Texas Law Review Online

Volume 97

Response

The Privilege Against Cellphone Incrimination

Bryan H. Choi†

The standard approach to the problem of compelled decryption of cellphones has been to treat cellphones like glorified lockboxes. The contents are assumed to be the equivalent of private papers, leaving only the passcode subject to dispute. Orin Kerr has helpfully labeled this dichotomy as the "treasure" versus the "key."[1]

Much of the debate has centered on whether the government may compel production of the key. When the passcode is a memorized phrase, it is a classic example of "contents of the mind" that may be withheld under the

† Assistant Professor of Law and Computer Science & Engineering, The Ohio State University Moritz College of Law. For invaluable input at formative stages, I thank Doug Berman, Joshua Dressler, David Gray, Margaret Hu, Orin Kerr, Guy Rub, Laurent Sacharoff, Ric Simmons, Chris Slobogin, Kathy Strandburg, Dan Tokaji, and Chris Walker, as well as Mark Graber and participants of the 2019 Schmooze at University of Maryland Carey School of Law. All opinions, errors, and omissions are my own.

1. Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEXAS L. REV. 767, 768, 771 (2019).

Fifth Amendment privilege against self-incrimination. Some courts have sidestepped this obstacle (1) by allowing the government to compel decryption as long as the passcode itself is never revealed[2], or (2) by finding that the passcode is not privileged testimony.[3] By contrast, other courts have refused to allow compelled decryption for any reason—even when the passcode is a fingerprint or other biometric feature that is typically non-testimonial, physical evidence.[4]

Kerr's position is that this debate over the key is essentially moot, because the treasure itself can never be privileged.[5] Whether that treasure is encrypted or unencrypted should not change its availability to law enforcement. Other commentators, including Laurent Sacharoff, are more circumspect, arguing that the "foregone conclusion" doctrine[6] restricts the

2. *See, e.g.*, United States v. Apple MacPro Comput., 851 F.3d 238, 243 (3d Cir. 2017); United States v. Spencer, No. 17-cr-00259-CRB-1, 2018 WL 1964588, at *2 (N.D. Cal. Apr. 26, 2018); *In re* Boucher, No. 2:06–mj–91, 2009 WL 424718, at *3–4 (D. Vt. Feb. 19, 2009).

3. *See, e.g.*, *In re* Search of [Redacted] Wash., D.C., 317 F. Supp. 3d 523, 535–36, 539 (D.D.C. 2018); *In re* Search Warrant Application for [Redacted], 279 F. Supp. 3d 800, 803–06 (N.D. Ill. 2017); Commonwealth v. Gelfgatt, 11 N.E.3d 605, 616–17 (Mass. 2014); State v. Diamond, 905 N.W. 2d 870, 875–78 (Minn. 2018). *See generally* Aloni Cohen & Sunoo Park, *Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries*, 32 HARV. J.L. & TECH. 169 (collecting pertinent cases).

4. *See In re* Search of Residence in Oakland, CA, 354 F. Supp. 3d 1010, 1016 (N.D. Cal. 2019); *In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073–74 (N.D. Ill. 2017); Seo v. State, 109 N.E.3d 418, 431 (Ind. Ct. App. 2018), *vacated*, 119 N.E.3d 90 (Ind. 2018).

5. Kerr, *supra* note 1, at 787 ("When a suspect is ordered to produce a decrypted version of an electronic device, the compelled act ordinarily will be only to unlock the device. Any additional searching is the government's job, and the government need not know what it will find when it begins to look."). Whether documents are unprivileged because they are non-compelled, non-testimonial, or both, has never been squarely resolved. *See* Akhil Reed Amar & Renée B. Lettow, *Fifth Amendment First Principles: The Self-Incrimination Clause*, 93 MICH. L. REV. 857, 887–88 (1995). Thanks to Chris Slobogin for pointing out the slippage in this area.

6. In brief, the "foregone conclusion" doctrine allows the government to compel a suspect to produce documents when the suspect's "act of production" would not communicate any new information or knowledge to the government. *See* Kerr, *supra* note 1, at 771–73. The contrapositive implication is that whenever an act of production *would* reveal new information to the government,

government from compelling decryption of any files it cannot describe with particularity.[7] In that regard, Sacharoff sees connective tissue tying the Fifth Amendment back to the particularity requirement in the Fourth Amendment.[8]

This Essay takes a different tack: How might the line of cases refusing to compel decryption of cellphones be consistent with Fifth Amendment principles? The theory advanced here is that those judicial decisions are best understood as treating cellphones as an extension of "self."[9] This reframing counters Kerr's key/treasure metaphor, not by challenging the "key" comparison—as is usually done—but by challenging the "treasure" comparison. A cellphone is not like a lockbox; it is more like the mind. In other words, decrypted data is *always* privileged testimony when it is extracted directly from within the chassis of a cellphone.

