" and concluding that "the existence and the location" of the "unencrypted version of the Z drive" was a foregone conclusion); Commonwealth v. Gelfgatt, 11 N.E.3d 605, 615–16 (Mass. 2014) (finding a foregone conclusion where the government did not know any files on the hard drive but knew the defendant controlled the hard drives).

In addition to the two groups of courts discussed in the main text, a third group exists. But this group does not illuminate how the foregone conclusion doctrine applies to subpoenas seeking to force decryption. With this group, the government knew of particular files on the encrypted hard drive, so the court did not need to—and did not—consider whether knowledge of potential unencrypted data suffices. *See In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *3–4 (D. Vt. Feb. 19, 2009) ("Second Circuit precedent, however, does not require that the government be aware of the incriminatory contents of the files; it requires the government to demonstrate 'with reasonable particularity that it knows of the existence and location of subpoenaed documents.'") (emphasis omitted); *In re* The Decryption of a Seized Data Storage System, No. 13-M-449 (E.D. Wis. Apr. 19, 2013) (order denying application to compel decryption), http://www.wired.com/images_blogs/threatlevel/2013/04/encryption-case.pdf [http://perma.cc/79NL-UF6J], *overruled on other (foregone conclusion) grounds*, No. 13-M-449 (E.D. Wis. May 21, 2013) (order granting ex parte request for reconsideration of the government's application under the All Writs Act), http://ia801700.us.achive.org/6/items/gov.uscourts.wied.63043/gov.uscourts.wied.63043.6.0.pdf [https://perma.cc/FPK3-YYTC].

second group allows it virtually always. None of these courts explain their reasoning, or even acknowledge the issue. So lawyers on both sides will need to marshal reasons in favor of one approach and against the other.[23]

CONCLUSION

If the government wants a fingerprint, it's getting it. If the government wants a password, it's not getting it. And if the government wants a decrypted hard drive, it may or may not get it.

23. A potential starting point for prosecutors is the limited authority, outside the encryption context, explicitly recognizing that the government need only have "knowledge of . . . the actual documents, not the information contained" within a subpoenaed document. *In re Grand Jury Subpoena, Dated April 18, 2003*, 383 F.3d at 910; *see also Ponds*, 454 U.S. at 325 (holding that knowledge of information related to the subpoenaed documents is not sufficient to compel a testimonial act of production).