SMU | Dedman School of Law

SMU Law Review

Volume 72 | Issue 4 Article 10

January 2019

A Right to Go Dark (?)

David C. Gray
University of Maryland School of Law

A Right to Go Dark (?)

David Gray

ABSTRACT

In 2013, reports based on documents leaked by former National Security Agency contractor Edward Snowden revealed committed efforts by federal agencies to develop and deploy data surveillance technologies. These revelations documented the ability of government agencies to monitor internet usage, read the contents of communications, and access data stored in the cloud and on personal devices. These revelations marked a turning point in the public conversation as consumers became aware of the extent to which national security and law enforcement agencies can monitor a wide range of activities in physical and virtual spaces.

The market responded. Technology companies began to tout their commitments to privacy. Some waged quixotic battles to resist government requests for user information. Others deployed and promoted privacy-protective technologies. Google began encrypting data flows between their servers. Encrypted email and messaging services entered the mainstream. Hardware companies made encryption a standard feature on computers and mobile devices. As this new movement to "go dark" took hold, government officials, including then-Director of the Federal Bureau of Investigation (FBI) James Comey, went on the attack, arguing that encryption would hamstring law enforcement and threaten national security.

These issues came to a head in 2016 when the FBI sought access to an Apple iPhone recovered from the perpetrators of a December 2015 terrorist attack in San Bernardino, California. The FBI had a warrant to search the phone but could not serve that warrant because the phone was encrypted, and the sole possessor of the password was dead. The FBI sought the assistance of Apple to circumnavigate the phone's encryption. Apple refused and later contested a court order compelling the company to decrypt the phone. In addition to its own rights, Apple and its amici suggested that forcing a technology company to compromise encryption would threaten the rights of customers. The FBI eventually dropped the suit, but debates about a right to "go dark" persist, stoked by continuing complaints by government agencies and legislative proposals to limit the availability of robust encryption.

Debates about privacy and technology tend toward grand abstractions. This article takes a different tack by focusing on three potential doctrinal grounds for such a right: the Fourth Amendment, which governs searches and seizures; the Fifth Amendment, which bars compelled testimonial incrimination; and evidentiary rules on privilege, which sometimes protect information sharing between some parties. It concludes that shifts in the

law and the new ways we interact with technologies point to an emergent right to go dark.

TABLE OF CONTENTS

I. INTRODUCTION 622
II. A FOURTH AMENDMENT RIGHT TO GO DARK (?) 629
III. A FIFTH AMENDMENT RIGHT TO GO DARK (?) ... 644
IV. A COMMON LAW RIGHT TO GO DARK (?)..... 655
V. CONCLUSION 667

I. INTRODUCTION

ON December 2, 2015, environmental engineer Syed Rizwan Farook was attending a training event and holiday party at the Inland Regional Center with fellow employees of the San Bernardino, California Health Department.[1] At some point, Farook left the event, perhaps after a dispute with coworkers, but soon returned in the company of his wife Tashfeen Malik.[2] The couple had armed themselves with assault rifles, handguns, and pipe bombs.[3] They opened fire, killing fourteen people and wounding nearly two dozen more.[4] Then they fled the building, leaving behind a cluster of pipe bombs attached to a remote trigger, which blessedly never detonated.[5]

Law enforcement quickly identified Farook and Malik as the perpetrators. Later that day, the two were spotted driving in their sports utility vehicle.[6] A pursuit ensued. When officers succeeded in stopping and surrounding their vehicle, Farook and Malik again opened fire, wounding several officers on the scene.[7] Officers returned fire.[8] Both Farook and Malik were killed.[9] A search of their car turned up guns, bombs, and thousands of rounds of ammunition. As Federal Bureau of Investigation (FBI) official David Bowdich would later put it, "[T]here was obviously a mission here."[10]

1. Adam Nagourney et al., *San Bernardino Shooting Kills at Least 14; Two Suspects Are Dead*, N.Y. TIMES (Dec. 2, 2015), https://www.nytimes.com/2015/12/03/us/san-bernardino-shooting.html [https://perma.cc/XB6N-YSD7].
2. *Id.*
3. *Id.*
4. *Id.*
5. *Report Sheds Light on Chaos, Bloodshed of San Bernadino Terror Attack*, CBS NEWS, https://www.cbsnews.com/news/report-sheds-light-on-chaos-bloodshed-of-san-bernardino-terror-attack/ [https://perma.cc/CQZ3-JHRM] (last updated Sept. 10, 2016).
6. *Id.*
7. *Id.*
8. *Id.*
9. *Id.*
10. Doug Smith, *Federal Agents Investigating Possible Terrorism Link in San Bernardino Mass Shooting*, L.A. TIMES (Dec. 3, 2015), https://www.latimes.com/local/lanow/la-me-ln-fbi-probe-terror-link-san-bernardino-shooting-20151203-story.html [https://perma.cc/H2TF-AA27].

But what was that mission? Was it an act of revenge for workplace slights, real or imagined? Was the motive more sinister and far-reaching? Both Farook and Malik were Muslim, so some immediately suspected terrorism. But Farook was born in Illinois.[11] Malik was born in Pakistan but had immigrated legally.[12] She had also recently given birth to the couple's first child.[13] By outward appearances, they did not seem to be zealots or extremists. They had no known ties to terrorist groups. To the contrary, they appeared by all outward measures to live a comfortable middle-class life. But if not terrorism, then what could be the motive for their "mission"? And if this was an act of terrorism, then were they acting on their own or were they part of a network? Were more attacks coming? When? Where? Why? How? Who?

As these and other questions swirled in the hours and days after the attack, investigators identified a source of potentially valuable information: an iPhone 5C Farook carried for his work.[14] Armed with a warrant, officers obtained some information from Apple servers where back-up copies of some data from the phone were stored.[15] Unfortunately, those back-up copies were neither current nor complete.[16] Investigators needed to access the device, but it was running a recent update to Apple's iOS operating system, which meant that most of the data that would have been interesting to investigators, including contacts, mails, text messages, and photographs, were encrypted and out of reach without the passcode Farook had taken to his grave.[17] The software provided additional security, limiting the number of times agents could experiment with possible passcodes without risking permanent loss of the data.[18]

Stymied, officers asked Apple for assistance in decrypting the phone.[19] Apple declined.[20] Agents then sought and received an order from Magistrate Judge Sheri Pym compelling Apple to provide "reasonable technical assistance" to agents seeking to conduct a warranted search of the phone.[21] Apple again objected, this time taking its protest public.[22] In

11. Saeed Ahmed, *Who Were Syed Rizwan Farook and Tashfeen Malik?*, CNN (Dec. 4, 2015), https://www.cnn.com/2015/12/03/us/syed-farook-tashfeen-malik-mass-shooting-profile/index.html?no-st=1573583199 [https://perma.cc/EZ4U-ASFV].

12. *Id.*

13. *Id.*

14. *See* Declaration of Christopher Pluhar at 1–3, *In re* An Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. ED 15-0451M (C.D. Cal. Feb. 16, 2016).

15. *Id.*

16. *Id*. at 3–5.

17. *See id.* at 2–3.

18. *Id.* at 3.

19. Gov't's *Ex Parte* Application for Order Compelling Apple Inc. to Assist Agents in Search at 1–4, *In re* An Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. ED 15-0451M (C.D. Cal. Feb. 16, 2016).

20. *Id.*

21. Order Compelling Apple, Inc. to Assist Agents in Search at *1–2, *In re* An Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, 2016 U.S. Dist. LEXIS 20543 (C.D. Cal. Feb. 16, 2016) (No. ED 15-0451M).

22. *See, e.g.*, Sarah Parvini & Matt Hamilton, *Apple vs. FBI: Protestors Gather at the Grove in Support of Tech Giant's Defiance*, L.A. TIMES (Feb. 23, 2016), https://www.la

doing so, it brought the San Bernardino investigation into the middle of a debate between law enforcement and technology companies that had been brewing for years.[23]

In 2013, former National Security Agency (NSA) contractor Edward Snowden leaked more than a million top secret files to Glenn Greenwald and Laura Poitras of the *Guardian*.[24] Greenwald and Poitras began reporting on some of the programs revealed in these files in June 2013, revealing a broad-based effort by federal law enforcement and national security agencies to gather, access, store, and analyze a wide range of data, sometimes with the cooperation of technology companies and sometimes by more direct means, including hacking.[25] The Snowden revelations sparked broad public conversations about government surveillance, leading to some modest legislative and executive reforms. But, in June 2013, government investigators were concerned with Snowden himself. As part of their investigation, government agents sought access to an email account associated with Snowden and hosted by Lavabit.[26]

In 2013, Lavabit was at the vanguard of the movement to provide consumers with secure communications and data storage. Among its products was an email service boasting asymmetric encryption.[27] Agents served Lavabit with a court order and then a warrant seeking disclosure of the SSL keys to its encrypted email service.[28] Although Lavabit had in the past complied with search warrants for the contents of some of its users' accounts,[29] it refused to turn over its SSL keys to law enforcement because doing so would have compromised the privacy and data security of all its clients.[30] Faced with increasing pressure from the government and bound by a court-issued gag order, Lavabit ceased operations.[31] Soon after, a company called Silent Circle, which also provided encrypted com-

---

times.com/local/lanow/la-me-ln-apple-fbi-protesters-support-apple-defiance-20160223-story.html [https://perma.cc/Q94Z-NFA6].

23. *See* Geoffrey S. Corn & Dru Brenner-Beck, *"Going Dark": Encryption, Privacy, Liberty, and Security in the "Golden Age of Surveillance," in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 330, 363–68 (David Gray & Stephen Henderson eds., 2017) (recounting the history of encryption debates going back to the Clipper chip controversy in the 1990s).

24. Ewen MacAskill, *Edward Snowden: How the Spy Story of the Age Leaked Out*, GUARDIAN (June 12, 2013), https://www.theguardian.com/world/2013/jun/11/edward-snowden-nsa-whistleblower-profile [https://perma.cc/H6M9-BLN8].

25. *See id.*

26. Dominic Rushe, *Lavabit Founder Refused FBI Order to Hand Over Email Encryption Keys*, GUARDIAN (Oct. 3, 2013), https://www.theguardian.com/world/2013/oct/03/lavabit-ladar-levison-fbi-encryption-keys-snowden [https://perma.cc/U4FV-BN49].

27. Michael Phillips, *How the Government Killed a Secure E-Mail Company*, NEW YORKER (Aug. 9, 2013), https://www.newyorker.com/tech/annals-of-technology/how-the-government-killed-a-secure-e-mail-company [https://perma.cc/UB4T-EMAX].

28. *See id.*

29. *See generally, e.g.*, Bowman v. United States, 2017 WL 3594665 (N.D. Ohio Aug. 21, 2017) (No. 5:16CV162) (documenting Lavabit's compliance with a warrant for account information).

30. *See Phillips*, *supra* note 27.

31. Ledar Levison, *Secrets, Lies & Snowden's Email: Why I Was Forced to Shut Down Lavabit*, GUARDIAN (May 20, 2014), https://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email [https://perma.cc/9DPL-25DN].

munications services, closed its doors, citing worries that it could no longer guarantee the security of its products against court-backed efforts by government agents to gain access.[32]

Threats of legal pressure from government investigators forced Lavabit and Silent Circle to shutter their businesses, but the market for secure electronic communications, internet access, and data storage exploded in the weeks and months after the initial Snowden revelations.[33] That demand grew as citizens and consumers continued to learn about the extent of surveillance efforts by both government and private actors. At the same time, major technology firms like Google, Yahoo, and Apple faced public criticism on grounds that they had failed to protect their customers from government prying.[34] By 2014, many major technology players had responded by offering more robust encryption as an option on many of their devices, as well as encrypted communication and data storage platforms.[35] In September 2014, Apple went a step further, introducing default encryption as a feature of iOS 8.[36] Apple even claimed not to have or to keep encryption keys, crowing that, "[u]nlike our competitors, Apple cannot bypass your passcode, and therefore cannot access [encrypted] data."[37] Only users, armed with passcodes they selected, could decrypt their devices. IOS 8 converted consumer devices into unbreakable data lockboxes that could be accessed only with the cooperation of their users. Everyday consumers now had the ability to "go dark."

High-profile law enforcement and national security officials immediately criticized Apple for offering lock-down encryption on its devices. Then-Attorney General Eric Holder warned that, "[w]hen a child is in danger, law enforcement needs to be able to take every legally available step to quickly find and protect the child and to stop those [who] abuse children."[38] He continued, "It is worrisome to see companies thwarting

32. Parmy Olson, *Encryption App Silent Circle Shuts Down E-Mail Service 'To Prevent Spying'*, FORBES (Aug. 9, 2013), https://www.forbes.com/sites/parmyolson/2013/08/09/encryption-app-silent-circle-shuts-down-e-mail-service-to-prevent-spying/#4fa7a28e6376 [https://perma.cc/5H4K-XTM6].

33. A.W. Geiger, *How Americans Have Viewed Government Surveillance and Privacy Since Snowden Leaks*, FACT TANK (June 4, 2018), https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/ [https://perma.cc/4XQY-NJZM].

34. Micah Lee, *Apple Still Has Plenty of Your Data for the Feds*, INTERCEPT (Sept. 22, 2014), https://theintercept.com/2014/09/22/apple-data/ [https://perma.cc/FG7A-4XSW].

35. Steve Henn, *How Well Do Tech Companies Protect Your Data from Snooping?*, NPR (June 12, 2014), https://www.npr.org/sections/alltechconsidered/2014/06/12/320997037/how-well-do-tech-companies-protect-your-data-from-snooping [https://perma.cc/3VCF-4H3L].

36. Matthew Green, *Is Apple Picking a Fight with the U.S. Government?*, SLATE (Sept. 23, 2014), https://slate.com/technology/2014/09/ios-8-encryption-why-apple-wont-unlock-your-iphone-for-the-police.html [https://perma.cc/TW9R-LXGP].

37. David E. Sanger & Brian X. Chen, *Signaling Post-Snowden Era, New iPhone Locks out N.S.A.*, N.Y. TIMES (Sept. 26, 2014), https://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html [https://perma.cc/RL54-ZPGJ].

38. Kif Leswing, *Apple and the FBI Are in the Middle of a Huge Battle That Could Affect the Privacy of Millions of People—Here's Everything That's Happened So Far*, BUS.

our ability to do so."[39] Then-Director of the FBI James Comey charged that data encryption and encrypted communications platforms would compromise law enforcement and national security efforts.[40] The Chief of Detectives for the Chicago Police Department predicted that "Apple will become the phone of choice for the pedophile."[41]

These dire predictions seemed to prove out when agents found themselves locked out of Syed Farook's iPhone. Here were law enforcement officers in the midst of an urgent investigation with lives potentially in the balance. They had abided the most demanding Fourth Amendment standards, presenting their case to a federal judge and securing a probable cause warrant granting them access to the contents of the phone. But they could not exercise their lawful authority to search the phone because Apple had chosen to embed robust encryption in their operating system. Did Farook have a right to go dark? Did Apple have the right, as then-Attorney General Loretta Lynch asked, to make that decision for all of us about when and in what circumstances citizens and corporations can thwart legitimate law enforcement and national security operations?[42]

The near universal response on the part of government officials was "no."[43] Legislators began suggesting that companies should be required to maintain keys to their encrypted products in order to guarantee the ability of government agents to lawfully access data and devices through "backdoors."[44] Judge Pym issued an order under the All Writs Act com-

---

INSIDER (Mar. 2, 2016), https://www.businessinsider.com/fbi-vs-apple-history-of-apples-fight-over-the-locked-san-bernardino-shooters-iphone [https://perma.cc/HG6Y-2JTE].

39. *Id.*

40. Don Reisinger, *Former National Security Officials Support Encryption*, FORTUNE (Dec. 16, 2015), https://fortune.com/2015/12/16/national-security-encryption/ [https://perma.cc/G82K-NYJS].