The strongest support for this radical notion comes straight from the

---

then the government should not be able to invoke the foregone conclusion doctrine. However, the foregone conclusion doctrine is difficult to rationalize and has not been applied in a consistent manner.

7. Laurent Sacharoff, *What Am I Really Saying When I Open My Smartphone?*, 97 TEXAS L. REV. ONLINE 63, 64, 67–68 [hereinafter Sacharoff, *Smartphone*]; Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 FORDHAM L. REV. 203, 234–37 (2018) [hereinafter Sacharoff, *Unlocking the Fifth Amendment*]; *see also In re* Grand Jury Subpoena Duces Tecum, 670 F.3d 1335, 1344 (11th Cir. 2012).

8. *Contra* Kerr, *supra* note 1, at 788 (arguing that the two particularity requirements "serve different roles and satisfy different standards"); *cf.* Dan Terzian, *Forced Decryption as a Foregone Conclusion*, 6 CAL. L. REV. CIR. 27, 29–30 (2015) ("The government's demand for the unencrypted version tells the respondent exactly what needs to be produced[.]").

9. *See* Bryan H. Choi, *For Whom the Data Tolls: A Reunified Theory of Fourth and Fifth Amendment Jurisprudence*, 37 CARDOZO L. REV. 185, 195–96 (2015) ("Data records are cognitive prosthetics . . . ."); Sacharoff, *Unlocking the Fifth Amendment*, *supra* note 7, at 250 (describing the passcode as "the corpus callosum between our minds and our vast repositories of personal information"); Stephen B. Wicker, *Smartphones, Contents of the Mind, and the Fifth Amendment*, COMM. ACM, Apr. 2018, at 28, 29–30 (collecting commentary on Martin Heidegger's theory of phenomenology and the use of smartphones as an extension of mind). *See generally* Lawrence B. Solum, *Legal Personhood for Artificial Intelligences*, 70 N.C. L. REV. 1231, 1239 & n.28 (1992) (". . . *X* may be given the legal status of personhood in order to confer rights on *Y*.").

horse's mouth. In *Riley v. California*[10], the Supreme Court introduced a new rule of cellphone exceptionalism, marveling at the "immense storage capacity," the "pervasiveness" of popular use, and the "qualitatively different" precision and comprehensiveness of recordkeeping performed by everyday cellphones.[11] The Court began this discussion with a passing quip that "the proverbial visitor from Mars might conclude [cellphones] were an *important feature of human anatomy*."[12] Four years later, in *Carpenter v. United States*[13], the Court quoted the same language—that cellphones are "almost a 'feature of human anatomy'"—to extend the rule of cellphone exceptionalism and strike down the warrantless use of a cellphone's locational data.[14] As the Court made clear in both cases, this holding is one of exceedingly narrow scope: it extends only to cellphones, not to any other devices.[15]

Cellphones are always-in-use devices. Unlocking a cellphone reveals the user's last activities, including which apps are open, the sequence in which they were last used, and notes that are in the midst of being composed.

10. 134 S. Ct. 2473 (2014).

11. *Id.* at 2489–91.

12. *Id.* at 2484 (emphasis added).

13. 138 S. Ct. 2206 (2018).

14. *Id.* at 2218 (2018) (quoting *Riley*, 134 S. Ct. at 2484). In isolation, this quote could be dismissed as droll hyperbole, but a simple joke would not bear repetition in the Supreme Court Reporter.

15. *Id.* at 2220 ("Our decision today is a narrow one. . . ."); *Riley*, 134 S. Ct. at 2494–95 ("Modern cell phones are not just another technological convenience."); *see also* City of Ontario v. Quon, 560 U.S. 746, 760 (2010) ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification.").

It also offers user-facing background data, such as notifications and reminders, fitness and locational tracking, and recent payments. Deeper in the background are valuable system performance metrics such as network usage, memory usage, battery usage, and other metadata generated dynamically rather than statically.[16] In aggregate, the modern cellphone snapshots its user's thoughts in real time.[17] Even accepting arguendo that every cellphone user voluntarily "consents" to the automatic creation of a nanosecond-by-nanosecond record of their existence, the lesson of *Riley* and *Carpenter* is that when it comes to cellphones, quantitative differences are qualitative ones too.[18]

Although both *Riley* and *Carpenter* were brought as Fourth Amendment petitions, the Court understood that the implications would run into the Fifth Amendment. In *Carpenter*, Justice Alito wrote a strident dissent that affording cellphones special protections was akin to "resurrect[ing]" *Boyd v. United States*[19]—the landmark case that had erected the Fourth and Fifth Amendments as overlapping protections for private papers.[20] Only Justice

16. *See generally* RICK AYERS ET AL., NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, GUIDELINES ON MOBILE DEVICE FORENSICS 15–20, 40–42, 48–50 (2014).

17. *But cf.* Nita A. Farahany, *Incriminating Thoughts*, 64 STAN. L. REV. 351, 388–89 (2012) (arguing that the privilege should not apply to "the retrieval of memorialized evidence, whether stored in the brain, in electronic circuits, or on paper").

