Copyright 2014 by Dan Terzian
Northwestern University Law Review
Vol. 109

FORCED DECRYPTION AS EQUILIBRIUM—WHY IT'S CONSTITUTIONAL AND HOW *RILEY* MATTERS

*Dan Terzian**

Fourth Amendment jurisprudence seeks equilibrium.[1] When new technology frustrates the government's ability to obtain evidence, "the Supreme Court generally adopts lower Fourth Amendment protections . . . to help restore the status quo ante level of government power."[2] Conversely, when new technology "makes evidence substantially easier for the government to obtain, the Supreme Court often embraces higher protections to help restore the prior level of privacy protection."[3] One need not search far back to find equilibrium-seeking in action—see *Riley v. California*,[4] a Supreme Court decision of just this past term on the Fourth Amendment and cellphones.

Yet equilibrium-seeking is not confined to that Amendment. In the Fifth Amendment, too, the Court seeks equilibrium. Throughout Self-Incrimination Clause jurisprudence, one finds the Court balancing privacy against the government's need to obtain evidence.[5]

Enter: encrypted data and the compelled production thereof, an area in want of equilibrium. Previously, when the government obtained a warrant for data, *it got that data*. But now when the sought data is encrypted, the government instead gets a password prompt. If that password is strong, the computer is, in *Riley*'s words, "all but 'unbreakable.'"[6] This leaves the government with just one option: obtaining a subpoena to force the person to enter her password and thereby decrypt the data. But does the Fifth Amendment's Self-Incrimination Clause bar this forced decryption?

---

* Law Clerk, United States District Court; Dan@danterzian.com. Thanks to editors of the Northwestern University Law Review Online for their comments.

1 *See generally* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011) [http://perma.cc/N9V-8LC6].

2 *Id.* at 480.

3 *Id.*

4 No. 13–132 (U.S. June 25, 2014) [http://perma.cc/KV2W-ZXBC].

5 Dan Terzian, *The Fifth Amendment, Encryption, and the Forgotten State Interest*, 61 UCLA L. REV. DISC. 298, 307–09 (2014) (collecting cases) [http://perma.cc/K6DR-EVV2].

6 *Riley*, No. 13-132, slip op. at 12–13; *see also* Phillip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171, 175; 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/ [http://perma.cc/5469-AMZL].

Lower courts have not yet sought, nor even considered, equilibrium in answering this question.[7] The only federal appeals court ruling on the issue essentially held that the Fifth Amendment prohibits forced decryption.[8] There goes the government's ability to obtain digital evidence in that circuit.

This is a mistake. Courts should begin seeking equilibrium in their Fifth Amendment analyses. *Riley* itself, even though a Fourth Amendment case, signals courts to do so. The *Riley* Court sought equilibrium, and its decision tells lower courts to do similarly, to "feel free to read Supreme Court precedents narrowly" in other cases involving new technologies.[9] Encryption is such a new technology: It vitiates the government's ability to gather evidence. Paper documents—even if locked in a safe—can be recovered;[10] an encrypted computer's documents cannot. Maintaining equilibrium here requires permitting forced decryption, and Self-Incrimination Clause precedent can be interpreted as permitting it. Courts should therefore adopt that interpretation.

This Essay first introduces Self-Incrimination Clause doctrine apart from any equilibrium analysis (Part I); then discusses *Riley* and its equilibrium-seeking (Part II); and last argues that *Riley* supports finding forced decryption constitutional (Part III).

I. THE SELF-INCRIMINATION CLAUSE

The Self-Incrimination Clause declares that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself . . . ."[11] The privilege against self-incrimination, where applicable, gives persons the right to refuse the government's demands for information, data, or objects.[12] The privilege applies wherever the government (1) compels (2) a testimonial communication or act that (3) is incriminating.[13] In practice, the analysis focuses only on the element of testimonial communications or acts, because the other two's existence or nonexistence is "obvious."[14]

Communications or acts can be testimonial for two independent reasons: because they convey an implied communication or because they

---

[7] Terzian, *supra* note 5, at 300 & n.3; *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012) [http://perma.cc/HFX4-BWGA]; Commonwealth v. Gelfgatt, 468 Mass. 512 (2014) [http://perma.cc/M6D4-Y69F].