41. Craig Timberg & Greg Miller, *FBI Blasts Apple, Google for Locking Police Out of Phones*, WASH. POST (Sept. 25, 2014), https://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html?utm_term=.deb4b6708d9c [https://perma.cc/T6FF-5DVX].

42. Thomas Brewster, *Loretta Lynch Says Americans Back DoJ in Fight to Unlock Apple's iPhones*, FORBES (Mar. 1, 2016), https://www.forbes.com/sites/thomasbrewster/2016/03/01/iphone-backdoors-loretta-lynch/#368c02dd1510 [https://perma.cc/U256-QMP7].

43. The exception here is General Michael Hayden, former director of the NSA and the Central Intelligence Agency. In the middle of the encryption controversy after San Bernardino, he took the position that everyone should have the right to deploy and use robust encryption but that the intelligence agencies would have a reciprocal right to develop and deploy decryption tools and then it would be "game on" for the NSA to break it. *See Michael Hayden: America Is Safer with End-to-End Encryption*, NPR (Mar. 1, 2016), https://www.wbur.org/onpoint/2016/03/01/michael-hayden-nsa-encryption [https://perma.cc/6QW8-PF65]; Jose Pagliery, *Ex-NSA Boss Says FBI Director Is Wrong on Encryption*, CNN (Jan. 13, 2016), https://money.cnn.com/2016/01/13/technology/nsa-michael-hayden-encryption/index.html [https://perma.cc/GKX9-KXLJ].

44. That push for legislation granting law enforcement and intelligence agencies access to encrypted data ended when Congress failed to pass the Compliance with Court Orders Act of 2016. *See* Andy Greenberg, *The Senate's Draft Encryption Bill Is 'Ludicrous, Dangerous, Technically Illiterate'*, WIRED (Apr. 8, 2016), https://www.wired.com/2016/04/senates-draft-encryption-bill-privacy-nightmare/ [https://perma.cc/7PTD-WMWE]. The effort was revived recently when FBI Director Christopher Wray suggested that law enforcement officers have been unable to access 7,800 devices because of encryption. *See* Morgan Chalfant, *New Push to Break Deadlock Over Encrypted Phones*, HILL (Apr. 8, 2018), https://the

pelling Apple to create an access point into Farook's phone by developing technology capable of circumnavigating the encryption on his iPhone.[45] Apple resisted, relying in part on its own First Amendment rights.[46] Technology companies, civil libertarians, academics, and others jumped to Apple's defense, arguing that limiting the ability of companies to develop and deploy encryption technologies would compromise privacy interests, render a whole range of sensitive information vulnerable, threaten First Amendment rights to association and freedom of the press, expose political activists in repressive regimes to threats of death, and impede technological development.[47]

The Apple encryption controversy raised important questions of constitutional rights and public policy that ultimately went unanswered. The FBI identified a private contractor who was able to unlock Farook's iPhone, effectively mooting the case.[48] But the going dark debate has continued to simmer.[49] Legislation compelling the installation of backdoors has been introduced here and in other western democracies.[50] Law enforcement agents have continued to criticize technology compa-

---

hill.com/policy/cybersecurity/382048-new-push-to-break-deadlock-over-encrypted-phones [https://perma.cc/HAQ3-LVE3]. The Senate Judiciary Committee has also been working with technology industry players to find a means to grant law enforcement access to encrypted data. *Id.*

45. Order Compelling Apple, Inc. to Assist Agents in Search, *supra* note 21, at *1–4.

46. Apple Inc's Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Gov't's Motion to Compel Assistance at 32–34, *In re* An Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. ED 15-0451M (C.D. Cal. Feb. 16, 2016) [hereinafter Apple Inc's Motion to Vacate Order].

47. Among the organizations and groups filing briefs in the case were: Access Now and Wickr Foundation; ACLU of Southern California; ACT, the App Association; Electronic Frontier Foundation and Technologists, Researchers, and Cryptographers; Privacy International and Human Rights Watch; Airbnb, Inc.; Atlassion Pty. Ltd.; Automattic Inc.; CloudFlare, Inc.; eBay Inc.; GitHub, Inc.; Meetup, Inc.; reddit, Inc.; Square Inc.; Squarespace, Inc.; Twilio Inc.; Twitter, Inc.; and Wickr Inc.; AT&T Mobility LLC; Intel Corporation; Amazon.com, Box, Cisco Systems, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest, Pinterest, Slack, Snapchat, WhatsApp, and Yahoo; AVG Technologies, The Computer & Communications Industry Association, Data Foundry, Golden Frog, The Internet Associations and the Internet Infrastructure Coalition; The Electronic Privacy Information Center (EPIC); BSA, The Software Alliance, the Consumer Technology Association, the Information Technology Industry Council, and Tech Net; Center for Democracy and Technology; The Media Institute; Non Party Law Professors; iPhone Security and Applied Cryptography Experts Dino Dai Zovi et al.; Richard Taub; and Lavabit LLC.

48. *See* Samantha Masunaga, *FBI Doesn't Have to Say Who Unlocked San Bernadino Shooter's iPhone, Judge Rules*, L.A. TIMES (Oct. 2, 2017), https://www.latimes.com/business/la-fi-tn-fbi-iphone-20171002-story.html [https://perma.cc/JF6T-RMTZ].

49. *See* Corn & Brenner-Beck, *supra* note 23, at 333–38 (recounting the modern "going dark" debate).

50. *Compare Telecommunications and Other Legislation Amendment (Assistance and Access) Act Bill 2018* (Cth) (Austl.) (enabling law enforcement and intelligence agencies to compel access to encrypted communications), *with* Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation [TKÜV] [Telecommunications Monitoring Order], Mar. 11, 2005, BGBL at 3136 (Ger.) (requiring that telecommunication service providers be able to surveil communications), *and* the Investigatory Powers Act 2016, 2 c. 25, § 253 (Gr. Brit.) (permitting the Secretary of State to serve notice on telecommunication providers of a requirement to technical assistance), *and* the proposed American legislation discussed *supra* note 44.

nies for developing and installing encryption in their products.[51] And technology companies have continued to assert their purported rights to develop and deploy encryption and other technologies that enhance the ability of users to go dark.[52] Lavabit has even reopened its doors, offering a new suite of products offering secure communication and data storage.[53] Amidst all of this conversation and activity, the privacy interests of citizens and consumers have been part of the conversation, but there has been shockingly little effort to explain whether and how those privacy interests might support a right to go dark. This article aims to fill that gap.

Do we have the right to go dark? It is a question that grows more important as digital communications, data storage, smart devices, and internet connected products ranging from phones to refrigerators become increasingly central to our lives. Take, as an example, personal devices like smartphones and wearable fitness trackers. These devices can and must gather intimate information in order to provide services and user benefits. Many devices also gather a range of rather quotidian information that, when aggregated and analyzed, can be quite revealing.[54] It is therefore natural to consider much of the information these devices gather to be private.[55] But that does not answer the going dark question. Information can be private but still accessible to government agents through lawful means, such as warranted searches.[56] To ask whether citizens and consumers have a right to go dark is, therefore, to ask whether they have a right to act as the sole conduits to their data by deploying technological means that guarantee absolute immunity from government intrusion and information gathering without their cooperation.

---

51. Then-Deputy Attorney General Rod Rosenstein accused tech companies of being unwilling to develop "responsible encryption" and asserted that the public will bear the cost of law enforcement's inability to access encrypted data. *See* Sari Horwitz, *Justice Dept. Might More Aggressively Seek Encrypted Data from Tech Companies*, WASH. POST (Oct. 10, 2017), https://www.washingtonpost.com/world/national-security/justice-dept-might-more-aggressively-seek-encrypted-data-from-tech-companies/2017/10/10/f33a91fc-adf7-11e7-9e58-e6288544af98_story.html [https://perma.cc/53WD-ZM2D]. In Florida, Polk County Sheriff Grady Judd threatened to arrest Apple CEO Tim Cook if his agency was unable to execute a warrant for encrypted data. Seung Lee, *Apple's CEO Hears It from a Florida Sheriff*, NEWSWEEK (Mar. 12, 2016), https://www.newsweek.com/apple-ceo-hears-it-florida-sheriff-436306 [https://perma.cc/5G9E-QCHC].

52. Cook has defended data encryption as the only way to protect privacy and reaffirmed the right to keep data encrypted. *Apple CEO Tim Cook Talks Importance of Encryption,* MSNBC (Apr. 6, 2018), https://www.msnbc.com/msnbc/watch/apple-ceo-tim-cook-talks-importance-of-encryption-1204842563515 [https://perma.cc/36A3-4UAF]. Tech giants Alphabet, Amazon, Apple, and Facebook have been urging Australian lawmakers to reconsider a law requiring tech companies to assist in decrypting data. *Apple and Facebook Among Tech Firms Lobbying Against Australia's Encrypted Data Law*, CNBC (Oct. 3, 2018), https://www.cnbc.com/2018/10/03/tech-giants-allied-against-proposed-australia-law-seeking-encrypted-data.html [https://perma.cc/4KTA-QX6S].

53. LAVABIT, https://lavabit.com/ [https://perma.cc/34W8-VB8H] (last visited Oct. 12, 2019).

54. Carpenter v. United States, 138 S. Ct. 2206, 2217–22 (2018); United States v. Jones, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring); United States v. Maynard, 615 F.3d 544, 558–59 (2010).

55. *Carpenter*, 128 S. Ct. at 2217; Riley v. California, 573 U.S. 373, 386 (2014).

56. *Carpente*r, 128 S. Ct. at 2222–23; *Riley*, 573 U.S. at 401.

Debates about privacy and technology tend toward grand abstractions. This article takes a different tack by focusing on the three most salient sources of legal limits on the ability of law enforcement and other government agents to access and gather information: the Fourth Amendment, the Fifth Amendment prohibition on compelled witnessing, and evidentiary privileges. It concludes that, although present doctrine probably does not support a general right to go dark, that may well change as technologies continue to play more central roles in our lives and government agencies continue to deploy and use technologies capable of facilitating programs of broad and pervasive surveillance.

II. A FOURTH AMENDMENT RIGHT TO GO DARK (?)

The Fourth Amendment guarantees that

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[57]

The threshold question in any Fourth Amendment case is whether government conduct constitutes a "search."[58] If government conduct is a "search," then it falls within the regulatory purview of the Fourth Amendment. If not, then government agents may act at their discretion, free from Fourth Amendment restraints.[59] One might assume that determining whether government action constitutes a "search" is a fairly straight-forward task. We all know what it is to "search." Any "seeking," "looking into," or "looking through," in order "to find or discover something" would qualify.[60] I search for my keys before leaving the house; I search for a friend in a crowded restaurant; and I search for information on the internet about a political candidate. Not complicated. But, in its vast, and perhaps well-intentioned, wisdom, the Supreme Court has made the task rather more complicated.

It all started with *Olmstead v. United States*, decided in 1928.[61] There, prohibition agents suspected that Roy Olmstead—of all things a former lieutenant in the Seattle police force—was engaged in a conspiracy to import and distribute illegal liquor in violation of the Volstead Act.[62] In an effort to look for information and to seek evidence of Olmstead's illegal activities, federal agents installed a wiretapping device on telephone

57. U.S. CONST. amend. IV.

58. *Carpenter*, 138 S. Ct. at 2211; DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE 251 (2017).

59. *Jones*, 565 U.S. at 421–22 (Alito, J., concurring); GRAY, *supra* note 58, at 253; David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 67 (2013).

60. GRAY, *supra* note 58, at 158–60.

61. 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

62. *Id.* at 455–56.

lines leading into his home.[63] The agents found what they sought.[64] By listening to Olmstead's conversations, the agents were able to document his participation in the conspiracy and discover when and where his shipments of liquor from Canada would arrive.[65]

By any common definition, we might describe these activities as a "search." By less common definition, the Court did not. Over a spirited dissent written by Justice Louis Brandeis, Chief Justice William Howard Taft held for the Court that wiretapping Olmstead's phone line was not a search for purposes of the Fourth Amendment because it entailed "the use of the sense of hearing and that only."[66] Moreover, "[t]here was no entry of the houses o[r] offices of the defendants."[67] Absent some looking or touching coupled with a physical intrusion of a person, house, paper, or effect, there was no search.[68] Absent a search, the Fourth Amendment imposed no restraints on the officers' use of wiretaps to look for information and certainly did not require approval by a detached and neutral magistrate in the form of a warrant supported by probable cause.[69]

After *Olmstead*, law enforcement officers were left to their own discretion as to whether, when, and why they would use wiretapping and other surveillance and eavesdropping technologies. At least with respect to the Fourth Amendment, they were free to listen in on anyone, anytime, for good reasons, for bad reasons, or for no reasons at all, so long as they did not physically intrude into a constitutionally protected area.[70]

By the middle of the twentieth century, the Court had come to regret granting that broad license. Relatively rare in 1928, telephones had become ubiquitous by 1967.[71] So too had law enforcement agencies, which grew dramatically in size, number, and scale during and after Prohibi-

63. *Id.* at 456–57.

64. *Id.* at 457.

65. *Id.*

66. *Id.* at 464. The Chief Justice offered no particular justification for isolating our aural senses in this way. Presumably, he would have felt differently about officers touching Olmstead or his property, looking through his papers, smelling the contents of his barrels, or tasting his liquor (at least three times, just to make sure!). One is left to wonder how he would describe a police officer's looking for or trying to find evidence by *asking* informants and *listening* to their answers. Or consider a normal exchange in many houses: "Honey, I'm searching for my keys. Have you seen them?" It seems perfectly normal to include that asking as part of the search, but it is ineffective, to say the least, without also listening to the answer.

67. *Id.*

68. *Id.* at 466.

69. *Id.* at 464.

70. *See generally* Berger v. New York, 388 U.S. 41 (1967) (Fourth Amendment regulates installation of eavesdropping devices in a private office); Silverman v. United States, 365 U.S. 505 (1961) (Fourth Amendment regulates use of a listening device pushed through a party wall until it physically touched a heating duct in the target's building); Irvine v. California, 347 U.S. 128 (1954) (trespassory entry into a home to install a listening device violates the Fourth Amendment); Goldman v. United States, 316 U.S. 129 (1942) (use of "detectaphone" to listen through a party wall is not subject to Fourth Amendment regulation).

71. Alexander Scolnik, Note, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORD. L. REV. 349, 363 (2009).

tion.[72] By the late 1950's, law enforcement agencies had also become much more aggressive, not only in investigating and prosecuting crime, but in domestic surveillance and intelligence-gathering as well.[73] Predictably, political activists and dissidents were among their favorite targets.[74] Perhaps the most notorious of these efforts was the Federal Bureau of Investigation's Counter Intelligence Program,[75] which infamously targeted political activists such as Fred Hampton and Martin Luther King Jr.[76] But many state and municipal police forces also had officers and units dedicated to monitoring and, in some cases, infiltrating political groups.[77]

Amidst all of this, wiretapping and other forms of electronic surveillance had become common tools in domestic spying programs, at least in part because of the license granted by *Olmstead*.[78] As a result, every American faced the very real prospect that they might be subject to government surveillance for insufficient reasons, for bad reasons, or for no reasons at all.[79] Concerned with the general threat to the right of the

72. GRAY, *supra* note 58, at 191–95.

73. S. REP. NO. 94-755, bk. III at 3 (1976).

74. *Id.* at 4–5.

75. This counterintelligence program was designed to disrupt groups and neutralize individuals deemed to be threats to domestic security. *Id.* at 3.

76. *Id.* at 7 (explaining surveillance of Martin Luther King Jr.).