18. *See Carpenter*, 138 S. Ct. at 2220 ("[This case] is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years. . . . [I]n no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements." (citation omitted)); *Riley*, 134 S. Ct. at 2488 ("That is like saying a ride on horseback is materially indistinguishable from a flight to the moon.").

19. 116 U.S. 616 (1886).

20. *Carpenter*, 138 S. Ct. at 2253 (Alito, J., dissenting) (complaining that *Boyd* was "the first—and, until today, the only—case in which this Court has ever held the compulsory production of

Thomas joined Justice Alito. Meanwhile, in a separate opinion, Justice Gorsuch mused that "we would do well to reconsider" the testimony doctrine, because "there is substantial evidence that the privilege against self-incrimination was also originally understood to protect a person from being forced to turn over potentially incriminating evidence."[21] Justice Gorsuch's dicta echoed more forceful statements made by Justice Thomas in an earlier case, *United States v. Hubbell*.[22]

Taken together, these cases reveal deep discomfort with treating cellphones like other digital devices. And the expressed nature of that discomfort signals that the reverberations may stretch from the Fourth Amendment to the Fifth Amendment and well beyond.

* * *

At least three salutary effects follow from the premise that cellphones are not only a feature of human anatomy but an extension of self.

First, this shift in framing would help resolve the uncomfortable doctrinal split between memorized passphrases and biometric passcodes.[23] Within the computer security field, biometric means of authentication are

documents to the same standard as actual searches and seizures"); *id.* at 2255 (expressing frustration that the majority has adopted "a resurrected version of *Boyd*"); *see also* Choi, *supra* note 9, at 189–93 (describing the evolution of doctrine since *Boyd*).

21. *Carpenter*, 138 S. Ct. at 2271 (Gorsuch, J., dissenting).

22. 530 U.S. 27, 49 (2000) (Thomas, J., concurring) ("A substantial body of evidence suggests that the Fifth Amendment privilege protects against the compelled production not just of incriminating testimony, but of any incriminating evidence.").

23. *Cf.* Orin S. Kerr, *Are We Overprotecting Code? Thoughts on First-Generation Internet Law*, 57 WASH. & LEE L. REV. 1287, 1288–89 (2000) (arguing that the regulation of code should be attuned to its function, not just its form).

generally regarded as more secure than conventional passcodes, because they are more easily guarded, more difficult to spoof, and less likely to go missing.[24] In the legal domain, the opposite holds true: biometric features are readily seized and repurposed for law enforcement aims.[25] Under the current situation, it is as though straw houses were legally shielded from police entry but brick houses were not.

An increasing number of courts have begun to rebel against this artificial schism. Thus far, a slight majority of courts that have considered this question have adopted Kerr's approach and authorized compelled decryption of cellphones regardless of what the mode of authentication is. This judicial turn achieves the desired result of harmonization—but at the cost of twisting the doctrine beyond recognition. In the past, a subject would never have been required to lift a finger to produce arbitrary, unspecified documents without first receiving an offer of immunity from prosecution.[26]

A sharp minority view has refused to compel decryption regardless

---

24. N.K. Ratha et al., *Enhancing Security and Privacy in Biometrics-Based Authentication Systems*, 40 IBM SYS. J. 614, 614–15 (2001). More accurately, the attack vectors are different. A more robust protection scheme might rely on a hybrid of biometric and memorized tokens, akin to two-factor authentication.

25. Schmerber v. California, 384 U.S. 757, 765 (1966) (holding that blood sample could be withdrawn and tested for intoxication because the test result "was neither petitioner's testimony nor evidence relating to some communicative act or writing by the petitioner"); *see also* Maryland v. King, 569 U.S. 435, 472–76 (2013) (Scalia, J., dissenting) (describing use of DNA database to assist with unsolved crimes and complaining that "taking DNA samples from arrestees has nothing to do with identifying them"). *See generally* Margaret Hu, *Biometric ID Cybersurveillance*, 88 IND. L.J. 1475 (2013).

26. *Hubbell*, 530 U.S. at 45 (rejecting "foregone conclusion" rationale where "the Government has not shown that it had any prior knowledge of either the existence or the whereabouts of the . . . documents ultimately produced by respondent") (citing Kastigar v. United States, 406 U.S. 441 (1972)).

whether the passcode is memorized or biometric. This approach is quite straightforward to parse as soon as one treats the cellphone as an extension of the subject's mind. Under that assumption, the government may not compel the cellphone to read a passcode in order to reveal its contents, any more than the government may compel the subject to read aloud his own diary in order to reveal his state of mind.[27] The fact that the government has access to the biometric feature turns out to be inconsequential, because the thing to be unlocked—the cellphone—remains privileged.