[8] *See* In re *Grand Jury Subpoena*, 670 F.3d at 1346–49.

[9] Richard Re, *Symposium: Inaugurating the Digital Fourth Amendment*, SCOTUSBLOG (June 26, 2014, 12:37 PM), http://www.scotusblog.com/2014/06/symposium-inaugurating-the-digital-fourth-amendment [http://perma.cc/W4D-PE2D].

[10] Terzian, *supra* note 5, at 310.

[11] U.S. CONST. amend. V [http://perma.cc/LVJ4-D38N].

[12] *See* United States v. Doe, 465 U.S. 605, 617 (1984) [http://perma.cc/GQ8Q-Y6FK].

[13] In re *Grand Jury Subpoena*, 670 F.3d at 1341.

[14] *See id.*

require substantial mental effort. Implied communications arise from producing documents. If you, say, produce files from a specific computer, you're implying that you possess or control that computer.[15] This production can be testimonial and therefore barred by the Fifth Amendment.[16]

Implied communications pose no real concern to forced decryption's constitutionality for two reasons. First, the government can compel the production if it provides act of production immunity. This "immuniz[es] the testimonial component of the act"—the government cannot use it to prove ownership—but lets the government use the data obtained from the computer to prove anything else.[17]

Second, the government may be able to compel production through the "foregone conclusion" exception. Where the government can "independently confirm" the testimonial component (here, computer ownership) through specific "prior knowledge" that goes beyond mere suspicion, it can still compel production.[18] So when the government finds a desktop computer in Winston's unshared studio apartment, that computer's password prompt lists the user as "Winston," and the only fingerprints on the computer are Winston's, his ownership is likely a foregone conclusion and the files' production can be compelled.[19]

Contrast implied communications with the stronger reason why forced decryption could be viewed as testimonial: through substantial mental effort. Compelled acts requiring substantial mental effort are testimonial, while those requiring little are not.[20] Note that the foregone conclusion exception applies here too—if the government seeks a specific document and knows it's on your computer, the exception applies regardless of the mental effort involved.[21]

---

[15] *See* United States v. Hubbell, 530 U.S. 27, 35–36 (2000) [http://perma.cc/WYJ5-NPUE]; Samuel A. Alito, Jr., *Documents and the Privilege Against Self-Incrimination*, 48 U. PITT. L. REV. 27, 57–59 (1986).

[16] *See Hubbell*, 530 U.S. at 36–37; Nicholas Soares, Note, *The Right to Remain Encrypted: The Self-Incrimination Doctrine in the Digital Age*, 49 AM. CRIM. L. REV. 2001, 2004–05 (2012).

[17] *See, e.g.*, Alito, *supra* note 15, at 57; Reitinger, *supra* note 6, at 189–91, 196–200 (noting contrary authority in limited circumstances not relevant here).

[18] *Hubbell*, 530 U.S. at 44–45. *See generally* Vivek Mohan & John Villasenor, *Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era*, 15 U. PA. J. CONST. L. HEIGHTENED SCRUTINY 11 (2012) (examining the foregone conclusion doctrine's application to digital data and proposing new analytical framework) [http://perma.cc/339W-63T8].

[19] *Cf.* In re *Grand Jury Subpoena*, 670 F.3d at 1346–49.

[20] Terzian, *supra* note 5, at 304; Fisher v. United States, 425 U.S. 391, 411 (1976) (emphasis added) ("[H]is Fifth Amendment privilege is not violated because nothing he has said or done is deemed to be *sufficiently* testimonial for purposes of the privilege.") [http://perma.cc/N7CT-2UXP].

[21] *See, e.g.*, In re *Grand Jury Subpoena*, 670 F.3d at 1346–49; *Hubbell*, 530 U.S. at 44–45.