77. The New York City Police Department's Bureau of Special Services was a secretive division of some fifty detectives who routinely surveilled and kept dossiers on individuals based on their race and political affiliations. Emanuel Perlmutter, *Police Intelligence Unit Watches Racial Activity*, N.Y. TIMES, July 27, 1964, at 19. A successful class action suit was brought against the Bureau of Special Services and the New York City Police Department alleging that the surveillance conducted by the bureau violated constitutional protections. *See generally* Handschu v. Special Servs. Div., 605 F. Supp. 1384 (D. Mass. 1985).

78. *See, e.g.*, Katz v. United States, 389 U.S. 347, 353 (1967).

79. The "Church Committee," so named after Senator Frank Church, would later describe the nature of this surveillance threat in vivid terms:

> Too many people have been spied upon by too many Government agencies and to[o] much information has [been] collected. The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power. The Government, operating primarily through secret informants, but also using other intrusive techniques such as wiretaps, microphone "bugs," surreptitious mail opening, and break-ins, has swept in vast amounts of information about the personal lives, views, and associations of American citizens. Investigations of groups deemed potentially dangerous—and even of groups suspected of associating with potentially dangerous organizations—have continued for decades, despite the fact that those groups did not engage in unlawful activity. Groups and individuals have been harassed and disrupted because of their political views and their lifestyles. Investigations have been based upon vague standards whose breadth made excessive collection inevitable. Unsavory and vicious tactics have been employed—including anonymous attempts to break up marriages, disrupt meetings, ostracize persons from their professions, and provoke target groups into rivalries that might result in deaths. Intelligence agencies have served the political and personal objectives of presidents and other high officials. While the agencies often committed excesses in response to pressure from high officials in the Executive branch and Congress, they also occasionally initiated improper activities and then concealed them from officials whom they had a duty to inform. Governmental officials—including

people to be secure against unreasonable searches posed by emerging eavesdropping and surveillance technologies, the Court elected to reshape its Fourth Amendment jurisprudence. That project took shape in *Katz v. United States*, decided in 1967.[80]

Charles Katz was prominent in bookmaking circles as, among other things, a college basketball handicapper.[81] He conducted much of his interstate bookmaking business using one or another of three public telephone booths located near his apartment on Sunset Boulevard in Los Angeles, California.[82] The FBI got wind of his activities and hit upon an ingenious plan to look for and try to find evidence against Katz. First, the agents arranged with the telephone company to disable one of the phones.[83] Then, the agents installed an "electronic ear" listening device between the remaining two phone booths, which would allow them to eavesdrop on Katz's conversations no matter which he chose to use.[84] Their ploy was successful. The agents found what they were looking for: evidence documenting Katz's participation in illegal sports betting.[85]

The agents in *Katz* had clearly done their homework on the Fourth Amendment. Toeing the lines drawn in *Olmstead*, they were only using their senses of hearing; the target for their eavesdropping was a public telephone booth, which is not a person, house, paper, or effect; and the listening device was installed outside the booths, so there was no physical intrusion. Add the fact that they had permission from the owner of the booth—the telephone company—to install the device, and it is easy to understand their confidence in the constitutionality of this investigative tactic. Therefore, it must have been shocking when the Court held that they had violated the Fourth Amendment by failing to secure a warrant based on probable cause before installing and using this technology to eavesdrop on Katz's conversations.[86]

Writing for the Court in *Katz*, Justice Potter Stewart redrew the Fourth Amendment landscape. Noting long-simmering doubts about the merits of *Olmstead* in the Court's jurisprudence,[87] Justice Stewart marked a clean break holding that "the Fourth Amendment protects people, not places."[88] Although he eschewed the idea that the Fourth Amendment established "a general constitutional 'right to privacy'" in the sense of a "right to be let alone by other people," he nevertheless concluded that

---

> those whose principal duty is to enforce the law—have violated or ignored the law over long periods of time and have advocated and defended their right to break the law.

GRAY, *supra* note 58, at 2–3 (quoting S. REP. NO. 94-755, bk. III at 5 (1976)).

80. *Katz*, 389 U.S. at 353–54.

81. Harvey Schneider, *Katz v. United States: The Untold Story*, 40 MCGEORGE L. REV. 13, 13 (2009).

82. *Id.*

83. *Id.*

84. *Id.* at 13–14.

85. *Katz*, 389 U.S. at 348–49.

86. *Id.* at 354–56.

87. *Id.* at 353–54.

88. *Id.* at 351.

the Fourth Amendment provides constitutional protections for what a person reasonably "seeks to preserve as private, even in an area accessible to the public."[89]

In an influential concurring opinion, Justice John Marshall Harlan II pointed out that the Court's holding offered a new definition of "search."[90] On this definition, government conduct is a search for purposes of the Fourth Amendment, if it violates "an actual (subjective) expectation of privacy" where that expectation is "one that society is prepared to recognize as 'reasonable.'"[91] Applying this definition to the facts in *Katz*, Justice Harlan had no reservations in supporting the majority's holding because the government's "electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth."[92] It was therefore conduct regulated by the Fourth Amendment. As to the form of that regulation, the Court held that agents needed to either secure a warrant from a detached and neutral magistrate based on probable cause before eavesdropping on Katz's conversations or cite constitutionally salient reasons sufficient to justify their failure to secure a warrant.[93]

Although *Katz* seemed progressive at the time, its novel definition of search has evolved so as to exclude from Fourth Amendment regulation a whole range of government activities that most English speakers would readily identify as "searches."[94] For example, the Court has held that we have no reasonable expectation of privacy in information voluntarily shared with third parties, at least where government agents access that information through those third parties.[95] In elaborating this "third-party doctrine," the Court has held that there is no search for purposes of the Fourth Amendment when government agents look through telephone calling records,[96] look through banking records,[97] or try to find information by recruiting a confidential informant or undercover officer to infiltrate a group and surreptitiously record conversations by wearing a wire.[98]

The Court has also held that we have no reasonable expectation of privacy in any information we expose to public view.[99] Applying this

89. *Id.* at 350–51.
90. *Id.* at 361 (Harlan, J., concurring).
91. *Id.*
92. *Id.* at 353 (majority opinion).
93. *Id.* at 358–59.
94. GRAY, *supra* note 58, at 68–69.
95. Smith v. Maryland, 442 U.S. 735, 744–46 (1979); GRAY, *supra* note 58, at 84–89.
96. *Smith*, 442 U.S. at 745–46.
97. Cal. Bankers Ass'n v. Schultz, 416 U.S. 21, 52 (1974).
98. Lopez v. United States, 373 U.S. 427, 440 (1963).
99. Florida v. Riley, 488 U.S. 445, 451 (1989); GRAY, *supra* note 58, at 78–84. One might wonder how this rule squares with the facts in *Katz*. As the Court made clear in that case, Katz did not have a reasonable expectation of privacy as against visual surveillance in a glass-walled public phone booth but did have an expectation of privacy as against aural surveillance by virtue of his entering the booth and closing the door. Katz v. United States, 389 U.S. 347, 353 (1967).

"public observation doctrine," the Court has held that looking into homes from public thoroughfares and accessible airspace is not a search.[100] Neither is looking for someone on public streets or using radio-beeper tracking devices to follow someone's public movements.[101] Interestingly, trespassing upon private land is also not a search, so long as agents do not enter upon the curtilage immediately surrounding a home.[102]

The third-party doctrine and the public observation doctrine have come under considerable scrutiny in recent years.[103] So too have tangential rules governing Fourth Amendment standing.[104] This is due in part to the broad licenses these doctrines grant for government agents to deploy and use a wide range of contemporary surveillance technologies, including closed-circuit television camera networks, license plate readers, drones, RFID tracking, cellular phone tracking, biometrics, and Big Data (which allows for the aggregation and analysis of high volumes of varied information from many vectors moving at high velocity). The emergence and rapid expansion of these technologies mark ours as an age of surveillance and pose the threat, if not the promise, of a surveillance state.[105]

Attentive to the consequences of broad and invasive government surveillance, scholars, critics, and activists have been pushing the courts to act. Some argue for revising the application of the Court's reasonable expectations of privacy standard, perhaps to include surveillance that is long-term, data-intensive, or particularly revealing.[106] Others advocate a new definition of "search" that would encompass a wider range of government conduct.[107] In a series of recent cases, a majority of the Justices on the Supreme Court seem to be sympathetic to these concerns, resulting in new constitutional rules governing the installation of GPS tracking devices[108] and law enforcement access to the cell site location data gathered and stored by cellular service providers.[109] Regardless of where these new lines of doctrine go, however, they are unlikely to provide grounds for a Fourth Amendment right to go dark. The reason why is

100. *Riley*, 488 U.S. at 449–50; California v. Ciraolo, 476 U.S. 207, 215 (1986).

101. United States v. Knotts, 460 U.S. 276, 285 (1983).

102. United States v. Dunn, 480 U.S. 294, 304–05 (1987); Oliver v. United States, 466 U.S. 170, 183 (1984); Hester v. United States, 265 U.S. 57, 58–59 (1924).

103. *See*, *e.g.*, United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

104. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 423 (2013) (Breyer, J., dissenting); GRAY, *supra* note 58, at 89–92; David Gray, *Collective Standing Under the Fourth Amendment*, 55 AM. CRIM. L. REV. 77, 86–97 (2018); Christopher Slobogin, *Standing and Covert Surveillance*, 42 PEPP. L. REV. 517, 520–29 (2015); Arnold Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1269–72 (1983).

105. GRAY, *supra* note 58, at 23–55; Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721, 1723–25 (2014); Margaret Hu, *Orwell's 1984 and a Fourth Amendment Cybersurveillance Nonintrusion Test*, 92 WASH. L. REV. 1819, 1829 (2017).

106. GRAY, *supra* note 58, at 104–29.

107. *See*, *e.g.*, Gray & Citron, *supra* note 59, 62.

108. *Jones*, 565 U.S. at 412–13.

109. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

evident if we return to the technology at issue in the San Bernardino case: a cellular phone.

In 2014, the Court decided *Riley v. California*.[110] Riley had been arrested on weapons charges. During a search incident to arrest of his person, officers found his cellular phone, which they accessed without a warrant or claim of emergency.[111] By examining messages, call logs, and pictures on the phone, the officers established Riley's ties to a gang and a shooting incident.[112] At trial, Riley unsuccessfully challenged the admissibility of evidence derived from his phone.[113] He was convicted and eventually appealed to the Supreme Court.[114] In a decision remarkable for its potentially far-reaching reasoning, the Court held that cellphone users have a heightened expectation of privacy in the contents of their phones.[115]

Cellphones, the *Riley* Court pointed out, have become a ubiquitous feature of modern life, to the point where they are, in essence, an extension of our bodies.[116] Almost everyone has one. They go with us everywhere and have come to serve as repositories for a wide variety of content and data.[117] Phones are also conduits to data stored on third-party servers.[118] These features, in the Court's view, put cellular phones on par with homes, offices, and file cabinets, all of which are afforded the highest levels of protection under the Fourth Amendment.[119] Based on this analysis, the Court held that accessing the contents of a cellular phone is a search.[120] Then it went further, holding that law enforcement officers cannot rely on the search incident to arrest doctrine when searching a cellular phone but, instead, must secure a warrant or cite facts sufficient to justify an exception to the warrant requirement, such as an emergency.[121] The Court also suggested that accessing data stored in "the cloud" would also be a search for purposes of the Fourth Amendment.[122]

In light of the Court's holding in *Riley*, it is tempting to think that the Fourth Amendment would provide grounds for a Fourth Amendment right to go dark. What better way, after all, to ensure against unauthorized government snooping of our phones and data repositories linked to our phones than to encrypt our devices and data stored in third-party

110. 573 U.S. 373 (2014).
111. *Id.* at 378–79.
112. *Id.* at 379.
113. *Id.* at 373.
114. *Id.*
115. *Id.* at 401.
116. *Id.* at 385 ("[M]odern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.").
117. *Id.*
118. *Id.* at 397.
119. *Id.* at 396–97.
120. *Id.* at 401.
121. *Id.* at 401–02.
122. *Id.* at 397.

servers? Although tempting, this conclusion does not immediately follow from the holding in *Riley*.

Affording Fourth Amendment protections, whether to a home or phone, is not the same as affording a right to go dark. Consider the text. By its language, the Fourth Amendment guards only against threats of *unreasonable* searches and seizures. *Eo ipso*, it does not grant any rights of security against *reasonable* searches and seizures. In fact, some scholars contend that the warrant clause, which describes a procedure for establishing the reasonableness of a search, implies that government agents have a right to engage in reasonable searches and seizures.[123] That is probably a step too far. The fundamental role of the Fourth Amendment is to limit government power, not the powers of the people or the conduct of persons.[124] But the fact that the text includes the warrant clause certainly cuts against any inference that the Fourth Amendment provides the people or persons with a right to prevent reasonable searches. And, that, of course, is precisely what a right to go dark would mean.

Consistent with this reading of the text, the Supreme Court's Fourth Amendment jurisprudence does not provide ready grounds for a Fourth Amendment right to go dark. The vast majority of the Court's Fourth Amendment doctrine governs nonconsensual searches, drawing lines between those that are and are not "reasonable." Why bother if those subject to nonconsensual searches maintain final authority to prevent or refuse a government search? Take, for example, the knock and announce rule.[125]

The knock and announce rule allows officers serving a lawful warrant to effectuate a forcible entry into a home so long as they knock, announce themselves, and provide those on the premises a reasonable opportunity to comply.[126] The whole enterprise would be rendered nonsensical if citizens had a right under the Fourth Amendment to deploy walls, doors, and locks invulnerable to lawful entry. So, too, the Court's doctrine governing warranted searches, emergency searches, and special needs searches. Why spill all this ink if the targets of searches ultimately have final veto power over the authority of law enforcement, courts, and administrative agencies to approve a lawful search? And then there is the rather long line of cases dealing with consent searches.[127] Read uncriti-

123. Corn & Brenner-Beck, *supra* note 23, at 338–48; Loewy, *supra* note 104, at 1231–44.

124. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) ("[A] central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'" (quoting United States v. Di Re, 332 U.S. 581, 595 (1948))); GRAY, *supra* note 58, at 249–51; Renee McDonald Hutchins, *Tied up in Knotts? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 444 (2007).

125. Wilson v. Arkansas, 514 U.S. 927, 929 (1995).

126. *Id.* at 931–32.

127. United States v. Drayton, 536 U.S. 194, 206–07 (2002) (holding that law enforcement asking questions of passengers on a bus did not constitute an illegal seizure and that consent given to search passenger and bags was valid); Ohio v. Robinette, 519 U.S. 33, 35 (1996) (upholding consent to search a vehicle that was given after law enforcement completed valid traffic stop); Schneckloth v. Bustamonte, 412 U.S. 218, 248–49 (1973) (holding

cally, these cases might suggest that citizens can prevent searches and seizures by simply refusing to give consent. But, of course, refusing to give consent to search just pushes an encounter down another road, requiring that officers secure a warrant or otherwise establish that they acted reasonably. Refusal to give consent is far from being the last word.

Recognizing a right to go dark under the Fourth Amendment would also seem to run contrary to the balancing of interests implied in the Amendment's focus on reasonableness.[128] The Court has long held that determining what is "reasonable" for purposes of the Fourth Amendment requires striking a balance among the competing interests at stake.[129] On the one hand, searches compromise a target's privacy interests, property interests, and personal security interests.[130] On the other hand, searches advance governmental interests in public security, usually by facilitating the detection, investigation, and prosecution of crime.[131] The Justices generally regard a search or a class of searches as reasonable for purposes of the Fourth Amendment if they strike an appropriate balance among these competing interests.[132] Recognizing a right to go dark under the Fourth Amendment would effectively render this balancing of interests approach irrelevant. In fact, recognizing a right to go dark would virtually extinguish the ability of government agents to use many investigative techniques that play an important role in vindicating public interests, providing for public security, prosecuting crime, and protecting the public, including its most vulnerable members.[133]

None of this means that the Fourth Amendment by itself would bar the deployment and use of encryption or other efforts to go dark. The humbler claim is simply that there is no right under the Fourth Amendment to thwart lawful searches by physical or technological means. It follows that, should Congress pass a law limiting the deployment and use of encryption

---

that a suspect need not know that he has the right to decline a search in order for the search to be based on valid consent).