Second, this personification of cellphone *ex rel.* owner applies only to the device itself, not to the data contained therein.[28] Even if the Fifth Amendment bars the government from extracting any encrypted data residing "at rest" on the cellphone, it does not stand in the way of other surveillance techniques to capture data after it has departed the cellphone.[29] By analogy, a thought remains a thought only as long as it remains locked in one's mind. Thus third-party informants will always remain a weak link, even with end-

27. *See* Amar & Lettow, *supra* note 5, at 921; *cf.* Barrett v. Acevedo, 169 F.3d 1155, 1168 (8th Cir. 1999) (examining circuit split as to whether personal diaries can be subpoenaed). Such compulsion of internal state-of-mind is distinguishable from the compulsion of voice exemplars "solely to measure the physical properties of the witnesses' voices." United States v. Dionisio, 410 U.S. 1, 7 (1973). *But see* Richard Nagareda, *Compulsion "to Be a Witness" and the Resurrection of* Boyd, 74 N.Y.U. L. REV. 1575, 1628–29 (1999) (arguing that the compelled creation of a voice exemplar is "indistinguishable from a compelled oral statement while in police custody").

28. Couch v. United States, 409 U.S. 322, 328 (1973) ("It is important to reiterate that the Fifth Amendment privilege is a *personal* privilege: it adheres basically to the person, not to information that may incriminate him.").

29. *See* Roger Dingledine & Nick Mathewson, *Anonymity Loves Company: Usability and the Network Effect*, *in* SECURITY AND USABILITY: DESIGNING SECURE SYSTEMS THAT PEOPLE CAN USE 547, 548–49 (Lorrie Faith Cranor & Simson Garfinkel eds., 2005).

to-end encryption.[30] Additionally, intermediaries will continue to have access to routing and quality-of-service metadata, such as cell-site location information, which can be obtained with warrant.

Another important implication of this division between device and data is that it throws further weight behind those judicial decisions that have allowed compelled decryption of specific files known by the government to exist.[31] A subpoena for specific digital files does not implicate the cellphone itself, just as a subpoena for specific tax files does not implicate the subject himself.[32] There, the target is the known files, not the cellphone, such that the location of those files becomes irrelevant. Thus, this Essay corroborates Sacharoff's proposed rule of particularity for compelled decryption cases.[33] One flag of caution, however, is the potential to exploit the required records doctrine as an end run around any such rule of particularity.[34]

Third, compelled production of an entire decrypted cellphone is not like compelled production of discrete, named files. Direct access to the cellphone itself allows law enforcement to freeze-frame the user's state of mind at the time of arrest or seizure. A cellphone is more than the sum of its files. To be

30. *See* Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 985, 991, 999 (2016) (summarizing the mainstream consensus that "the solid edifice of the third party doctrine has begun to erode" but observing that "both courts and the academy have struggled to develop a workable scheme" to succeed it). *Contra* Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. (forthcoming 2019) (interpreting *Carpenter* to mean that "the Supreme Court has declared the third-party doctrine to be almost dead").

31. *See, e.g.*, *In re* Grand Jury Subpoena Duces Tecum, 670 F.3d 1335, 1349 (11th Cir. 2012).

32. Fisher v. United States, 425 U.S. 391, 411 (1976) ("The existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers.").

33. *See* Sacharoff, *Unlocking the Fifth Amendment*, *supra* note 7, at 231–35.

34. *See* Choi, *supra* note 9, at 214–16.

sure, certain files are static—such as image files and text messages—but those static files are situated within a dynamic environment that automatically captures the user's ongoing cognitive engagement. Cellphones never turn fully off; their memory state is preserved in transient files that remember the user's last active moment. In fact, when law enforcement requests blanket decryption of a cellphone, that just-in-time memory is a prime objective because it is the only type of evidence that cannot be produced in any other way. This capture of evanescent evidence is the antithesis of document production.[35]

* * *

This Essay closes by anticipating three key objections and offering a few additional thoughts on downstream implications for a personhood theory of cellphones.

First: The most substantial objection is that disallowing compelled decryption erects an impregnable zone of privacy that has never existed before—other than in the human mind.[36] For Kerr, the equilibrium-adjustment theorist, this change is unwelcome: a Fourth Amendment warrant has always been sufficient in the past to yield access to incriminating

35. *See* AYERS ET AL., *supra* note 16, at 41 ("[C]aution should be taken to avoid altering the state of a mobile device when handling it, for example, by pressing keys that may corrupt or erase data.").

36. *Contra* Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 816–18 (2005) (explaining that "the Fifth Amendment created a 'zone of privacy' around personal papers" until the latter half of the twentieth century); *see also* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 62–63 (2008) (describing early American attitudes treating the privacy of letters as "sacred" and "inviolable").

evidence, but that access would now be impeded by a new, extraneous barrier.[37] The balance of power would swiftly tilt in favor of criminals, to the detriment of public interest.

