YLD PERSPECTIVES
FBA INNOVATION
PRESENTED BY THE YOUNGER LAWYERS DIVISION OF THE FEDERAL BAR ASSOCIATION

HOW THE GOVERNMENT WILL DECRYPT YOUR IPHONE

BY DAN TERZIAN

Through you. The government will decrypt your iPhone by forcing you to do it

Well, that's what the government will *try* to do. It's the only real option. Absent a statute mandating a government backdoor or an investigation yielding a password, law enforcement typically can't access the data stored on an encrypted phone.[1]

Few cases address whether the government can constitutionally force you to decrypt your phone. And those that do reach mixed results. Some apparently hold it's always allowed; others clearly hold it's usually barred under the Fifth Amendment Self-Incrimination Clause. The Massachusetts high court falls in the former group; the Eleventh Circuit the latter.

But which group is "right"?

I submit that the right answer should be that forced decryption is always constitutional. Here's why.

* * *

Two things are beyond debate. First, the government can force you to provide fingerprints.[2] Which the government can then use to unlock your phone.[3] Except, a fingerprint alone won't always unlock it, such as when "more than 48 hours have elapsed from the last time" your iPhone was unlocked.[4]

Second, the government can't make you provide an alpha-numeric password. In oft-repeated dicta, the Supreme Court recognized that the government can "force[] [you] to surrender a key to a strongbox containing incriminating documents," but it can't force you "to reveal the combination to [a] wall safe."[5] A password is essentially a combination, so the government can't force you to produce it.[6]

* * *

Now on to the debatable: can the government force you to decrypt your phone? For two reasons, it should.

First, forced decryption should be constitutional because it's a foregone conclusion.[7] The government can compel production of anything where it sufficiently knows that the sought item exists (i.e., its existence is a foregone conclusion).[8]

Courts have divided on how this foregone conclusion doctrine applies to forced decryption. Some courts clearly hold that the government must know of "a certain file" on a phone before it can force decryption.[9] Yet other courts appear to hold that knowledge of an individual file isn't necessary, and the government need only know that general unencrypted data exists on the phone.[10] In turn, the government always knows this when it sees an iPhone's password prompt.[11] So the government can always force you to decrypt your phone under this approach.

Dan Terzian practices commercial litigation and insurance coverage. Dan also has an active pro bono practice, in which he has prepared a federal civil rights action for trial—before settling on terms favorable to the client—and drafted a cert petition to the U.S. Supreme Court.

Before coming to Duane Morris, Dan clerked for Chief Judges Ramona Manglona and Frances Tydingco-Gatewood of the U.S. District Courts for the Northern Mariana Islands and Guam. Before that, he was a C.V. Starr Lecturer at the Peking University School of Transnational Law in Shenzhen, China.

Outside of his practice, Dan has published extensively on encryption and also on the Financial Institutions Reform, Recovery and Enforcement Act of 1989. His publications have appeared in the *Los Angeles Times*, *American Banker*, *Northwestern Law Review*, *Penn State Law Review*, *UCLA Journal of International Law and Foreign Affairs*, *California Law Review Circuit*, *Georgetown Law Journal Online*, and *UCLA Law Review Discourse*. He has been cited or quoted by, among others, the Fourth Circuit of the United States Court of Appeals, the Air Force Court of Criminal Appeals, the Congressional Research Service, *American Banker*, *MIT Technology Review*, *U.S. News & World Report*, and *The Verge*.

Dan is a 2011 graduate of UCLA School of Law, where he served as an editor of the Law Review and was elected to the Order of the Coif, and a 2007 graduate of Cal Poly, San Luis Obispo.

None of these courts explain why they adopt their respective approaches. Nor do they even acknowledge their splitting with others.

Regardless, the courts requiring knowledge of unencrypted data should have the better argument. The foregone conclusion doctrine requires that the government have "knowledge of . . . the actual documents, not the information contained" within a document.[12] Accordingly, when the government subpoenas "all documents . . . relating to . . . calendars,"[13] the government must know that the calendar exists—not of any potential entries in the calendar.[14]

The same goes for encrypted iPhones. The government shouldn't need to know what particular files are contained within the unencrypted iPhone. All it needs to know is that an unencrypted iPhone exists. Which it knows by seeing a password prompt that it can't crack. Thus, the unencrypted iPhone's existence should be a foregone conclusion, and the government should be able to force you to decrypt your phone.

Second, forced decryption should also be allowed because the government can force you to perform physical acts.[15] This includes forcing you to provide handwriting or voice samples, or to make a particular gesture.[16] By contrast, the government can't force you to say anything or undertake acts requiring substantial mental effort.[17] For this reason, the government can't make you search eleven broad categories of documents and then produce 13,000 responsive pages.[18]

In this dichotomy of physical acts and testimonial communications, three courts have held that forced decryption is the latter.[19] In reaching this conclusion, these courts reason that decrypting a hard drive "certainly use[s] the contents of [the respondent's] mind . . . ."[20] These courts also rely on the key-combination dicta already discussed: "A password, like a combination, is in the suspect's mind, and is therefore testimonial."[21]

Yet this reasoning is at least partially erroneous. The key-combination dicta should be irrelevant. It's about producing unlocking mechanisms, not about producing an unlocked safe. Plus, pre-digital dicta on safes—which can always be cracked—should hold little sway in the context of unbreakable encryption.[22] Surely the Court did not intend its dicta originating in 1988[23] (when state-of-the art was a 386 with a .02 GB hard drive) to resolve this issue.