128. *See*, *e.g.*, *Wilson*, 514 U.S. at 935–36 (discussing the balancing of property and law enforcement interests underlying the knock and announce rule). *See generally* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011) (describing the Court's ongoing effort to strike a reasonable balance between privacy interests and law enforcement interests).

129. *Wilson*, 514 U.S. at 934; Zurcher v. Stanford Daily, 436 U.S. 547, 560–63 (1978) (balancing interests between law enforcement and third-parties); Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 306–07 (1967) (balancing interests between law enforcement and citizens in the seizure of "mere evidence").

130. *Wilson*, 514 U.S. at 932; *Zurcher*, 436 U.S. at 560–61; *Hayden*, 387 U.S. at 310–11.

131. *Wilson*, 514 U.S. at 936; *Zurcher*, 436 U.S. at 554–55; *Hayden*, 387 U.S. at 301.

132. *Wilson*, 514 U.S. at 936; *Zurcher*, 436 U.S. at 559; *Hayden*, 387 U.S. at 298–99.

133. *See Child Pornography*, U.S. DEPT. JUSTICE, https://www.justice.gov/criminal-ceos/child-pornography [https://perma.cc/6PQV-3ERA] ("The methods many offenders use to evade law enforcement detection have also become increasingly sophisticated. Purveyors of child pornography continue to use various encryption techniques and anonymous networks on 'The Dark Internet', attempting to hide their amassed collections of illicit child abuse images. Several sophisticated online criminal organizations have even written security manuals to ensure that their members follow preferred security protocols and encryption techniques in an attempt to evade law enforcement and facilitate the sexual abuse of children.").

technologies capable of thwarting warranted searches, that law would not be vulnerable to Fourth Amendment challenges.[134] Thus, when it comes to the Fourth Amendment itself, it seems that all we can say is, "If you got a warrant, I guess you're gonna come in."[135]

The San Bernardino case provides a useful concrete example for elaborating these points. The paradigm case of a reasonable search for purposes of the Fourth Amendment is one licensed by a warrant that is based upon probable cause, supported by oath or affirmation, issued by a detached and neutral magistrate, and that describes with particularity both the place to be searched and the evidence sought.[136] The agents in San Bernardino had a probable cause warrant to search Farook's phone. That seems to be all the Fourth Amendment requires in order for their proposed search to be reasonable.[137] If we read the Fourth Amendment as also guaranteeing a right to go dark, then, despite the officers' compliance with the demands of the warrant clause, Farook would still maintain a superior right to prevent those officers from serving their warrant. This would imply his further right to privilege his privacy interests above public interests in identifying terrorist plots and preventing terrorist attacks, not to mention our collective interests in prosecuting and punishing terrorists. It is hard to see any evidence in the text of the Fourth Amendment or the Court's Fourth Amendment jurisprudence for recognizing such a right.

The Fourth Amendment guards against unreasonable searches and seizures. It does not guarantee an additional right to secure oneself against reasonable searches. Returning to our discussion of *Riley*, this means that information and data can be deemed private under the Fourth Amendment but nevertheless remain accessible to government agents through lawful means. We can have a reasonable expectation of privacy in the contents of our cellular phones but still not have a right to prevent law enforcement from gaining access to our phones and data stored on our phones if they have a warrant. That, it seems, is where the Fourth Amendment rests on the right to go dark question. But might this conclusion be too hasty? Might it miss the place of the Fourth Amendment in our constitutional structure and the role it plays in addressing new threats posed by modern surveillance capacities and practices?

Although the *Katz* Court framed the Fourth Amendment in terms of privacy, the word "privacy" appears nowhere in the text. Neither do concerns with protecting privacy appear in the drafting history of the Fourth

134. There might well be grounds to object on First Amendment grounds. *See*, *e.g.*, Apple Inc's Motion to Vacate Order, *supra* note 46, at 32–34.

135. GRATEFUL DEAD, *Truckin'*, *on* AMERICAN BEAUTY (Warner Bros. 1970).

136. GRAY, *supra* note 58, at 169–72.

137. This assumes, of course, that probable cause existed, that the officers abided the terms of the warrant when conducting the search, and that the means and methods used when conducting the search were not unreasonable in terms of the force used.

Amendment.[138] True, Fourth Amendment protections for houses sound in common law treatments of homes as sovereign fiefdoms providing spaces to which persons can withdraw from society, seeking succor from the travails and vicissitudes of the world.[139] But, tellingly, the Fourth Amendment does not protect the privacy of persons in their homes. It instead protects the right of "the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[140] That wording is not a matter of capricious happenstance. It reflects a drafting history and historical context in which the Fourth Amendment was understood as guaranteeing a collective right against the unconstrained use of government powers to search and seize.[141] Moreover, the Fourth Amendment was adopted against the backdrop of eighteenth century efforts to use search and seizure powers to suppress political and religious freedom.[142] In this regard, the Fourth Amendment can and must be read as a precondition to functioning democracy that is of a piece with rights guaranteed in Article I, the First Amendment, the Second Amendment, the Ninth Amendment, and the Tenth Amendment.[143]

The democratic order imagined by the Constitution and Bill of Rights is now in peril.[144] There can be little doubt that we live in an age of surveillance.[145] The dystopian visions familiar from the works of George Orwell, Aldous Huxley, and even J.R.R. Tolkien are upon us.[146] Daily, we are subjected to the threat or reality of visual surveillance from closed-circuit television cameras.[147] We are tracked through our cellular phones and GPS-enabled devices.[148] Our activities on- and off-line are monitored through financial records and the volumes of "digital exhaust" we generate every moment of our lives. The Snowden revelations and

138. Minnesota v. Carter, 525 U.S. 83, 93, 97 (Scalia, J., concurring); David Gray, *Fourth Amendment Categorical Imperative*, 116 MICH. L. REV. ONLINE 14, 15 (2017).

139. *See*, *e.g.*, Weeks v. United States, 232 U.S. 383, 390 (1914) ("The maxim that 'every man's house is his castle' is made a part of our constitutional law in the clauses prohibiting unreasonable searches and seizures, and has always been looked upon as of high value to the citizen.").

140. U.S. CONST. amend. IV.

141. GRAY, *supra* note 58, at 146–56; David Gray, *Fourth Amendment Remedies as Rights: The Warrant Requirement*, 96 B.U. L. REV. 425, 443–57 (2016) [hereinafter Gray, *The Warrant Requirement*].

142. Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018); Riley v. California, 573 U.S. 373, 382 (2014); Wilkes v. Wood (1763) 98 Eng. Rep. 489 (K.B.); Entick v. Carrington (1765) 95 Eng. Rep. 807 (K.B.); GRAY, *supra* note 58, at 141–44, 160–65; Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1195 (2016).

143. Gray, *The Warrant Requirement*, *supra* note 141, at 446–47; Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 432–33 (1974) ("[T]he phraseology of the amendment, akin to that of the first and second amendments and the ninth, [was not] accidental.").

144. GRAY, *supra* note 58, at 23–55.

145. *Id.*

146. *Id.* at 1–6; Hu, *supra* note 105, at 1824–25 (discussing the role of literary dystopias in contemporary Fourth Amendment discourse).

147. Slobogin, *supra* note 105, at 1752–54.

148. Carpenter v. United States, 138 S. Ct. 2206, 2216–17 (2018).

subsequent reporting have disclosed to the public both the extent of existing governmental surveillance and a clear ambition on the part of the Executive Branch to achieve omniscience.[149]

As Justice Sonia Sotomayor has pointed out, the threat and reality of broad and indiscriminate surveillance is "inimical to democratic society."[150] As a government of the people, democratic societies are designed for the people to watch the government, holding those in power to the people's standards through their critical gaze.[151] In a surveillance society, the vector of power runs in the other direction.[152] In a surveillance state, it is the people who are constantly judged and disciplined by government's gaze.[153] We need not rely on fiction to see the dangers. The twentieth century provides us with ample examples of oppressive regimes where surveillance was deployed and used as a tool of social control.[154] What the Snowden documents reveal is that we are standing at the precipice of a constitutional crisis driven by ongoing government efforts to conduct the kinds of broad and indiscriminate surveillance programs characteristic of a surveillance state.

In the face of these challenges, the political branches have proven unwilling or unable to constrain the rapid expansion of government surveillance programs.[155] Demonstrably buoyed by various interminable wars (on terrorism, on drugs, on poverty, etc.), executive agencies have pur-

149. GRAY, *supra* note 58, at 43.

150. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring). The Court appears to have embraced Justice Sotomayor's views on the threats of broad and indiscriminate surveillance. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2217; Riley v. California, 573 U.S. 373, 395–96 (2014).

151. ORWELL ROLLS IN HIS GRAVE, at 13:25–14:00 (Sag Harbor-Basement Pictures 2003) (Professor Robert McChesney explains that "a self-governing society, a democratic society" requires a media that "keeps track of people in power and people who want to be in power"). *See generally* ROBERT W. MCCHESNEY, RICH MEDIA, POOR DEMOCRACY: COMMUNICATION POLITICS IN DUBIOUS TIMES (1999).

152. David A. Anderson, *Freedom of the Press in Wartime*, 77 U. COLO. L. REV. 49, 51 (2006) (arguing that "control of press access to information" allows the government to manipulate public opinion).

153. Deven R. Desai, *Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hording*, 90 NOTRE DAME L. REV. 579, 598–99 (2014) (discussing how advanced surveillance technologies enable the government to infringe on the right of association).

154. The Ministry for State Security (Stasi) of the former German Democratic Republic employed an extensive network of informants and spies in order to quash dissent and maintain control over the public. Virtually everyone in the German Democratic Republic was either an employee/informant of the Stasi or a target of its oversight. *See* Paul M. Schwartz, *Constitutional Change and Constitutional Legitimation: The Example of German Unification*, 31 HOUS. L. REV. 1027, 1052–53 (1994).

155. In 2018, the House of Representatives voted to renew the NSA's warrantless surveillance program for another six years and rejected a bipartisan push to establish privacy limits. Charlie Savage, Eileen Sullivan & Nicholas Fandos, *House Extends Surveillance Law, Rejecting New Privacy Safeguards*, N.Y. TIMES (Jan. 11, 2018) https://www.nytimes.com/2018/01/11/us/politics/fisa-surveillance-congress-trump.html [https://perma.cc/D4YE-AJRA]; *see also* United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring) ("To date, however, Congress and most States have not enacted statutes regulating the use of GPS tracking technology for law enforcement purposes.").

sued more and greater surveillance powers.[156] Perhaps fearful of the political consequences, legislatures have so far not set any real constraints.[157] Until recently, courts have often been similarly ineffectual and, ironically, defer to the superior democratic legitimacy and policy expertise of the political branches.[158] As a result, the security of the people against unreasonable searches and seizures has been dramatically degraded. Added to that is the problem of cheating. As the Snowden documents reveal, executive agents appear perfectly willing to violate even the minimal constitutional and legal constraints under which they live, engaging in illegal activities or outsourcing surveillance work to foreign states and private contractors, who may not be subject to the same constitutional constraints.[159]

None of this is unexpected. In fact, it is the natural teleology of the executive state.[160] The exercise of police and security powers inevitably drives executive agents to pursue more and greater powers, including the ability to conduct broad and pervasive surveillance. What better way to fight crime and protect the public than to achieve omniscience? Of course, it was precisely this well-understood trajectory of executive power that inspired our founders to include structural constraints on the Executive in the body of the Constitution and to afford to persons and the peo-

156. *See* ELIZABETH HINTON, FROM THE WAR ON POVERTY TO THE WAR ON CRIME 61–62 (2016) (explaining the federal push to integrate policing into the social welfare state and how the war on crime and the war on poverty go hand-in-hand). *See generally* Gerald G. Ashdown, *The Blueing of America: The Bridge Between the War on Drugs and the War on Terrorism*, 67 U. PITT. L. REV. 753 (2006) (describing the parallels in development in the wars on drugs and terror through increased surveillance); Corey Rayburn Yung, *The Emerging Criminal War on Sex Offenders*, 45 Harv. C.R.-C.L. L. REV. 435 (2010) (exploring what defines a war on crime and the emergence of a war on sex offenders).

157. *See supra* note 155 and accompanying text.

158. Three of the most promising of these recent decisions are *Carpenter*, 138 S. Ct. 2206 (2018), regulating law enforcement access to cell site location date; *State v. Andrews*, 227 Md. App. 350 (2016), regulating the deployment and use of cell site simulators; and *Jones*, 565 U.S. 400, regulating the installation of GPS tracking devices during criminal investigations.

159. Kim Zetter, *NSA Is Intercepting Traffic from Yahoo, Google Data Centers*, WIRED (Oct. 30, 2013), https://www.wired.com/2013/10/nsa-hacked-yahoo-google-cables/ [https://perma.cc/6R54-LLGA].

160. 2 Francis Maseres, *The Canadian Freeholder: In Three Dialogues Between an Englishman and a Frenchman, Settled in Canada* 243–44 (London, B. White 1779) (commenting on *Wilkes v. Wood*, (1763) 98 Eng. Rep. 489 (K.B.), and noting that appointed members of the executive are "fond of the doctrines of reason of state, and state necessity, and the impossibility of providing for great emergencies and extraordinary cases, without a discretionary power in the Crown to proceed sometimes by uncommon methods not agreeable to the known forms of law."); *see also* Boyd v. United States, 116 U.S. 616, 635 (1886) ("Though the proceeding in question is divested of many of the aggravating incidents of actual search and seizure, yet, as before said, it contains their substance and essence, and effects their substantial purpose. It may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure.").

ple rights designed, in part, to guarantee security against overreaching executive power.[161]

From this perspective, we can see our current crisis as the result of a structural failure. The coordinate branches have simply failed to perform their roles. Given this state of affairs, might the Fourth Amendment imply a right to self-help? Might it entail a right of the people to secure for themselves their constitutional birthright when Congress and the courts fail to act?

Although there is no recognized right to go dark in the Supreme Court's Fourth Amendment jurisprudence, there is a substantial case to be made that the Fourth Amendment, as a guardian of democratic principles, contains a residual right to self-help. That right is prominent in the *Katz* definition of "search," which requires that a subject manifest an expectation of privacy.[162] Much discussion of the Court's Fourth Amendment jurisprudence since 1967 has focused on what expectations of privacy are "reasonable." But that is only half of the inquiry under *Katz*. Courts are also interested in whether a target has manifested an expectation of privacy.[163] Here, countermeasures and other forms of self-help play an important role in guaranteeing Fourth Amendment rights. Just as examples, the courts have encouraged citizens to erect fences around their yards,[164] close doors,[165] shutter windows,[166] deploy blinds,[167] and conduct their affairs behind opaque walls.[168] Encryption and other efforts

161. *See* Entick v. Carrington (1765) 95 Eng. Rep. 807, 817 (K.B.) ("[W]e can safely say there is no law in this country to justify the defendants [in executing a search unsupported by law or precedent]; if there was, it would destroy all the comforts of society."); *see also Jones*, 565 U.S. at 405 (stating that *Entick* "is a 'case we have described as a 'monument in English Freedom'" and is considered "'the true and ultimate expression of constitutional law' with regard to search and seizure" (quoting Brower v. County of Inyo, 489 U.S. 593, 596 (1989))); Johnson v. United States, 333 U.S. 10, 14 (1948) ("The right of officers to thrust themselves into a home is also a grave concern, not only to the individual but to a society which chooses to dwell in reasonable security and freedom from surveillance.").

162. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("[T]here is a twofold requirement, first that a person must have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

163. *But see generally* Orin S. Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113 (2015) (arguing that courts only look at reasonable expectation of privacy and never subjective manifestation).