A pro forma response is that equilibrium-adjustment theory may be irrelevant to a Fifth Amendment analysis, which is typically thought to be more strictly categorical than the Fourth Amendment framework.[38] As long as the definition of "self" can be construed to encompass cellphones, it is not clear that the rule requires a coherent rationale.[39]

A more principled defense rests on the ground that a privilege against cellphone incrimination guards only the isolated contents of the device. As long as data remains sequestered within the cellphone, it can cause no more harm to the outside world than an idle murderous thought. But any data that contacts the outside world immediately loses its privilege, just as any thought communicated to another person does.[40] Thus ordinary surveillance methods

37. Kerr, *supra* note 1, at 791–94 (discussing Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011)).

38. *Id.* at 792 ("[P]erhaps equilibrium-adjustment is solely a Fourth Amendment dynamic that should not extend beyond it."); Sacharoff, *Unlocking the Fifth Amendment*, *supra* note 7, at 248 (noting the common stance of those who "reject any balance between the Fourth and Fifth Amendment" and believe "the Fourth Amendment already contains the relevant balance between privacy and disclosure"). *But see* David Alan Sklansky, *Two More Ways Not to Think About Privacy and the Fourth Amendment*, 82 U. CHI. L. REV. 223, 235–41 (2015) (critiquing the basic validity of equilibrium-adjustment theory).

39. *See* Amar & Lettow, *supra* note 5, at 857–58 ("From the beginning it lacked an easily identifiable rationale . . . ."); John H. Langbein, *The Historical Origins of the Privilege Against Self-Incrimination at Common Law*, 92 MICH. L. REV. 1047, 1084 (1994) ("Across the centuries the privilege against self-incrimination has changed character profoundly . . . .").

40. This rule extends to cloud computing where the content is subpoenaed from a cloud service provider rather than from the cellphone. Even if fiduciary duties were applicable to the Fourth Amendment analysis, see for example Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611 (2015), they play no role in the Fifth Amendment self-incrimination setting. Thus, compelling a third-party intermediary to assist with remote decryption—as opposed to direct

should continue to remain quite effective.[41] Data communications are pervasive and highly leaky, and even the widespread availability of end-to-end encryption cannot erase the basic incentives for third parties (including but not limited to co-conspirators) to cooperate with prosecutors.[42] In short, it is not empirically obvious that extending the self-incrimination privilege to cellphones would alter overall rates of criminal prosecution.[43] A privilege limited to cellphones does not "resurrect *Boyd*" any more than a privilege limited to spouses or to clergy.[44] And to the extent that the

decryption of the device itself—would not raise any Fifth Amendment concerns. *See also* Elizabeth Pollman, *Reconceiving Corporate Personhood*, 2011 UTAH L. REV. 1629, 1647–49 (2011) (discussing judicial recognition of corporate criminal liability). The same analysis can be applied to other forms of remote data such as cell-site location information.

41. *See* David W. Opderbeck, *Encryption Policy and Law Enforcement in the Cloud*, 49 CONN. L. REV. 1657, 1662 (2017) ("[E]ncryption does not change the fact that traditional methods of investigation and surveillance remain fundamentally important in the digital age."); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) ("We do not . . . call into question conventional surveillance techniques and tools, such as security cameras.").

42. *See, e.g.*, John Leyden, *The 'One Tiny Slip' that Put LulzSec Chief Sabu in the FBI's Pocket*, REGISTER (Mar. 7, 2012), https://www.theregister.co.uk/2012/03/07/lulzsec_takedown_analysis/ [https://perma.cc/95G6-KX85].

43. *Cf.* Miriam H. Baer, *Sorting Out White-Collar Crime*, 97 TEXAS L. REV. 225, 226–27, 226 nn.1–3 (2018) (collecting scholarly debate whether white-collar crime is overcriminalized or underenforced); Stephen J. Schulhofer, Miranda, Dickerson, *and the Puzzling Persistence of Fifth Amendment Exceptionalism*, 99 MICH. L. REV. 941, 942–43, 942 n.4 (2001) (reciting "very dead" empirical debate whether *Miranda* warnings resulted in lost convictions). *See generally* Herbert L. Packer, *Two Models of the Criminal Process*, 113 U. PA. L. REV. 1, 63 (1964) ("Every significant move in the Due Process direction has been greeted with predictions of an imminent breakdown in the criminal process.").