Consider the following examples of testimonial communications through mental effort. Producing handwriting or voice samples requires relatively little mental effort—just, basically, commanding yourself to write or speak—so compelling their production is not testimonial and thus is permissible.[22] But responding to a subpoena seeking documents spanning eleven broad categories and amounting to over 13,000 responsive pages? That requires substantial mental effort and is therefore testimonial.[23]

Now, which example do you think forced decryption (compelling a person to enter a password) is more like: writing some words or mining box after box for responsive documents? Me too. This is how current doctrine can be interpreted as permitting forced decryption.

To be sure, this interpretation is more nuanced at the margins. Maybe, for instance, Julia does not remember her password and learning it requires finding its various components stowed in numerous boxes. Even here, though, forced decryption still does not require substantial mental effort. Julia does not need to analyze a subpoena and make judgments about whether certain documents are responsive.[24] Rather, she knows exactly what she needs to do—physically compile the password's components and then decrypt her computer—with no judgments being necessary.

Courts have not yet framed the issue this way.[25] The Eleventh Circuit, the only federal appeals court deciding it, found forced decryption testimonial.[26] Its analysis hinged on a line of Supreme Court dicta: the production of strongbox keys can be compelled, but combinations to a safe cannot.[27] Because computer passwords are more like combinations than keys, the Eleventh Circuit concluded that a password's production is testimonial.[28] It then concluded that forced decryption is also testimonial because using a decryption password requires substantial mental effort, as it's also more like producing a combination than a key.[29]

This reasoning falters twice. First, it misreads Supreme Court dicta. The dicta regards only compelling production: The government can compel the production of keys but not the production of combinations.[30] It's silent on whether the government can compel unlocking (i.e., forcing a person to enter a combination without producing a copy). This silence, coupled with the dicta's rationale, suggests that compelled unlocking may be constitutional. The reason for the Court distinguishing between key- and

---

[22] *See Hubbell*, 530 U.S. at 35.

[23] *See id.* at 40–43.

[24] *Cf. id.* at 42–43.

[25] *See supra* note 7 and accompanying main text.

[26] *See* In re *Grand Jury Subpoena*, 670 F.3d at 1346.

[27] *See id.*; *Hubbell*, 530 U.S. at 43.

[28] *See* In re *Grand Jury Subpoena*, 670 F.3d at 1346.

[29] *See id.*

[30] *See Hubbell*, 530 U.S. at 43; *Doe*, 487 U.S. at 210 n.9.

combination- productions stems from the Court's concern over compelled creation. Combinations may not exist outside a person's mind, so producing them would require compelling the creation of a physical version, and it is this compelled creation that makes the response testimonial.[31] There are no such compelled creation concerns with compelled unlocking through forced decryption—the data is already there, the person just needs to unlock it; and unlocking it does not require creating a physical copy of the password.

The second stumble comes in the Eleventh Circuit's analysis of mental effort. Entering an oft-used password requires no more mental effort than finding a key.[32] You remember the key's location and then find it, just as you remember the password and then input it.

Put aside the relative merits of these competing interpretations, mine and the Eleventh Circuit's; they matter little here. Instead, just accept that the interpretation permitting forced decryption is theoretically possible under current Fifth Amendment doctrine, even if you think it improbable. Here's why lower courts should nevertheless adopt the improbable interpretation and permit forced decryption: *Riley v. California*.

II. EQUILIBRIUM-SEEKING IN *RILEY V. CALIFORNIA*

To start, *Riley* is not a Fifth Amendment case. It's a Fourth Amendment one, raising the question of whether the government can search a person's cellphone incident to arrest. The answer: Not without a warrant.[33]

That answer's not terribly important for forced decryption cases. What *is* important, however, are two principles *Riley* articulates that apply broadly to criminal procedure jurisprudence. But before discussing those principles, let me allay any initial concerns: It matters not that *Riley* regards the Fourth Amendment and forced decryption regards the Fifth. In both areas, "the Court zigs, zags, and balances, ad hoc" in an attempt to seek equilibrium.[34] Moreover, the Supreme Court long ago recognized that "[t]he values protected by the Fourth Amendment . . . substantially overlap [with] those . . . [that] the Fifth Amendment helps to protect."[35] Because *Riley* essentially regards computers and touches upon encryption's impenetrability, that overlap is twofold here.