164. Massachusetts v. Podgurski, 459 U.S. 1222, 1224 (1983) (Rehnquist, C.J., dissenting) (suggesting that an officer looking inside a van's open door does not constitute a search under the Fourth Amendment).

165. *See* Ker v. California, 374 U.S. 23, 36–37 (1963) (holding that marijuana observed through an open doorway was admissible under the plain view doctrine).

166. *See* Collins v. Virginia, 138 S. Ct. 1663, 1671–72 (2018) (suggesting in dicta that anything observed through an open window does not constitute a search); Florida v. Riley, 488 U.S. 445, 450–52 (1989) (holding that peering into openings in the roof of an enclosed greenhouse from public airspace is not a search).

167. Minnesota v. Carter, 525 U.S. 83, 85, 91 (1998) (holding that a warrant was supported by valid probable cause when officer observed respondents bagging cocaine through respondents' window).

168. *See supra* note 166; *cf.* Texas v. Brown, 460 U.S. 730, 742–43 (1983) (holding that law enforcement could seize heroin observed through the windows of a car during a routine driver's license checkpoint).

to go dark may be viewed as another in this long line of countermeasures, manifesting an expectation of privacy against data and electronic surveillance in the same way that traditional countermeasures manifest expectations of privacy against aural and visual surveillance. Nobody would contest the right of citizens to erect a fence or close a blind in order to protect against government snooping. Why should encryption be different?

The easy answer, of course, is that law enforcement officers can climb over a fence, open a door, or pull back a curtain. The problem with encryption is precisely that government agents acting lawfully cannot open an encrypted device or reveal encrypted data. Although there is certainly a right under the Fourth Amendment to manifest an expectation of privacy, it is quite a different proposition to claim that there is a right to prevent even lawful and reasonable searches and seizures. But that is a conclusion for reasonable times.

We live in a world where law enforcement has been granted an effective license to conduct a whole range of surveillance activities without real legal limits. New technologies have virtually removed any practical constraints on the exercise of that license. Intoxicated by the powers accompanying these expanded capacities, law enforcement and other government agencies have engaged in programs of broad and indiscriminate surveillance, threatening the core democratic values guarded by the Fourth Amendment. In our current environment, encryption and other technological means for going dark may provide the only realistic way for citizens to protect themselves against overreaching and oppressive government surveillance. If that is the only way for we, the people, to guarantee our collective right to be secure against unreasonable searches and seizures, then that existential reality might necessitate recognizing a complementary right to go dark.

Experiences with cellular phone technology during the 1990s provide a useful precedent. When first deployed, cellular phones were little more than handheld radios.[169] They used standard analog technology in common use on two-way radios.[170] The only real differences between these phones and two-way radios were that cellphones used a different frequency range and communicated through the intermediary of a cell network.[171] Cellular phone signals were fairly easy to intercept.[172] Just about anyone with a broad-band radio receiver could eavesdrop on conversations. Wireless home telephones operated on the same basic technology.[173] Conversations conducted using early cellphones and wireless

169. GRAY, *supra* note 58, at 32.

170. *Id.*

171. *Id.*; Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH. 1, 51–53 (2014).

172. GRAY, *supra* note 58, at 32.

173. *Id.* at 32–33.

home telephones were notoriously susceptible to interception.[174] In the wake of several high-profile incidents, the Federal Communication Commission introduced regulations that sought to protect the privacy of communications over wireless analog telephones.[175] Those regulations were notoriously hard to enforce, however. The interception technology was already out there, easy to make, and virtually impossible to detect.[176] The whole crisis came to an abrupt end when telephone manufacturers and cellular phone services converted to digital technologies that facilitated the widespread use of encryption.[177] There were hiccups, of course, such as when first generation A5/1 encryption was publicly broken in 1999, rendering transparent most communications on first generation cellular networks.[178] But cellular phone providers have regularly upgraded their networks, allowing for the introduction of A5/3 and A5/4 encryption, both of which remain immune from decryption by all but perhaps the most sophisticated national security agencies.[179]

Experiences with the interception of cellular phone signals and encryption as a self-help tool certainly seem to provide a useful precedent for a twenty-first century right to go dark. There is, of course, an important difference. No matter how robust the signals encryption deployed and used by cellular phone companies, service providers retain the ability to decrypt those signals. In fact, they are required to as a matter of statute under the Communications Assistance for Law Enforcement Act.[180] As a consequence, government agents armed with a lawful warrant issued under the Wiretap Act can gain access to the contents of encrypted cellular phone conversations.[181] Contemporary going dark technologies take matters one critical step further by rendering data and communications content opaque even to service providers. But, given the nature of contemporary threats, the ubiquity of electronic communications and data, and the key roles these technologies play in our lives, going dark may well be the only way to truly guarantee our security against threats of unreasonable search and seizure. If that is the case, then should we not have a right to do it?

III. A FIFTH AMENDMENT RIGHT TO GO DARK (?)

The Fifth Amendment guarantees that "[n]o person . . . shall be com-

174. *Id.*

175. Jerry Gray, *Florida Couple Are Charged In Taping of Gingrich Call*, N.Y. TIMES, Apr. 24, 1997, at A2; Travis LeBlanc & Lindsay DeFrancesco, *The Federal Commission as Privacy Regulator*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 727 (David Gray & Stephen E. Henderson eds., 2017).

176. LeBlanc & DeFrancesco, *supra* note 175, at 746–47.

177. GRAY, *supra* note 58, at 33; Pell & Soghoian, *supra* note 171, at 51–53.

178. GRAY, *supra* note 58, at 33; Pell & Soghoian, *supra* note 171, at 51–53.

179. GRAY, *supra* note 58, at 33; Pell & Soghoian, *supra* note 171, at 51–53.

180. Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. § 1002 (2012). For a concise discussion of CALEA, see LeBlanc & DeFrancesco, *supra* note 175, at 748–49.

181. 18 U.S.C. § 2511(2).

pelled in any criminal case to be a witness against himself . . . ."[182] Tracing its roots to seventeenth century common law and responses to the abuses of the Star Chamber,[183] the Fifth Amendment privilege against compelled witnessing is first and foremost a trial right.[184] It guarantees that no criminal defendant can be compelled by the state to take the witness stand and testify against herself in a formal magisterial proceeding on pain of contempt, fine, or adverse inference.[185] That made good sense in 1791, when investigative law enforcement agencies were virtually nonexistent.[186] But the Fifth Amendment's protections had been compromised considerably by the end of the nineteenth century when professionalized law enforcement agencies charged with detecting, investigating, and prosecuting crime became a more common fixture in American society.[187]

Professional law enforcement investigators were making frequent use of interrogations by the late nineteenth and early twentieth century.[188] Their goal was to secure confessions (sometimes by extreme means),[189] which could then be admitted into evidence at a later criminal trial.[190] These tactics created new challenges for the Fifth Amendment. If you can be compelled to make incriminatory statements or to provide evidence to investigators for later use at trial, then it is of little solace to know that you will be free to sit mute while being damned by your own words.[191] In response to these new challenges, the Court extended the Fifth Amendment right against compelled witnessing to other forums.[192] Among the most familiar instances of this expansion is *Miranda v. Arizona*, which provides a right against compelled self-incrimination during custodial interrogations.[193]

Although revolutionary when it was decided in 1966, *Miranda* has its roots in the 1886 case *Boyd v. United States*.[194] *Boyd* is particularly rele-

182. U.S. CONST. amend. V.

183. Joseph L. Rauh, Jr., *The Privilege Against Self-Incrimination from John Lilburne to Ollie North*, 5 CONST. COMM. 405, 405–06 (1988).

184. United States v. Patane, 542 U.S. 630, 641 (2004).

185. *Id.* at 637; Pennsylvania v. Muniz, 496 U.S. 582, 588–89 (1990).

186. *See* Miranda v. Arizona, 384 U.S. 436, 527 (1966); GRAY, *supra* note 58, at 197; Thomas Y. Davies, *Farther and Farther from the Original Fifth Amendment: The Recharacterization of the Right Against Self-incrimination as a "Trial Right" in Chavez v. Martinez*, 70 TENN. L. REV. 987, 1004 (2003); Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 620–21 (1999); Wesley MacNeil Oliver, *The Neglected History of Criminal Procedure, 1850–1940*, 62 RUTGERS L. REV. 447, 447–48 (2010); Carol S. Steiker, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820, 824 (1994); Silas J. Wasserstrom, *The Fourth Amendment's Two Clauses*, 26 AM. CRIM. L. REV. 1389, 1395 (1989).

187. GRAY, *supra* note 58, at 197–99.

188. *See Miranda*, 384 U.S. at 445–46 (discussing how emerging police forces adopted the use of incommunicado interrogations).

189. *See id.* at 446 (describing violent interrogation methods); Brown v. Mississippi, 297 U.S. 278, 281–83 (1936) (documenting a brutal interrogation that included partial lynching of a suspect).

190. *Miranda*, 384 U.S. at 446; GRAY, *supra* note 58, at 198–99.

191. GRAY, *supra* note 58, at 197–98.

192. *Miranda*, 384 U.S. at 467.

193. *Id.* at 463.

194. 116 U.S. 616 (1886).

vant to the question whether the Fifth Amendment might support a right to go dark. In that case, federal authorities suspected that Boyd was dodging import taxes owed on, among other goods, shipments of plate glass from England.[195] In an effort to gather evidence against him, prosecutors sought to review invoices associated with Boyd's import business.[196] They secured a court order under the authority of a federal statute forcing Boyd to produce those documents.[197] Boyd complied under protest, arguing that he was being compelled to provide the government with incriminating evidence in violation of the Fifth Amendment.[198] He was convicted and then appealed to the Supreme Court, which sided with Boyd.[199] In his opinion for the Court, Justice Joseph Bradley reported that "we have been unable to perceive that the seizure of a man's private books and papers to be used in evidence against him is substantially different from compelling him to be a witness against himself."[200] On that basis, the Court held that

> compelling the production of . . . private books and papers, to convict [a party] of crime, or to forfeit his property, is contrary to the principles of a free government. It is abhorrent to the instincts of an Englishman; it is abhorrent to the instincts of an American. It may suit the purposes of despotic power; but it cannot abide the pure atmosphere of political liberty and personal freedom.[201]

Heady stuff—and it is highly suggestive of a potential Fifth Amendment ground for a right to go dark.

There can be no doubt that the contents of our digital devices and electronic communications hold the potential for incrimination. Consider *Riley v. California*, the case in which the Supreme Court held that accessing the contents of a cellular phone is a search governed by the warrant requirement.[202] Photographs, contacts, and texts found on Riley's phone implicated him in gang activity and a shooting incident, providing prosecutors with key evidence critical to his conviction.[203] Might Riley, and therefore any of us, contend that being forced to disclose the contents of our devices or electronic communications is an act of compelled witnessing akin to Boyd's being compelled to produce documents?[204] The Court's reasoning in *Boyd* definitely suggests that we could. And, if this is right, then might we argue further that the only way to truly secure that right is through the deployment of robust encryption capable of guaran-

195. *Id.* at 618–19.
196. *Id.* at 619.
197. *Id.*
198. *Id.* at 618.
199. *Id.*
200. *Id.* at 633.
201. *Id.* at 631–32.
202. Riley v. California, 573 U.S. 373, 386 (2014).
203. *Id.* at 379–80.
204. For a brief but insightful discussion of these questions, see generally Bryan H. Choi, *The Privilege Against Cellphone Incrimination*, 97 TEX. L. REV. ONLINE 73 (2019).

teeing with absolute certainty the security of our digitized data?[205]

In 1886, it at least seems that there might well have been good grounds for a Fifth Amendment right to go dark. The problem is that, while the Court was expanding the procedural reach of the Fifth Amendment in *Miranda* and other cases, it was also busy limiting the scope of its application by adopting a narrow view of what conduct constitutes being a "witness" and what kind of witnessing is "compelled."

In an infamous opinion for the Court in *Pennsylvania v. Muniz*, Justice William Brennan carved *Boyd* back considerably by adopting a narrow definition of what it is to "be a witness."[206] Muniz had been arrested for driving under the influence of alcohol.[207] During the booking process, which was videotaped, he was asked a series of standard administrative questions, including his name, address, height, weight, eye color, date of birth, and current age.[208] He was also asked for the date of his sixth birthday.[209] At trial, the tape from his booking procedure was admitted to show that Muniz was unsteady, hesitant in answering questions, slurring his words, and unable to report accurately the date of his sixth birthday.[210] Relying on prior precedent, Justice Brennan reasoned that Muniz's physical comportment and the manner of his expression were not "testimonial" because that conduct did not disclose the results of a mental process.[211] Unlike factual assertions or disclosures of information, behavioral manifestations of drunkenness do not reveal the inner workings of the mind.[212] Although Muniz's answers to the booking questions did entail assertions of fact and disclosures of information and therefore were "testimonial," Justice Brennan pointed out that requests for this kind of biographical information were necessary to the routine administrative process of booking arrestees and therefore were exempt from Fifth Amendment protections.[213] The question relating to the date of Muniz's sixth birthday was different, however, in that it required expressing the results of a mental process but was not reasonably related to the booking process.[214] Evidence relating to that question and his response therefore fell within the compass of the Fifth Amendment's protections.[215]

The other line of twentieth century doctrine that has limited significantly the scope and reach of *Boyd* addresses when a testimonial expres-

205. *See id.* (arguing that some digital data should be subject to Fifth Amendment protections).
206. Pennsylvania v. Muniz, 496 U.S. 582, 596 (1990).
207. *Id.* at 585.
208. *Id.* at 585–86.
209. *Id.* at 586.
210. *Id.* at 587.
211. *Id.* at 604; Doe v. United States, 487 U.S. 201; Schmerber v. California, 384 U.S. 757, 761 (1966).
212. *Muniz*, 496 U.S. at 601.
213. *Id.*
214. *Id.* at 598–99, 601.
215. *Id.* at 599–600.

sion is "compelled."[216] In *Fisher v. United States*, the Court held that "the Fifth Amendment does not independently proscribe the compelled *production* of . . . incriminating evidence but applies only when the accused is compelled to make a *testimonial communication* that is incriminating."[217] In particular, the Court reasoned, compelling the production of documents that a suspect created previously by a voluntary act does not necessarily implicate the Fifth Amendment even if those voluntarily created documents contain self-incriminatory statements that might be regarded as testimonial under *Muniz*.[218] The Court allowed that the act of production might itself be testimonial but maintained that the Fifth Amendment provides no independent protection for the contents of documents voluntarily created such as diaries, journals, and business records.[219]

Together, *Muniz* and *Fisher* voided much of the pomp and promise of *Boyd*. They also seem to limit significantly the potential for a right to go dark grounded in the Fifth Amendment privilege against compelled witnessing. That is because much of the content law enforcement agencies might want to access on digital devices is not testimonial, not compelled, or is neither testimonial nor compelled. Consider again the facts in *Riley*. There, the investigating officers were interested in texts and pictures Riley had created of his own volition, free from state compulsion.[220] As a consequence, those documents were excluded from Fifth Amendment protections under *Fisher*. Officers were also interested in call records and contact lists stored on Riley's phone, none of which were results of Riley's mental processes.[221] In fact, at least with respect to call records, the information was not even created by Riley. Instead, that data was an artifact produced by his phone and installed apps, which created and reported those records independent of any conduct on his part. True enough, Riley initiated the underlying calls, but the data about those calls was not the result of any act of expression or mental process on his part.