44. *See* DAN MARKEL ET AL., PRIVILEGE OR PUNISH: CRIMINAL JUSTICE AND THE CHALLENGE OF FAMILY TIES 3–5 (2009) ("[W]ithout such protections, marriages would lack the open conversation appropriate for a confidential relationship."); R. Michael Cassidy, *Sharing Secrets: Is It (Past) Time for a Dangerous Person Exception to the Clergy-Penitent Privilege?*, 44 WM. & MARY L. REV. 1627, 1632–35 (2003) ("Privileges are recognized only when necessary to preserve relationships that society values above the truth-finding functions of its courts."). The trouble with *Boyd* was that it threatened to sweep *all* evidence beyond the reach of law enforcement. *See* Fisher v. United States, 425 U.S. 391, 409 (1976) (rejecting the "mere evidence" rule as a rationale for applying *Boyd* to private papers). To be sure, *Fisher* is sometimes read as having overturned *Boyd* in its entirety. *See, e.g.*, United States v. Doe, 465 U.S. 605, 618 (1984) (O'Connor, J., concurring) (alleging that *Fisher* "sounded the death-knell for *Boyd*"). But *Fisher* did not anticipate modern cellphones, nor did it foreclose other canons parallel to the "act of production" rule.

government's true purpose is something other than prosecution (such as victim rescue or anti-terrorism), it can always compel decryption by offering immunity.[45]

Second: Even if one accepts the premise that cellphones are a "feature of human anatomy,"[46] one might resist the conclusion that anatomical features are *per se* eligible for self-incrimination privileges.[47] The Supreme Court has authorized all manner of bodily invasions, as long as the need is sufficiently great.[48] Why should cellphones be any different?

The thin answer is that a nonconsensual giving of bodily evidence can be compelled only for authentications of identity or for inspections of physical attributes such as body shape, movement, or timbre.[49] Any time one's body is commandeered without being tethered to one of those limited,

45. *See* William J. Stuntz, *Self-Incrimination and Excuse*, 88 COLUM. L. REV. 1227, 1273–74, 1278 (1988) (explaining the doctrine of use immunity and noting that "the grant of immunity must as a practical matter cover the document's *contents*").

46. *See supra* notes 12–14 and accompanying discussion.

47. Schmerber v. California, 384 U.S. 757, 763–64 (1966).

48. *Compare* Winston v. Lee, 470 U.S. 753, 763–66 (1985) (applying reasonableness inquiry to decide whether law enforcement may extract a bullet lodged in suspect's body), South Dakota v. Neville, 459 U.S. 553, 563 (1983) (finding blood tests "so safe, painless, and commonplace" that the State could legitimately compel the suspect to accede to the test), *and Schmerber* 384 U.S. at 767 (holding that the human body is not "inviolate against state expeditions seeking evidence of crime"), *with* Birchfield v. North Dakota, 136 S. Ct. 2160, 2178 (2016) (finding heightened constitutional protections against blood tests because they "require piercing the skin" and "extract[ing] a part of the subject's body"), *and* Rochin v. California, 342 U.S. 165, 173 (1952) ("It would be a stultification of [the constitutional responsibility of] this Court to hold that in order to convict a man the police cannot extract by force what is in his mind but can extract what is in his stomach.").

49. *See* Hiibel v. Sixth Judicial Dist. Ct., 542 U.S. 177, 189–91 (2004) (compelled disclosure of identity presents no reasonable danger of incrimination); Pennsylvania v. Muniz, 496 U.S. 582, 597 (1990) (noting that "the cases upholding compelled writing and voice exemplars did not involve situations in which suspects were asked to communicate any personal beliefs or knowledge of facts"); United States v. Greer, 631 F.3d 608, 613 (2d Cir. 2011) (distinguishing use of tattoo as "an identifying physical characteristic" from its use for the "content of what [was] written" (quoting Gilbert v. California, 388 U.S. 263, 266–67 (1967))).

enumerable purposes, such compulsion should be privileged by default because it is likely a pretext for intercepting one's cognitive processes. Compelled decryption of cellphones does not ever meet either of those limited purposes.[50]

The thicker claim is that the Court's analogy to "human anatomy" refers specifically to the mind, not merely to an outer appendage. Being parted from one's cellphone is like losing one's memory and one's mental map of the world.[51] The intrusion of allowing the government to browse freely through one's phone is that it infringes on one's unpublished thoughts before they can be composed and put in order.[52] Prosthetic limbs do not trigger comparable concern, even when they are wired directly into the brain. Cellphones are not

50. One could imagine, however, being required to furnish a device serial number, MAC address, or equivalent identification. *See Hiibel*, 542 U.S. at 189; *cf.* United States v. Freed, 401 U.S. 601, 603–04, 605 (1971) (no privilege against required registration of firearms). A closer question is whether police could compel "textalyzer" data that reveals only whether the cellphone was in use. Ryan Tarinelli, *Nevada Considers Technology to Scan Cellphones After Crashes*, ASSOCIATED PRESS (Mar. 17, 2019), https://apnews.com/bf1d727c11be476b8446437ed67bd626 [https://perma.cc/69K6-NVHM] (citing whitepaper by Ric Simmons opining that "testing a cellphone after a crash is 'minimally intrusive'"); *cf.* California v. Byers, 402 U.S. 424, 430–31 (1971) (plurality opinion) (statute may require disclosure of data as long as that data is not "inherently suspect of criminal activities" (quoting Marchetti v. United States, 390 U.S. 39, 47 (1968))).