Moreover, to the extent this dicta is relevant, it indicates that forced decryption is constitutional because of the minimal mental effort involved. Remembering and entering a password requires no more mental effort than remembering a key's location and producing it.[24]

Conclusion

And that's why, IMO, forced decryption should be constitutional: because the unencrypted hard drive's existence is a foregone conclusion, and because forced decryption is a physical act.

[1] *See, e.g.*, Dan Terzian, *The Fifth Amendment, Encryption, and the Forgotten State Interest*, UCLA L. REV. DISCOURSE 298, 302–03 (2014).

[2] United States v. Hubbell, 530 U.S. 27, 34–35 (2000); Schmerber v. California, 384 U.S. 757, 764 (1966); Virginia v. Baust, No. CR14-1439, slip. op. at 5 (Va. Cir. Ct. Oct. 28, 2014), *available at* http://www.scribd.com/doc/245628784/Fingerprint-Unlocking-Ruling; *see also* United States v. Hook, 471 F.3d 678, 773–74 (7th Cir. 2006); John E. D. Larkin, *Compelled Production of Encrypted Data*, 14 VAND. J. ENT. & TECH. L. 253, 270 (2012).

[3] *Baust*, No. CR14-1439, slip. op. at 5.

[4] *See About Touch ID Security on iPhone and iPad*, APPLE (Dec. 2, 2014), http://support.apple.com/en-us/HT5949.

[5] *See* Doe v. United States, 487 U.S. 201, 210 n.9 (1988) (internal brackets and quotation marks omitted); *see also Hubbell*, 530 U.S. at 43.

[6] *See* In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012); US v. Kirschner, 823 F. Supp. 2d 665, 668–69 (E.D. Mich. 2010); In re Grand Jury Subpoena to 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, slip. op. at 5; *see also* SEC Civil Action v. Huang, No. 15-cv-269, 2015 U.S. Dist. LEXIS 127853 at *3–7 (E.D. Pa. Sept. 23, 2015).

[7] *See generally* Dan Terzian, *Forced Decryption as a Foregone Conclusion*, 6 CALIF. L. REV. CIRCUIT 27 (2015).

[8] *See In re Grand Jury Subpoena*, 670 F.3d at 1344, 1346 ("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 (1976).

[9] *See In re Grand Jury Subpoena*, 670 F.3d at 1346–47, 1349 & n.28; *Huang*, 2015 U.S. Dist. LEXIS 127853 at *9–10; *see also Baust*, No. CR14-1439, slip op. at 5.

[10] *See Fricosu*, 841 F. Supp. 2d at 1237 (stating that "[t]he fact that it 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); *see also Gelfgatt*, 11 N.E.3d at 615–16.

[11] *See* Simson Garfinkel, *The iPhone has Passed a Key Security Threshold*, MIT TECH. REV. (Aug. 13, 2012), http://www.technologyreview.com/news/428477/the-iphone-has-passed-a-key-security-threshold/.

[12] *In re Grand Jury Subpoena*, 383 F.3d at 910; *see also See Ponds*, 454 F.3d at 325.

[13] *In re Grand Jury Subpoena*, 383 F.3d at 908 (internal quotation marks omitted).

[14] *See id.* at 910–11 (holding that knowledge of "records establishing meetings" was not sufficient to compel production of calendars).

[15] *See* United States v. Hubbell, 530 U.S. 27, 34, 41–42 (2000); Fisher v. United States, 425 U.S. 391, 408 (1976); Schmerber v. California, 384 U.S. 757, 764 (1966); *In re Grand Jury Subpoena*, 670 F.3d at 1341.

[16] *Supra* note 15.

[17] *Hubbell*, 530 U.S. at 34, 41–42; Terzian, *supra* note 1, at 304; *see also* Miranda v. Arizona, 384 U.S. 467 (1966) (adopting procedural safeguards to protect a suspect's right to remain silent).

[18] *Hubbell*, 530 U.S. at 41–42.

[19] *In re Grand Jury Subpoena*, 670 F.3d at 1346, 1349 (stating that forced decryption "certainly use[s] the contents of [the respondent's] mind"); In re Grand Jury Subpoena to Boucher, No. 2:06–mj–91, 2007 U.S. Dist. LEXIS 87951 at *10 (D. Vt. Nov. 29, 2007), *overruled in part on other grounds*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009); Virginia v. Baust, No. CR14-1439, slip. op. at 5 (Va. Cir. Ct. Oct. 28, 2014), *available at* http://www.scribd.com/doc/245628784/Fingerprint-Unlocking-Ruling.

[20] *In re Grand Jury Subpoena*, 670 F.3d at 1349; *In re Grand Jury Subpoena to Boucher*, 2007 U.S. Dist. LEXIS 87951 at *10; *see also Baust*, slip. op. at 5.

[21] *In re Grand Jury Subpoena*, 670 F.3d at 1346–47; *In re Grand Jury Subpoena to Boucher*, 2007 U.S. Dist. LEXIS 87951 at *10; *see also Baust*, slip. op. at 5.

[22] *See, e.g.*, Terzian, *supra* note 1, at 309–10.

[23] *Doe*, 487 U.S. at 210 n.9.

[24] Dan Terzian, *Forced Decryption as Equilibrium: Why It's Constitutional and How* Riley *Matters*, 109 NW. U. L. REV. ONLINE 56, 60 (2014).