By a similar analysis, the location data routinely gathered and stored by personal devices, and particularly cellular phones, probably would not qualify for Fifth Amendment protection under current doctrine. Consider, as an example, cell site location information (CSLI). Whenever they are turned on, our cellular phones are in regular contact with the network of cellular base stations maintained by our service providers.[222] Each one of these "pings" generates a fairly precise location data point.[223] These data points are gathered by service providers at regular intervals—usually every few seconds.[224] Most providers store that data

216. Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 820 (2005).
217. Fisher v. United States, 425 U.S. 391, 408 (1976).
218. *Id.* at 409–10.
219. *Id.* at 411.
220. Riley v. California, 573 U.S. 373, 379 (2014).
221. *Id.*
222. Carpenter v. United States, 138 S. Ct. 2206, 2211–12 (2018).
223. *See id.*
224. *See id.*

for several years, which means that they possess a virtual "time machine" capable of retracing our past movements and creating a detailed history of our lives.[225] That kind of information has extraordinary law enforcement potential. For example, in *Carpenter*, investigators reviewed several months of cell site location data to document Carpenter's proximity to a number of armed robberies.[226] That objective evidence was valuable in itself but also provided important corroboration of testimony offered by coconspirators.[227]

The *Carpenter* Court ultimately held that CSLI is protected by the Fourth Amendment.[228] But is it also subject to Fifth Amendment protection? Given the current state of the law, it seems unlikely that it would be. CSLI is generated automatically as users' phones interact with service providers. There is no expressive act involved. None of this is the result of a user's mental processes. The data is aggregated and stored by cellular service providers. That process is also automatic, and also is not expressive. One might argue that there is an expressive act at the root of the process. After all, someone decided to gather and store the data, wrote the code, and installed the system. But to the extent this preparatory conduct can render the creation, gathering, and storing of CSLI expressive, it is still voluntary, not compelled.[229] Even if it was compelled,[230] any potential Fifth Amendment claim would belong to the cellular service provider, not the customer, because it is the cellular service provider who is being compelled to "speak." But, of course, corporations are not "persons" for purposes of the Fifth Amendment and therefore cannot resist requests to disclose business records on Fifth Amendment grounds.[231] So, although the Fourth Amendment might require law enforcement to get a warrant for CSLI, the Fifth Amendment prohibition against compelled witnessing does not seem to provide any additional constitutional protections.

These are points worth amplifying. Much of the data that law enforcement is likely to want to access on phones and other devices is created by these devices without any intentional actions on the part of users.[232] Con-

225. *Id.* at 2218; Stephen E. Henderson, *Fourth Amendment Time Machines (And What They Might Say About Police Body Cameras)*, 18 U. PA. J. CONST. L. 933 (2016).

226. *Carpenter*, 138 S. Ct. at 2212–13.

227. *See id.*

228. *Id.* at 2222.

229. *Id.* at 2217–18.

230. There is a reasonable argument to be made here that cellular service providers are "compelled" to gather and store CSLI, at least for short, relatively contemporary periods of time. That is because Federal Communication Commission regulations require that cellular service providers be able to identify the locations of callers who use cellular phones to call 911. *See* Stephanie K. Pell, *Location Tracking*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 44, 49 (David Gray & Stephen Henderson eds., 2017). But there is no federal mandate that service providers maintain long records of CSLI or store that information for an extended period of time.

231. Fisher v. United States, 425 U.S. 391, 409–10 (1976).

232. *See, e.g.*, Amanda Watts, *Cops Use Murdered Woman's Fitbit to Charge Her Husband*, CNN (Apr. 26, 2017), https://www.cnn.com/2017/04/25/us/fitbit-womans-death-investigation-trnd/index.html [https://perma.cc/DG7H-KUTT]; *see also* Jacob Gershman, *Prose-*

sider a recent case in Germany.[233] Prosecutors there were assembling evidence against a defendant, Hussein K., who was charged with raping and murdering a woman before disposing of her body next to a river.[234] Investigators were able to establish a pretty clear timeline of the crime, including the period during which the killer had dragged his victim's body down an embankment to the river's edge.[235] Although their suspect was not cooperating, investigators were able to access his iPhone, including data stored on its Health app, which has been an embedded feature of iOS since 2014.[236] That data documented the suspect's descending "stairs" and then ascended "stairs" during the timeframe when the perpetrator had disposed of the victim's body.[237] Not only that, the phone's descent and ascent was roughly equivalent to the height of the embankment next to the river where the victim's body was found.[238] This was a tidy little piece of detective work made possible by a commonly carried electronic device that constantly gathers and stores data documenting how many steps a user has taken and how many stairs he has climbed. But what is important for present purposes is that none of that information was in any way the result of an act of expression by the user. Neither was the generation or recording of that data "compelled" by any government agent.

Although not relevant in the German case, location data gathered and stored by phones and other personal devices can also be useful in establishing a suspect's proximity to a crime or locations associated with a criminal enterprise. Take, as an example, *Carpenter*. There, investigators used CSLI to tie Carpenter to a series of armed robberies by showing that his phone was in close proximity to the crimes when they occurred.[239] Granted, the location data at issue there came from his cellular phone provider rather than the phone itself, but the case nevertheless demonstrates the investigative value of precise location data. *United States v.*

---

cutors Say Fitbit Device Exposed Fibbing in Rape Case, WALL ST. J. (Apr. 21, 2016), https://blogs.wsj.com/law/2016/04/21/prosecutors-say-fitbit-device-exposed-fibbing-in-rape-case/ [https://perma.cc/WY5N-P8CG]; Christine Hauser, *Police Use Fitbit Data to Charge 90-Year-Old Man in Stepdaughter's Killing*, N.Y. TIMES (Oct. 3, 2018), https://www.nytimes.com/2018/10/03/us/fitbit-murder-arrest.html?partner=rss&emc=rss [https://perma.cc/E2AU-TT8S]. Data from these devices is also being used in civil litigation. *See, e.g.*, Samuel Gibbs, *Court Sets Legal Precedent with Evidence from Fitbit Health Tracker*, GUARDIAN (Nov. 18, 2014), https://www.theguardian.com/technology/2014/nov/18/court-accepts-data-fitbit-health-tracker [https://perma.cc/NMU5-XKAE].

233. *See* Philip Kuhn, *Die Version vom Handeln im Affekt ist mit dem heutigen Tag obsolet*, WELT (Aug. 1, 2018), https://www.welt.de/vermischtes/article172287105/Mordprozess-Hussein-K-Die-Version-vom-Handeln-im-Affekt-ist-mit-dem-heutigen-Tag-obsolet.html [https://perma.cc/A6JA-NCHE]. My thanks to Dr. Dominik Herrmann of the Otto-Friedrich-Universität Bamberg for drawing my attention to this case.

234. *Id.*

235. *Id.*

236. *Id.*; Hugh Langley & Husain Sumra, *How to Use Apple Health: Everything You Need to Know About the Platform*, WAREABLE (Apr. 1, 2019), https://www.wareable.com/apple/how-to-use-apple-health-iphone-fitness-app-960 [https://perma.cc/69VV-9ZN2].

237. Kuhn, *supra* note 233.

238. *Id.*

239. Carpenter v. United States, 138 S. Ct. 2206, 2211–12 (2018).

Jones provides another example.[240] In that case, officers used location data generated by a GPS tracking device attached to Jones's vehicle to document his regular proximity to areas associated with a drug conspiracy.[241] Importantly, that location data was generated by a government-installed device rather than Jones's phone, but as Justice Sotomayor pointed out in her influential concurrence in that case, "[w]ith increasing regularity, the government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones."[242] Amplifying this point, Chief Justice Roberts has compared cellular phones to ankle monitors that allow "the Government" to "achiev[e] near perfect surveillance," not just of identified suspects, but all of us.[243] Moreover, much of that data is shared with software applications and stored both on the devices and in the cloud.[244] Nevertheless, under the Court's current Fifth Amendment doctrine, location data generated by native GPS chips, stored on our devices, and shared through the cloud would all be voluntarily produced, apparently immunizing the data from Fifth Amendment protection.

Personal information and location data do not remotely exhaust the kinds of information gathered and stored by electronic devices that might be of interest to law enforcement. For example, many folks now wear fitness trackers and other devices capable of gathering biometric data including heartrate and documenting the precise nature of their movements.[245] There are even sunglasses that monitor brain waves.[246] How helpful would it have been for investigators in the German case if they could have accessed data showing that their suspect had an elevated heartrate during the timeframe when the victim's body was moved and discarded? How much better if they could document that he was engaged in a lot of pulling, lifting, and dragging—all movements that would be recorded by a device to monitor users engaged in sports like CrossFit? To shift the hypothetical, imagine that officers are investigating a car accident where they suspect that one of the drivers fell asleep behind the wheel. It would certainly be helpful if officers could access the driver's Fitbit to see whether his heartrate had dropped just before the crash and his smart glasses to see whether his head lolled and his brainwaves

240. United States v. Jones, 565 U.S. 400 (2012).
241. *Id.* at 403–04.
242. *Id.* at 415 (Sotomayor, J., concurring).
243. *Carpenter*, 138 S. Ct. at 2218.
244. Riley v. California, 573 U.S. 373, 397 (2014).
245. Many fitness trackers are capable of automatically sensing not only when a user has started to exercise but also the activity and specific data relevant to that activity such as cadence rate for runners and strokes per minute for swimmers. *See, e.g.*, FITBIT, INC., FITBIT CHARGE 3 USER MANUAL 34 (2019), https://staticcs.fitbit.com/content/assets/help/manuals/manual_charge_3_en_US.pdf [https://perma.cc/KWM2-B6BM].
246. Husain Sumra, *Smith Lowdown Focus Review*, WAREABLE (Feb. 22, 2018), https://www.wareable.com/reviews/smith-lowdown-focus-smartglasses-review [https://perma.cc/PK2Q-7P6Q]; *A Deep Dive Into Brainwaves: Brainwave Frequencies Explained*, MUSE (June 25, 2018), https://choosemuse.com/blog/a-deep-dive-into-brainwaves-brainwave-frequencies-explained-2/ [https://perma.cc/5UFR-S8QS].

slipped into a pattern consistent with dozing off.[247] Better still, imagine that they had evidence that his heartrate and brainwaves had fluctuated several times in the minutes before the crash, documenting a pattern of dozing and reawakening. That kind of evidence would be useful not only to determine what happened but also to establish that the driver had acted recklessly.

Although no court has squarely addressed the Fifth Amendment status of data on digital devices, cases dealing with similar kinds of information seem to assume that voluntarily or incidentally created information falls within the exceptions carved out by *Muniz* and *Fisher*. That is evident in a relatively new set of cases dealing with the Fifth Amendment consequences of compelling a suspect to decrypt encrypted digital data.[248] Unsurprisingly, a stable consensus has formed for the proposition that compelling a suspect to decrypt encrypted devices or data by non-expressive means, such as a fingerprint or through facial recognition, does not implicate the Fifth Amendment privilege against compelled witnessing.[249] By contrast, courts are divided on the question whether compelling a suspect to disclose or input a passcode is barred by the Fifth Amendment.[250] Some courts have concluded that disclosing or inputting a passcode is testimonial and entitled to full Fifth Amendment protections.[251] Others have admitted the testimonial status of passcodes but have compelled production under the foregone conclusion doctrine, which allows courts to compel testimonial expressions when what is revealed has been established by independent means.[252] As applied to data on personal devices, this suggests that, if officers can show that a device belongs to a suspect, then it is a foregone conclusion that the suspect knows the password and therefore can be compelled to disclose that password to law enforcement

247. This same kind of data would be generated by worn or onboard systems designed to notify drivers if they are losing attention or drifting to sleep. Systems and devices such as these are already available on the consumer market with more sophisticated systems capable of monitoring mood, emotion, and other factors affecting driver safety on the horizon. *See, e.g.*, *Affectiva Automotive AI*, AFFECTIVA, https://www.affectiva.com/product/affectiva-automotive-ai/ [https://perma.cc/27MJ-NY5B] (last visited Oct. 12, 2019).

248. Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 768, 768–70 (2019); Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 FORDHAM L. REV. 203, 205–10 (2018).

249. Kerr, *supra* note 248, at 796. *But see* Sacharoff, *supra* note 248, at 241 (arguing against Kerr); Laurent Sacharoff, *What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr*, 97 TEX. L. REV. ONLINE 63, 63–64 (2019) (same).

250. *Compare In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1349 (11th Cir. 2012) (declaring that compelled decryption violates the Fifth Amendment), *and* United States v. Mitchell, 76 M.J. 413, 420 (C.A.A.F. 2017) (holding that appellees phone was decrypted in violation of the Fifth Amendment), *with* United States v. Apple Mac Pro Comput., 851 F.3d 238, 248–49 (3d Cir. 2017) (allowing compelled decryption), United States v. Spencer, No. 17-cr-00259-CRB-1, 2018 WL 1964588, at *3 (N.D. Cal. Apr. 26, 2018) (same), United States v. Fricosu, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012) (same), State v. Stahl, 206 So. 3d 124, 136–37 (Fla. Dist. Ct. App. 2016) (same), Seo v. State, 109 N.E.3d 418, 425–31 (Ind. Ct. App. 2018), *vacated*, 119 N.E.3d 90 (2018) (compelled decryption not allowed), *and* Commonwealth v. Gelfgatt, 11 N.E.3d 605, 614–15 (Mass. 2014) (allowing compelled decryption).

251. *See* cases cited *supra* note 250.

252. *See* cases cited *supra* note 250.

without violating his Fifth Amendment privilege against compelled witnessing.[253]

Although the law governing compelled decryption is still developing, what is most notable about these cases for the present exploration is what courts and commentators seem to assume: that the contents themselves have no independent claim to Fifth Amendment protection.[254] But is that so obvious? It may be if we look at electronic devices through an analog lens. From this perspective, our electronic devices are vessels akin to diaries, datebooks, and file cabinets stocked with voluntarily created documents. But are smartphones and wearable devices really the same as diaries and datebooks? Perhaps not.

The Supreme Court has recognized some basic anthropological facts about our personal devices: they are ubiquitous, and increasingly, they are part of us.[255] More and more, our electronic devices act as extensions of our carbon-selves. They go with us everywhere, which gives them access to events, experiences, and memories that are uniquely ours. They are parallel first-person observers, but they are also enhancements, allowing us to augment or outsource many functions we once performed using our factory-installed, carbon-based processors. They remember for us. They remind us. They keep track of where we have been and with whom. They monitor our activity, movement, heartrate, and even our mood. They add to our funds of knowledge. And this is just the beginning. We are in the midst of an ongoing process of coevolution with digital technologies. At the forefront are devices that are surgically implanted, in whole or in part, literally becoming part of us.[256] We might now speak metaphorically of devices that are "an important feature of human anatomy,"[257] but today's metaphor is likely to be tomorrow's literalism. We are becoming cyborgs, and these devices are part of us.[258]

If our present relationship with electronic devices marks the beginning of our next evolutionary step, then rules developed to contend with analog technologies like pen and paper appear to have little relevance. To see the point, imagine that neuroscientists were able to break the code of human cognition and developed a device capable of reading thoughts and memories.[259] Would the Fifth Amendment allow law enforcement to

253. Kerr, *supra* note 248, at 773–77.

254. *But see* Choi, *supra* note 204, at 74 (arguing against the separation of devices and data when analyzing the Fifth Amendment status of cellular phones as extensions of users); Slobogin, *supra* note 216, at 841–44 (arguing that the Fifth Amendment should respect a "zone of privacy" protecting some kinds of personal documents).

255. Riley v. California, 573 U.S. 373, 385 (2014).

256. Haley Weiss, *Why You're Probably Getting a Microchip Implant Someday*, ATLANTIC (Sept. 21, 2018), https://www.theatlantic.com/technology/archive/2018/09/how-i-learned-to-stop-worrying-and-love-the-microchip/570946/ [https://perma.cc/WJM5-3PGH].

257. *Riley*, 573 U.S. at 385.

258. The idea that electronic devices can become so integrated with ourselves and our lives so as to extend our cognition was advanced by Andy Clark and David Chalmers. *See generally* Andy Clark & David Chalmers, *The Extended Mind*, 58 ANALYSIS 7 (1998).