Now on to *Riley's* two core principles. First, *Riley* thrice signals that there should be computer-rules of criminal procedure, just as there are

---

[31] Terzian, *supra* note 5, at 305; Mohan & Villasenor, *supra* note 18 at 13–14.

[32] Terzian, *supra* note 5, at 310–11.

[33] Riley v. California, No. 13-132, slip op. at 10, 25, 27–28 (June 25, 2014) (noting exigent circumstances that may permit a search without a warrant).

[34] Akhil Reed Amar & Renée B. Lettow, *Fifth Amendment First Principles: The Self-Incrimination Clause*, 93 MICH. L. REV. 857, 872 (1995) (Fifth Amendment) [http://perma.cc/3FAK-WFDQ]. *See generally* Terzian, *supra* note 5 (Fifth Amendment); Kerr, *supra* note 1 (Fourth Amendment).

[35] Schmerber v. California, 384 U.S. 757, 767 (1966) [http://perma.cc/4UAT-NFFP].

vehicle-rules.[36] First by declaring that many cellphones "are in fact minicomputers;"[37] second by distinguishing these minicomputers from other objects kept on the person;[38] and third by declaring that searching minicomputers cannot be analogized to other searches incident to arrest.[39] On distinguishing computers, the Court recognized that cellphones are "qualitatively different" from other objects people carry.[40] The details they contain about "the privacies of life" are so vast that they "implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[41] And as for not analogizing computer searches to other contexts, the Court declined to "import[ ] [constitutional standards] from the vehicle context" to cellphones.[42] It then also rejected "an analogue test" that would allow the government to search photos on a cellphone just as it could search photos in a wallet.[43]

Riley's second notable contribution is how it determines the cellphone-search rule: by seeking equilibrium. Though this equilibrium-seeking is not explicit, it is nevertheless apparent.[44] The Court noted that people carried relatively little personal information on their person before cellphones existed, so searches incident to arrest did not give the government much evidence.[45] Cellphones changed this. They contain immense amounts of "quantitative and . . . qualitative data" about a person's life,[46] which make an arrestee's privacy interest in her cellphone "dwarf those in [her other personal property at hand]."[47] Moreover, allowing cellphones to be searched would make it too easy for the government to obtain evidence, because such searches "would typically expose to the government far more than the most exhaustive search of a house."[48] At bottom, the Court's forbidding cellphone searches incident to arrest maintained equilibrium by providing higher protections for cellphones than for other objects, to help restore the prior level of privacy protection.

---

[36] *See* Orin Kerr, *The Significance of* Riley, VOLOKH CONSPIRACY (June 25, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/25/the-significance-of-riley/ [http://perma.cc/Z72B-67G9].

[37] *Riley*, No. 13-132, slip op. at 17.

[38] *Id.*, slip op. at 17–21.

[39] *See id.*

[40] *Id.*, slip op. at 19.

[41] *Id.*, slip op. at 17, 28 (quoting Boyd v. United States, 116 U.S. 616, 625 (1886) [http://perma.cc/TH32-UST4]).

[42] *Id.*, slip op. at 22–23.

[43] *Id.*, slip op. at 24–25.

[44] *See* Kerr, *supra* note 36.

[45] *Riley*, No. 13-132, slip op. at 19.

[46] *See id.*, slip op. at 17.

[47] *See id.*, slip op. at 22 (bracketed phrase replacing reference to *United States v. Robinson*, 414 U.S. 218 (1973), discussed in *id.*, slip op. at 7–8).

[48] *Id.*, slip op. at 20 (emphasis omitted).

III. FORCED DECRYPTION AS EQUILIBRIUM

Riley's two principles illuminate the forced decryption issue. The repeated assertions that computers are different—suggesting there should be computer-specific criminal procedure rules—send a flare to lower courts: Don't "too quickly follow broad statements from pre-digital opinions, even if those opinions emanated from the Supreme Court itself."[49] Instead, courts should "feel free to read Supreme Court precedents narrowly" in the context of criminal procedure and new technologies.[50] Just as *Riley* rejected an analogue test to determine the constitutionality of cellphone searches, lower courts should reject the same test to determine whether forced decryption is constitutional. They need not inquire whether forcing Julia to decrypt her hard drive is more like producing a safe combination than a strongbox key. So even if the supposedly *better* interpretation of pre-digital Fifth Amendment doctrine is that forced decryption is forbidden, lower courts should instead—if there's good reason to—adopt the *possible* interpretation that forced decryption is permissible. And that good reason, *Riley* tells us, is maintaining equilibrium.