51. *See* Marc Jonathan Blitz, *Freedom of Thought for the Extended Mind: Cognitive Enhancement and the Constitution*, 2010 WIS. L. REV. 1049, 1073–75 (2010) (discussing Andy Clark & David Chalmers, *The Extended Mind*, *in* ANDY CLARK, SUPERSIZING THE MIND: EMBODIMENT, ACTION, AND COGNITIVE EXPERIENCE, app. at 220–32 (2008)).

52. *See* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 1008–10 (1996) (discussing cases invalidating government inspection of private materials that reveal the content of a person's thoughts); Seana Valentine Shiffrin, *A Thinker-Based Approach to Freedom of Speech*, 27 CONST. COMMENT. 283, 285, 294 (2011) (arguing that "forms of discourse meant primarily for self-consumption" should be strongly protected because "it is essential to the appropriate development and regulation of the self . . . that one has protection from unchosen interference with one's mental contents from processes that would disrupt or disable the operation of these processes"); *cf.* Bryan H. Choi, *A Prospect Theory of Privacy*, 51 IDAHO L. REV. 623, 626 (2015) (advancing an economic argument for privatizing personal data).

an extension of physical anatomy; they are an extension of *thinking* anatomy.

Third: What are the limits of a rule recognizing cellphones as an extension of self? The clear directive of *Riley* and *Carpenter* is that cellphones are unique, full stop.[53] By proposition, this rule cannot extend to laptops, portable drives, home electronics, or other generic personal devices. While all digital devices share the same basic architectural design, none other captures the pervasive and comprehensive cognitive engagement that cellphones do. For another device to receive equivalent recognition, it would need to match the profound intimacy of the cellphone. In that regard, this Essay stakes out a different position than Kerr and others who see no easy limiting principles to draw between digital devices.[54]

At the same time, a cellphone remains merely an *extension* of self.[55] Death moots any specter of self-incrimination; the cellphone does not embody a person after death.[56] Likewise, cellphones can be replaced or

53. *See supra* note 15.

54. *Compare* ORIN S. KERR, THE DIGITAL FOURTH AMENDMENT ch.6 (forthcoming), https://ssrn.com/abstract=3301257 [https://perma.cc/Y2NK-TEGH] (arguing that *Carpenter* replaced the "traditional focus on places and things" with a new rule based on "information transfers"), *with* Ohm, *supra* note 30 (contending that the rule of *Carpenter* applies to any "massive database of information containing non-public information about individuals").

55. *See* Jack M. Balkin, *The Path of Robotics Law*, 6 CAL. L. REV. CIR. 45, 59 (2015) ("A key feature of robotic substitution is that it is *partial*. Robots and AI entities . . . are agents for a particular reason or function, straddling the line between selves and tools, or persons and instruments."); *cf.* Pollman, *supra* note 40, at 1655, 1665 (observing that "corporations have received many, but not all, of the protections and guarantees that are afforded to natural persons" and worrying that the personhood metaphor "may in fact impede or muddy consideration" of whether corporations should hold a certain right).

56. *See* Robert B. McKay, *Self-Incrimination and the New Privacy*, 1967 SUP. CT. REV. 193, 218 n.103 (noting that *Costello v. United States*, 352 F.2d 848 (2d Cir. 1965), *cert. granted*, 383 U.S. 942 (1966), "was mooted before argument by the death of petitioner"). *Compare* Jason Mazzone, *Facebook's Afterlife*, 90 N.C. L. REV. 1643, 1654–55, 1655 nn.58–59 (2012) (noting that, under American law, classic privacy rights die with the person), *with* Brian R. Hood, Note, *The*

discarded without implicating loss of self. Impoundment and damage by law enforcement may be subject to laws governing chattel rather than bodily injury.[57] In these and other sanity tests, the lodestar should be whether the claim of cellphone qua self is directed against law enforcement action that materially interferes with the subject's freedom of thought.[58]

Two edge cases are worth special mention. The more trivial case is the unencrypted cellphone. In the Fourth Amendment setting, opening the device remains a "search" but the device's unencrypted status makes available justifications such as plain-view and exigency. Likewise in the Fifth Amendment setting, the cellphone remains part of the "self" but the device's unencrypted status voids the element of compulsion.[59] That said, the case of the unencrypted cellphone may be a rapidly diminishing set as device manufacturers move to make encryption the default setting.

Attorney–Client Privilege and a Revised Rule 1.6: Permitting Limited Disclosure After the Death of the Client, 7 GEO. J. LEGAL ETHICS 741, 743–44, 744 n.8 (1994) (collecting cases holding that an attorney's duty of confidentiality "generally survives the client's death").

57. *Cf. In re* Apple Inc. Device Performance Litig., 347 F. Supp. 3d 434, 455–56 (N.D. Cal. 2018) (allowing trespass-to-chattels claim).