259. MICHAEL S. PARDO & DENNIS PATTERSON, MINDS, BRAINS, AND LAW (2013); Michael S. Pardo, *Lying, Deception, and fMRI: A Critical Update*, *in* NEUROLAW AND RE-

compel someone to submit to having his mind read?[260] On one reading of *Fisher* and *Muniz*, the answer seems to be yes.[261] After all, memories are voluntarily or incidentally created and simply reading those memories off a brain would not require an act of expression on the part of a brain's owner. But, upon further consideration, it is clear that arguments along these lines are fallacies based on a fantasy.

The fantasy is a form of dualism. This defense of mind readers imagines that our brains exist separately from our minds, souls, or selves.[262] The Fifth Amendment, so it goes, protects the ghost in the machine,[263] not the meat. Violating the flesh does not sully the soul. This dualistic account of the mind has been roundly debunked by both philosophers[264] and neuroscientists.[265] Although it may be helpful in certain contexts to speak in loose metaphors about our minds as if they exist apart from our brains, they do not; and it is potentially catastrophic to hold otherwise in any context that matters. This is surely one such situation. Taking seriously a dualistic account of mind and body when faced with the prospect of mind reading technology would eviscerate Fifth Amendment protections. After all, we are talking about strapping someone down to a table and forcibly penetrating their innermost thoughts and memories on grounds that the Fifth Amendment provides greater protections for our mouths than our brains and the thin claim that reading thoughts off our brains does not in any way violate our minds. So, even if a scientific method was devised to penetrate the phenomenon of the mind, the brutality of that process would run afoul of the Fifth Amendment.

Courts have not had to take seriously threats posed to the Fifth Amendment by mind reading technologies because no such technologies yet exist. As it stands, our thoughts and memories are encrypted by our inscrutable brains. Nevertheless, it seems quite likely that if investigating agents could compel a suspect to submit to a scan that would decrypt the electrical firings along neural pathways in her brain, then the Fifth

---

SPONSIBILITY FOR ACTION (Bebhinn Donnelly-Lazarov ed., Cambridge University Press, 2018).

260. Kiel Brennan-Marquez, *A Modest Defense of Mind Reading*, 15 YALE J.L. & TECH. 214, 216–21 (2013); Nita A. Farahany, *Incriminating Thoughts*, 64 STAN. L. REV. 351, 351–408 (2012).

261. Brennan-Marquez, *supra* note 260, at 240–41; Farahany, *supra* note 260, at 397–99.

262. The dualist conception of the self traces back at least as far as Plato but is usually associated with the work of Rene Descartes. *See, e.g.*, RENÉ DESCARTES, MEDITATIONS ON FIRST PHILOSOPHY, Meditation VI (Oxford Univ. Press 2008) (1641). Cartesian dualism is a form of what some contemporary philosophers have described as a physicalist or property dualism. Noted philosophers like Chalmers and Frank Jackson defend a form of phenomenalist dualism focused on the explanatory gap between a description of externally observable conditions of a phenomenon and the subjective experience of a phenomenon.

263. GILBERT RYLE, THE CONCEPT OF MIND 18 (Routledge 2009) (1949).

264. *See, e.g.*, *id.*

265. *See., e.g.*, THOMAS SZASZ, THE MEANING OF MIND: LANGUAGE, MORALITY, AND NEUROSCIENCE 106 (1996); George Windholz, *Pavlov and the Mind-Body Problem*, INTEGRATED PHYSIOLOGICAL & BEHAV. SCI., Apr. 1997, at 149–51.

Amendment would stand in the way.[266] If that is right, then it seems that, for the same reasons, we might have good Fifth Amendment grounds to claim a right to go dark. Biology renders our brains opaque to the world unless we choose to decrypt and disclose by some act of expression. The right to go dark, in the form of robust encryption, provides parallel protections for our silicon-based neural enhancements. It is digital insurance that puts our silicon minds on the same footing with our carbon minds, guaranteeing our right against compelled witnessing no matter where we keep and store our thoughts and memories.

IV. A COMMON LAW RIGHT TO GO DARK (?)

A third potential ground for a right to go dark is the law of evidentiary privileges. Evidentiary privileges protect the contents of certain communications against "involuntary disclosure."[267] Although established by statute in many states, evidentiary privileges are grounded in the common law and remain a creature of common law in many jurisdictions, including federal courts. In the federal system, courts' authority to recognize and elaborate evidentiary privileges derives from Federal Rule of Evidence 501, which, in its revised form, provides that:

> The common law—as interpreted by United States courts in the light of reason and experience—governs a claim of privilege unless any of the following provides otherwise:
> - the United States Constitution;
> - a federal statute; or
> - rules prescribed by the Supreme Court.
>
> But in a civil case, state law governs privilege regarding a claim or defense for which state law supplies the rule of decision.[268]

The history of Rule 501 is fascinating. The Supreme Court proposed a very different version of Rule 501 to Congress in 1973.[269] As then con-

---

266. This would, after all, be akin to the kinds of techniques utilized during the Inquisitions of the seventeenth and eighteenth centuries that served, in part, as historical motivation for the Fifth Amendment.

267. Jaffee v. Redmond, 518 U.S. 1, 5 (1996).

268. FED. R. EVID. 501. This most recent version of Rule 501 is the product of the "restyling" project adopted by congressional inaction in December 2011. According to the Committee notes, these revisions are "intended to be stylistic only. There is no intent to change any result in any ruling on evidence admissibility." FED. R. EVID. 501 advisory committee's notes to 2011 amendments. Unrestyled Rule 501 provides that:

> Except as otherwise required by the Constitution of the United States or provided by Act of Congress or in rules prescribed by the Supreme Court pursuant to statutory authority, the privilege of a witness, person, government, state, or political subdivision thereof shall be governed by the principles of the common law as they may be interpreted by the courts of the United States in the light of reason and experience. However, in civil actions and proceedings, with respect to an element of a claim or defense as to which state law supplies the rule of decision, the privilege of a witness, person, government, state, or political subdivision thereof shall be determined in accordance with state law.

FED. R. EVID. 501 (1975) (amended 2011).

269. Trammel v. United States, 445 U.S. 40, 47 (1980).

ceived, Rule 501 would have stripped federal courts' authority to create evidentiary privileges with the exception of privileges dictated by the Constitution, such as the Fifth Amendment privilege against compelled self-incrimination.[270] At the same time, the Supreme Court recommended that Congress recognize a limited number of evidentiary privileges.[271] On that list were a lawyer-client privilege,[272] a psychotherapist-patient privilege,[273] a spousal privilege,[274] a clergy-penitent privilege,[275] a voting privilege,[276] a trade secret privilege,[277] a state secret privilege,[278] and a privilege protecting the identity of informants in criminal investigations.[279] Congress ultimately declined to adopt most of these recommendations. It did recognize an attorney-client privilege but, under Rule 501 as adopted, left the task of creating and elaborating other evidentiary privileges to the courts based on "principles of the common law," "reason," and "experience."[280]

In *Trammel v. United States*[281] and *Jaffee v. Redmond*,[282] the Supreme Court described how it would exercise the authority granted by Rule 501. First, the Court weighs the competing interests at stake in recognizing a privilege.[283] In general, this means assessing the social and public value of a particular relationship[284] and the need for confidential communication to secure those advantages.[285] The Court then weighs those benefits against the costs to truth seeking,[286] recognizing a privilege "only to the very limited extent that permitting a refusal to testify or excluding relevant evidence has a public good transcending the normally predominant

270. FED. R. EVID. 501 (proposed Nov. 20, 1972) ("Except as otherwise required by the Constitution of the United States or provided by Act of Congress, and except as provided in these rules or in other rules adopted by the Supreme Court, no person has a privilege to: Refuse to be a witness; or Refuse to disclose any matter; or Refuse to produce any object or writing; or Prevent another from being a witness or disclosing any matter or producing any object or writing.").

271. *Trammel*, 445 U.S. at 47.

272. FED. R. EVID. 503 (proposed Nov. 20, 1972).

273. FED. R. EVID. 504 (proposed Nov. 20, 1972).

274. FED. R. EVID. 505 (proposed Nov. 20, 1972).

275. FED. R. EVID. 506 (proposed Nov. 20, 1972).

276. FED. R. EVID. 507 (proposed Nov. 20, 1972).

277. FED. R. EVID. 508 (proposed Nov. 20, 1972).

278. FED. R. EVID. 509 (proposed Nov. 20, 1972).

279. FED. R. EVID. 510 (proposed Nov. 20, 1972).

280. FED. R. EVID. 501.

281. 445 U.S. 40 (1980).

282. 518 U.S. 1 (1996).

283. *Trammel*, 445 U.S. at 51 ("Here we must decide whether the privilege against adverse spousal testimony promotes sufficiently important interests to outweigh the need for probative evidence in the administration of criminal justice.").

284. *Id.* at 48 (noting that the marital privilege "is one affecting marriage, home, and family relationships—already subject to much erosion in our day . . . .").

285. *Id.* at 51 (requiring that privileges must be "rooted in the imperative need for confidence and trust.").

286. *Id.* at 50 ("Testimonial exclusionary rules and privileges contravene the fundamental principle that the public has a right to every man's evidence." (citations omitted) (internal quotation marks omitted)).

principle of utilizing all rational means for ascertaining truth."[287] Second, the Court looks to state practices, both as a source of "reason" and "experience" and out of an interest in avoiding conflicts that might frustrate state law by exposing in federal court the contents of communications that would be protected in state courts.[288] Finally, the Court considers federal authorities, including the unadopted rules proposed in 1973. Here, the Court has evinced reluctance to recognize privileges that are not either well-established in the common law[289] or among those enumerated in the unadopted proposed rules.

Jaffee provides a helpful example of how the Court exercises its authority under Rule 501. The question presented there was whether confidential communications between a patient and a licensed social worker in a therapeutic setting should be shielded from discovery during civil litigation.[290] Writing for the Court, Justice John Paul Stevens found that psychotherapy as a practice produces significant social benefits.[291] "The mental health of our citizenry," he wrote, "no less than its physical health, is a public good of transcendent importance."[292] Justice Stevens then highlighted the critical role that confidentiality plays in psychotherapy. In contrast to the diagnosis and treatment of "physical ailments," which "can often proceed successfully on the basis of a physical examination, objective information supplied by the patient, and the results of diagnostic tests," Justice Stevens pointed out that psychotherapists can only access the information they need from patient communications.[293] As a consequence, he continued, "psychotherapy . . . depends upon an atmosphere of confidence and trust in which the patient is willing to make a frank and complete disclosure of facts, emotions, memories, and fears."[294] At the same time, the nature of those disclosures are often very personal and "disclosure . . . may cause embarrassment or disgrace."[295] The possibility that disclosures to a psychotherapist might become public in a court of law, therefore, compromises the entire practice, potentially denying society the significant benefits of professional mental health treatment.[296] At the same time, Justice Stevens argued, the costs to truth-seeking from recognizing the privilege would be "modest."[297] That is be-

287. *Id.* (internal quotation marks omitted) (quoting Elkins v. United States, 364 U.S. 206, 234 (1960) (Frankfurter, J., dissenting)).

288. Jaffee v. Redmond, 518 U.S. 1, 13 (1996). These concerns are familiar from the Fourth Amendment context. *Elkins*, 364 U.S. at 221–22. The Court also consults state practices to assess the contemporary validity of a rule of privilege. *See, e.g.*, *Trammel*, 445 U.S. at 48 (noting that support for the spousal privilege had declined from thirty-two states in 1958 to twenty-four in 1974).

289. *Trammel*, 445 U.S. at 48 ("[T]he long history of the privilege suggests that it ought not to be casually cast aside.").

290. *Jaffee*, 518 U.S. at 20.

291. *Id.* at 10.

292. *Id.* at 11.

293. *Id.* at 10.

294. *Id.*

295. *Id.*

296. *Id.* at 11–12.

297. *Id.* at 11.

cause denial of the privilege would chill psychotherapy considerably, effectively preventing the very disclosures at issue from being made in the first place.[298] Thus, failure to recognize a psychotherapist privilege would dramatically compromise the benefits of psychotherapy without producing a substantial benefit to truth-seeking.[299]

The *Jaffee* Court also found considerable support for a psychotherapist privilege in both state and federal law. As Justice Stevens noted, "[A]ll 50 States and the District of Columbia ha[d] enacted into law some form of psychotherapist privilege . . . ."[300] And "[d]enial of the federal privilege therefore would frustrate the purposes of the state legislation that was enacted to foster these confidential communications."[301] In addition, the psychotherapist-patient privilege was among the rules proposed by the Court to Congress in 1973.[302] Furthermore, the record of the Judicial Conference Advisory Committee's deliberations reflect its view that psychotherapy depends on a patient's "willingness and ability to talk freely," which "makes it difficult if not impossible" for psychotherapy to function without "confidentiality and, indeed, privileged communication."[303] This consensus, the *Jaffee* Court concluded, "indicates that 'reason and experience' support recognition of the [psychotherapist] privilege."[304]

The list of widely recognized evidentiary privileges is short. In addition to the psychotherapist privilege recognized in *Jaffee*, the Court has exercised its authority under Rule 501 to protect confidential communications between spouses.[305] Rule 502 protects attorney-client communications.[306] There is also considerable support in state and federal courts for a clergy-penitent privilege[307] and a right to confidentiality at the ballot box, which were among the privileges recognized in the proposed rules. Although the Supreme Court has been skeptical of a physician-patient privilege,[308] confidentiality is a central feature of medical ethics.[309] Many states protect confidential communications with physicians for the purpose of diag-

298. *Id.* at 11–12.
299. *Id.*
300. *Id.* at 12.
301. *Id.* at 13.
302. *Id.* at 14.
303. *Id.* at 10 (quoting Rules of Evidence for United States Courts and Magistrates, 56 F.R.D. 183, 242 (1972)).
304. *Id.* at 13.
305. Trammel v. United States, 445 U.S. 40, 53 (1980); *see also* Hawkins v. United States, 358 U.S. 74, 80–82 (1958); Funk v. United States, 290 U.S. 371, 382 (1933); Jin Fuey Moy v. United States, 254 U.S. 189, 195 (1920); Graves v. United States, 150 U.S. 118, 121 (1893); Stein v. Bowman, 38 U.S. (1 Pet.) 209, 223 (1839).
306. FED. R. EVID. 502.
307. *See, e.g.*, Morales v. Portuondo, 154 F. Supp. 2d 706, 728–29 (S.D.N.Y. 2001).
308. *See Jaffee*, 518 U.S. at 10 (drawing a distinction between the work of physicians and psychotherapists insofar as "[t]reatment by a physician for physical ailments can often proceed successfully on the basis of a physical examination, objective information supplied by the patient, and the results of diagnostic tests"); *see also* United States v. Bek, 493 F.3d 790, 801 (7th Cir. 2007) ("Federal common law has not historically recognized a privilege between patients and physicians.").
309. For example, most physicians take a professional oath that includes some version of the Hippocratic pledge that "whatsoever I shall see or hear in the course of my profes-

nosis or treatment.[310] Federal law protects the confidentiality of health information,[311] and the Supreme Court has recognized the highly private nature of health-related information.[312] Therefore, there is good reason to include a physician-patient privilege on the tally of established evidentiary privileges. But that probably caps the list.

So, how might the law of evidentiary privileges support a right to go dark? Two possibilities come to mind. First, some digital data, electronic communications, and exchanges with devices may fall within the protections afforded by established privileges. To the extent this is so, a right to go dark would guarantee important protections, putting this data on equal footing with communications between live persons. This seems a perfectly plausible argument, though limited in terms of its scope. Second, we might want to recognize a new privilege that would ground a more general right to go dark, providing broad protections for a wide variety of digital data and devices. Here, the case for a common law right to go dark is on shakier ground. That may well change as our engagements with these technologies expand and evolve. Health-related technologies provide a nice example for discussion.