This is why courts should allow forced decryption: to maintain the equilibrium between individual privacy and government power that *Riley* also seeks to balance. Prior to encryption, the government obtained a warrant and got the sought data. Even if the sought documents were held in a safe and the government lacked the combination, the government still obtained them because it could crack the safe.[51]

Also note that the government has a right to this data once it obtains a warrant. As *Riley* recognized, the "answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant."[52] Once the government obtains that warrant—once it has probable cause to believe the cellphone contains evidence that "will aid in a particular apprehension or conviction" for a particular offense—privacy concerns cease, and the government has the right search it.[53] If the cellphone is unencrypted, the government then obtains the data pursuant to that warrant.

---

[49] Re, *supra* note 9.

[50] *See id.* (referring only to the Fourth Amendment).

[51] Terzian, *supra* note 5, at 310.

[52] *Riley*, No. 13-132, slip op. at 28.

[53] Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 307 (1967) [http://perma.cc/MUG8-UF66]. *See also id.*, slip op. at 16, 25–26, 28; OFFICE OF LEGAL EDUC., EXEC. OFFICE FOR U.S. ATTORNEYS, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 72–76 (3d ed. 2009), *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf (explaining process of obtaining a warrant for information stored on electronic storage media) [http://perma.cc/7LTG-URC8].

But if the data lies on an encrypted device, equilibrium is disrupted. Encryption can be virtually unbreakable, so the government cannot obtain readable data without forced decryption. Even though the government has the right to obtain this data with a warrant. Even though it would obtain this data if it were not encrypted. And even though all data, encrypted or not, is increasingly essential evidence.[54] In short, encryption transforms the government's right to obtain this evidence into a person's right to essentially destroy evidence by making it inaccessible, a right fundamentally counter to established jurisprudence.[55] The only way to restore the status quo—to return the government's ability to obtain evidence to its ex ante level—is through finding forced decryption constitutional.

How, exactly, courts go about restoring equilibrium is a question of line-drawing. Courts could say that forced decryption is always constitutional because it's a nontestimonial act and that's all that matters. Or they could find that forced decryption is just sometimes constitutional, only where maintaining equilibrium actually requires it. So if the government cannot at all obtain the data without forced decryption, it's constitutional; but if the government can easily obtain it (say by getting the password from the person's spouse), forced decryption is not constitutional. Elsewhere I've suggested a slight preference for the circumstantial approach.[56] But the absolute approach—that forced decryption is always constitutional—has merit as well. Chiefly, it's easier in application, and *Riley* rejects a circumstantial test in favor of an absolute ban on cellphone searches incident to arrest.[57] Wherever the line, it will likely be determined just as it was in *Riley*: by the Supreme Court.

IV. CONCLUSION

The Supreme Court's criminal procedure jurisprudence seeks equilibrium, and *Riley* calls for lower courts to seek it as well. Courts interpreting the Fifth Amendment and whether it permits forced decryption should therefore consider equilibrium. Permitting forced decryption maintains the status quo; forbidding forced decryption destroys it. Because Fifth Amendment doctrine can be interpreted as allowing forced decryption and because doing so maintains equilibrium, courts should find forced decryption constitutional.

---

[54] *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 532 (2005) (stating that "computers have become an increasingly important source of evidence" and searching them is an increasingly "essential step in the investigation") [http://perma.cc/6VRC-WX7F].

[55] *Cf.* Segura v. United States, 468 U.S. 796, 816 (1984) ("The essence of the dissent is that there is some 'constitutional right' to destroy evidence. This concept defies both logic and common sense.") [http://perma.cc/AFC4-9RCC].

[56] Terzian, *supra* note 5, at 311–12.

[57] *Riley*, No. 13-132, slip op. at 22, 26–28 (noting exigent circumstances that may permit a search without a warrant).