58. *See* Murphy v. Waterfront Comm'n, 378 U.S. 52, 55 (1964) (explaining that the privilege against self-incrimination reflects "our respect for the inviolability of the human personality and of the right of each individual 'to a private enclave where he may lead a private life'" (citation omitted)).

59. *See* Barrett v. Acevedo, 169 F.3d 1155, 1168 (8th Cir. 1999) (finding no compulsion where journal was abandoned in public); *cf.* Donald A. Dripps, *Against Police Interrogation—And the Privilege Against Self-Incrimination*, 78 J. CRIM. L. & CRIMINOLOGY 699, 700 (1988) ("[T]he bulk of confessions results from irrationality, mistake, and manipulation."); David S. Kaplan & Lisa Dixon, *Coerced Waiver and Coerced Consent*, 74 DENV. U. L. REV. 941, 947–48 (1997) ("In the context of the Fifth Amendment . . . voluntariness is defined as the absence of government coercion rather than the defendant's exercise of volition."); Ric Simmons, *Not "Voluntary" but Still Reasonable: A New Paradigm for Understanding the Consent Searches Doctrine*, 80 IND. L.J. 773, 790–94 (2005) (discussing the "intermediate, acceptable level of compulsion" allowed under *Miranda v. Arizona*, 384 U.S. 436 (1966)).

The more troubling edge case is where title and possession are split.[60] The most well-known case to date is that of the San Bernardino shooter, where the cellphone at issue was owned by an employer and provided to an employee for business use.[61] Other popular split arrangements include lease financing, family plans, and short-term rentals. Resolution of these cases may depend on diverse factors such as the titleholder's right of access, the frequency of such access, and the licensee's customary use.

Finally: This Essay has focused on compelled decryption and the privilege against self-incrimination, but it is worth leaving a few breadcrumbs on where a cellphone–personhood theory might lead in other related contexts. For example, the literature on data commodification is already abundantly rich,[62] but more could be written on the ethics of allowing users to monetize their cellphone use.[63] Other debates potentially enriched by a cellphone–personhood theory are those rooted in equal protection and due

60. *See, e.g.*, City of Ontario v. Quon, 560 U.S. 746, 750–53 (2010).

61. Associated Press v. FBI, 265 F. Supp. 3d 82, 89 (D.D.C. 2017).

62. *See generally* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000); Pamela Samuelson, *Privacy As Intellectual Property?*, 52 STAN. L. REV. 1125 (2000).

63. *See* Mike Isaac, *Flexing Power, Apple Paralyzes Facebook in 'Secret' App Feud*, N.Y. TIMES, Feb. 1, 2019, at A1, https://www.nytimes.com/2019/01/31/technology/apple-blocks-facebook.html [https://perma.cc/ZEW5-7ACA]; *see also* Mike Isaac, *Uber Tallies the Costs of Its Leader's Drive to Win at Any Price*, N.Y. TIMES, Apr. 24, 2017, at A1, https://www.nytimes.com/2017/04/23/technology/travis-kalanick-pushes-uber-and-himself-to-the-precipice.html [https://perma.cc/UQK9-3Z55]; *cf.* TIM WU, ATTENTION MERCHANTS: THE EPIC SCRAMBLE TO GET INSIDE OUR HEADS 307 (2016) (worrying that "fame, or the hunger for it, would become something of a pandemic, swallowing up more and more people and leaving them with the scars of chronic attention-whoredom.").

process concerns, such as net neutrality,[64] border searches,[65] and right to record.[66] Last, the vexing issue of government hacking takes on an entirely different tenor when one characterizes the host as not just a repository of personal effects but as the emergent manifestation of a person's mind.[67]

64. *See generally* Jerry Kang, *Race.Net Neutrality*, 6 J. ON TELECOMM. & HIGH TECH. L. 1 (2007) (wielding race theory to illuminate deontological objections against net discrimination).

65. *See* United States v. Wanjiku, 919 F.3d 472, 483–85 (7th Cir. 2019). *See generally* Thomas Mann Miller, Comment, *Digital Border Searches After* Riley v. California, 90 WASH. L. REV. 1943 (2015).

66. *See generally* Clay Calvert, *The First Amendment Right to Record Images of Police in Public Places: The Unreasonable Slipperiness of Reasonableness & Possible Paths Forward*, 3 TEX. A&M L. REV. 131 (2015); Margot E. Kaminski, *Privacy and the Right to Record*, 97 B.U. L. REV. 167 (2017).

67. *See* Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570 (2018) (detailing the explosive growth in use of malware by federal law enforcement); *see also* Alan Butler, *When Cyberweapons End up on Private Networks: Third Amendment Implications for Cybersecurity Policy*, 62 AM. U. L. REV. 1203, 1230 (2013) (concluding that "[c]ivilian networked devices" are protected by the Third Amendment); Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 659 (2011) (arguing that government intrusions are particularly offensive when they occur where "so many of the pieces of an individual's life" are aggregated "into a complete picture which an individual may not wish to share with just anyone").