There is an increasing number of medical health or "mHealth" apps in use on smartphones and wearable devices.[313] Some of these provide platforms through which users can communicate with healthcare professionals. Talkspace is a good example. Talkspace allows customers to communicate directly and anonymously with licensed mental health professionals. Talkspace and similar platforms often have access to the contents of communications between patients and therapists. Some companies commoditize information gleaned from that content.[314] Setting aside this complication, these kinds of apps would otherwise seem to fit nicely within established privileges such as the psychotherapist privilege or the doctor-patient privilege. It would therefore make good sense to recognize a right to encrypt those communications, thereby putting communications through these platforms on the same footing as commu-

---

sion, as well as outside my profession in my intercourse with men, if it be what should not be published abroad, I will never divulge, holding such things to be holy secrets."

310. Policy of the Privilege, 25 FED. PRAC. & PROC. EVID. § 5522 (1st ed.).

311. *See, e.g.*, 45 C.F.R. §§ 160, 164 (2018).

312. *See* Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001).

313. MHealth apps are "medical and public health practice supported by mobile devices." WORLD HEALTH ORG., MHEALTH: THE NEW HORIZONS FOR HEALTH THROUGH MOBILE TECHNOLOGIES 6 (2011), https://www.who.int/goe/publications/goe_mhealth_web.pdf [https://perma.cc/8QJU-DE44]. By 2018, 1.7 billion people (roughly 24% of the world's population) worldwide are expected to use mHealth apps on their smartphones. J. Frazee, M. Finley & JJ Rohack, *MHealth and Unregulated Data: Is This Farewell to Patient Privacy?*, 13 IND. HEALTH L. REV. 385, 385 (2016).

314. A 2015 study of mHealth apps found that nearly all apps studied shared information with third parties deemed sensitive, and at least 10% shared medical information. *See* Jinyan Zang et al., *Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps*, TECH. SCI. (Oct. 30, 2015), http://techscience.org/a/2015103001 [https://perma.cc/8HAM-Q2CV].

nications during live, in person treatment and therapy.[315]

By extension, there might also be good grounds for recognizing a limited right to go dark tailored to apps that diagnose or treat medical or mental illness. Many mHealth apps are making use of artificial intelligence (AI) to diagnose and treat patients. For example, there is an app that uses speech pattern analysis to diagnose Parkinson's disease.[316] Wearable sleep monitors, such as Fitbit, can aid in the diagnosis of sleep disorders. There is a raft of apps that use cognitive behavioral therapy to treat patients with a wide range of mental diseases, including depression and drug addiction. One of these, WoeBot, "uses brief daily chat conversations, mood tracking, curated videos, and word games to help people manage mental health."[317] WoeBot can be prescribed and monitored by a human therapist, but its creators believe it has the potential to operate independently. Using AI, Big Data, and taking advantage of constant access to its patients, WoeBot and its ilk may well be in a better position to monitor and treat patients than sadly limited carbon-based providers.

To the extent WoeBot and similar technologies are playing roles once reserved for human healthcare providers, there is every reason to think that its communications with its patients should be privileged. If that is right, then a right to go dark would give full effect to these protections, putting communications with AI providers on equal footing with those between meat sacks.

There is also a class of mHealth technologies that monitor, gather, and analyze biodata such as vital signs, activity levels, and sleep. Sometimes these apps provide data for human caregivers. For example, there are apps that work in conjunction with glucose monitors and insulin pumps to help patients monitor blood sugar levels and insulin dosing. Similarly, there are apps and devices that monitor heart rate and blood pressure to help physicians diagnose and treat cardiovascular diseases.[318] There are devices patients swallow to monitor when medication is taken and how well it is metabolized.[319] And there are wearable technologies that monitor eye movements to help diagnose vestibular disorders. Although these

315. One might wonder what value a right to go dark adds if we assume that communications through apps like Talkspace are covered by existing rules of privilege. The answer is impenetrability. Incidents of live oral communication are inherently ephemeral absent a specific effort to make a record. Encrypting digital communications puts them in essentially this same existential posture. Encryption would therefore protect these communications from unwarranted intrusion while also preserving the same possibilities for lawful discovery available for oral communications between caregivers and their patients.

316. Melanie Swan, *Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0*, J. SENSOR & ACTUATOR NETWORKS 217, 226 (2012).

317. Megan Molteni, *The Chatbot Therapist Will See You Now*, WIRED (June 7, 2017), https://www.wired.com/2017/06/facebook-messenger-WoeBot-chatbot-therapist/ [https://perma.cc/4WYT-7CP7].

318. *See, e.g.*, ALIVECOR, https://www.alivecor.com/ [https://perma.cc/UV28-VLCB] (last visited Oct. 12, 2019).

319. PROTEUS, http://www.proteus.com/evidence/cardiovascular-diseases/ [https://perma.cc/7AFA-J3KJ] (last visited Oct. 12, 2019).

technologies are clearly used to diagnose and treat physical and mental diseases, it is not clear that the data they gather falls within the protections of established evidentiary privileges. That is because there is no clear act of "communication" in the usual sense.

Evidentiary privileges protect communications. They do not impose a general bar on testimony by informational fiduciaries[320] such as clergy, psychotherapists, and doctors. That was not always the case for all fiduciaries. For example, at common law, the spousal privilege allowed husbands to bar their wives from offering any kind of adverse testimony at a criminal trial.[321] That privilege covered not just communications but all testimony relating to acts or events she might have observed.[322] As the Court reports in *Trammel*, this version of the spousal privilege existed at a time when defendants were barred from testifying on their own behalves at criminal trials out of concern both for self-incrimination and intractable unreliability. Insofar as a wife had no legal status separate from her husband, she too could not testify at a criminal trial where her husband was a defendant and for the same reasons.

The underlying justification of the spousal privilege has evolved considerably, of course. It is now understood as a way to secure and protect the sanctity of the marital relationship and the confidentiality of marital communications.[323] As a consequence, the extent of its protections has contracted considerably. Most relevant for present purposes is that many jurisdictions limit the scope of the privilege to confidential communications only.[324] A spouse may therefore be compelled to testify to her observations of events and any communications that might have occurred in the presence of a third party because none of this testimony involves the disclosure of confidential marital communications—just observations and nonconfidential communications.

The Court has suggested that the doctor-patient privilege follows this same pattern, protecting communications but not observations.[325] Thus, as the Court implied in *Jaffee*, a physician might be compelled to testify about the results of her "physical examination" and "the results of diagnostic tests" even as she stays mum about what her patient *said* in response to diagnostic questions.[326] Notably, this is not how the privilege is universally described. In some jurisdictions, the physician-patient privi-

320. The author takes this phrase from Jack Balkin and Kiel Brennan-Marquez. *See generally, e.g.*, Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016); Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611 (2015).

321. Trammel v. United States, 445 U.S. 40, 44 (1980).

322. *Id.*

323. *Id.* ("The modern justification for this privilege against adverse spousal testimony is its perceived role in fostering the harmony and sanctity of the marriage relationship."); *see also* Hawkins v. United States, 358 U.S. 74, 79 (1958) ("[T]he law should not force or encourage testimony which might alienate husband and wife, or further inflame existing domestic differences.").

324. *Trammel*, 445 U.S. at 44.

325. Jaffee v. Redmond, 518 U.S. 1, 10 (1996).

326. *Id.*

lege covers everything a doctor learns in the course of her professional treatment of a patient.[327] But, to the extent it holds, this distinction between communications and observations complicates the picture considerably when applied to health monitoring devices.

Take, for example, an app designed to help diabetics better control their blood sugars. Such an app might require that a user actively input information, such as foods eaten, activities, insulin doses, and sugar levels taken manually. Insofar as these inputs can be characterized as communications with a physician, they might be privileged and therefore amenable to protection under a right to go dark. But we can also imagine an app that engages in passive, observational data gathering. For example, it might gather blood sugar and insulin-dose data from an insulin pump, activity and location data from a wearable device or smartphone, and event information from an electronic calendar. This kind of passively acquired data would probably be more accurate and complete than a patient's subjective reports, providing a treating endocrinologist with a richer and more nuanced understanding of her patient's disease and treatment. But it probably would not qualify for protection under a doctor-patient privilege because it is passively gathered observational data akin to the physical diagnosis and test results cited by the Court in *Jaffee* as beyond the scope of a communication privilege.

Although results from objective medical tests and data gathered passively by mHealth apps may not be covered by the physician-patient privilege, there are good grounds for arguing that they should be. Statutory versions of the physician-patient privilege in many jurisdictions cover physical diagnosis and test results.[328] That lines up nicely with well-established privacy protections. Specifically, the Health Insurance Portability and Accountability Act (HIPAA) and parallel state laws grant considerable rights to privacy and confidentiality in patient records.[329] In 2015, the Food and Drug Administration (FDA) considered the application of HIPAA to mHealth apps.[330]

Under the FDA's recommended guidelines, data generated by apps and other technologies that act as medical devices would be afforded HIPAA protection.[331] An app acts as a medical device in the view of the FDA when it transforms a mobile platform into a regulated medical device, connects to an existing device for purposes of controlling its opera-

---

327. *See, e.g.*, 81 AM. JUR. 2D *Witnesses* § 428.

328. *See, e.g.*, CAL. EVID. CODE § 992 (West 2007) (including within the definition of "confidential communication between patient and physician" and "information obtained by an examination of the patient").

329. S. 162, 111th Reg. Sess. (Fla. 2009); Federal Employees Electronic Personal Health Records Act of 2007, S. 1456, 110th Cong.; MD. CODE ANN., HEALTH–GEN. § 4-302 (West 2017).

330. U.S. DEP'T OF HEALTH & HUMAN SERS. FOOD & DRUG ADMIN., MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 4 (2015), https://www.inea.com/PDF/Mobile%20Medical%20Applications%2002%2009%202015.pdf [https://perma.cc/XBB3-H83W].

331. *Id*. at 21–26.

tion, or is used to monitor or analyze patient-specific medical device data.[332] Any app or technology prescribed by a physician to aid in the diagnosis and treatment of a disease such as our diabetes app would certainly seem to qualify for protection under these FDA standards. If the data gathered by these devices is protected by HIPAA, then there may be good grounds to argue that they should be protected by the doctor-patient privilege as well. In fact, the digital footprints created by these apps and devices is often more revealing than the information included in a traditional medical health record.[333] After all, traditional testing in a clinical setting captures only one dimension of health status at a particular moment in time. By contrast, these technologies continuously monitor a person's habits, generating a wealth of health data that can be far more revealing.[334]

But these are all fairly specialized technologies. It may be straightforward to argue for protecting communications and data associated with devices that are prescribed or actively monitored by a physician or therapist. But what about the mine-run of mHealth apps deployed and used by users solely on their own initiative? Wearable devices like Fitbit, Pebbles, Garmin, and Apple Watch represent an exploding sector of the market for consumer technologies.[335] Linked to smartphones or cloud-based programs, these devices offer users a way to improve health, fitness, and wellbeing in a wide variety of ways along many dimensions. There are, of course, the standard activity, heartrate, and location trackers that allow users to monitor their exercise sessions and assess daily activity levels. There are also devices targeted at mental health such as PIP, a monitor that works with an accompanying app to help users cope with and reduce stress,[336] and Muse, a headband "that [gives] you accurate, real-time feedback on what's happening in your brain when you meditate"[337] (what could be more conducive to achieving a state of transcendental consciousness!). These kinds of self-help technologies might contribute incidentally to the diagnosis and treatment of disease, but they are really designed to assist users in reaching their own health, fitness, and wellness goals. They therefore would not seem to fall within the protection of any traditional privilege. But might these technologies qualify for their own privilege and thereby provide groundwork for a more general right to go dark? The

332. *Id.*

333. Jane Sarasohn-Kahn, *Here's Looking at You: How Personal Health Information Is Being Tracked and Used*, CAL. HEALTH CARE FOUND. (July 11, 2014), https://www.chcf.org/publication/heres-looking-at-you-how-personal-health-information-is-being-tracked-and-used/ [https://perma.cc/4P8S-7JWB].

334. *See* Frazee, Finley & Rohack, *supra* note 313, at 396.

335. Paul Lamkin, *Wearable Tech Market to Be Worth $34 Billion by 2020*, FORBES (Feb. 17, 2016), https://www.forbes.com/sites/paullamkin/2016/02/17/wearable-tech-market-to-be-worth-34-billion-by-2020/#7951b55d3cb5 [https://perma.cc/3L2J-ZKH4].

336. PIP, https://thepip.com/en-us/ [https://perma.cc/98BR-RSTW] (last visited Oct. 12, 2019).

337. MUSE, https://choosemuse.com/blog/40-days-of-meditation-with-muse-a-journey/ [https://perma.cc/H6K2-EYG2] (last visited Oct. 12, 2019).

best way to answer that question is to follow the analytic course charted by the Court in *Trammel* and *Jaffee*.

There can be little doubt that users' relationships with mHealth apps have significant social and public value. As the Court recognized in *Jaffee*, the physical and mental health "of our citizenry . . . is a public good of transcendent importance."[338] The Centers for Disease Control estimates that there were nearly 200,000 preventable deaths in 2014 attributed to heart disease, cancer, respiratory disease, and cardiovascular disease.[339] Researchers estimate that tens of thousands of these deaths could be prevented by lifestyle changes.[340] In addition to mortality, there are significant morbidity and treatment costs associated with diseases linked in part to lifestyle.[341] For example, treatment of Type 2 diabetes can exceed $100,000 over the lifetime of a patient,[342] and the American Diabetes Foundation estimates that the total costs of morbidity and treatment of Type 2 diabetes and prediabetes in the United States exceeds $322 billion each year.[343] Given these numbers, there can be little doubt that mHealth devices designed to prevent, treat, and manage diseases by affecting lifestyle have tremendous potential value for society.[344]

---

338. Jaffee v. Redmond, 518 U.S. 1, 11 (1996).

339. Macarena C. García et al., *Potentially Preventable Deaths Among the Five Leading Causes of Death—United States, 2010 and 2014*, 65 MORBIDITY & MORTALITY WEEKLY REP. 1245, 1247 (2016).

340. Alice Park, *Nearly Half of US Deaths Can be Prevented with Lifestyle Changes*, TIME (May 1, 2014), http://time.com/84514/nearly-half-of-us-deaths-can-be-prevented-with-lifestyle-changes/ [https://perma.cc/8EKG-TZKN].

341. Fatma Al-Maskari, *Lifestyle Diseases: An Economic Burden on the Health Services*, XLVII UN CHRONICLE 2 (2010), https://unchronicle.un.org/article/lifestyle-diseases-economic-burden-health-services [https://perma.cc/T9J6-ZSU7].

342. Xiaohui Zhuo et al., *Lifetime Direct Medical Costs of Treating Type 2 Diabetes and Diabetic Complications*, 45 AM. J. PREV. MED. 253, 257 (2013).

343. AMERICAN DIABETES ASS'N, http://www.diabetes.org/diabetes-basics/statistics/infographics/adv-staggering-cost-of-diabetes.html [https://perma.cc/R4QG-NKMG] (last visited Oct. 12, 2019).

344. *See, e.g.*, Lisa A. Cadmus-Bertram et al., *Randomized Trial of Fitbit-Based Physical Activity Intervention for Women*, 49 AM. J. PREVENTIVE MED. 414, 414 (2015) ("The Fitbit was well accepted in this sample of women and associated with increased physical activity at 16 weeks. Leveraging direct-to-consumer *m*Health technologies aligned with behavior change theories can strengthen physical activity interventions."); Deborah F. Tate, Elizabeth J. Lyons & Carmina G. Valle, *High-Tech Tools for Exercise Motivation: Use and Role of Technologies Such as the Internet, Mobile Applications, Social Media, and Video Games*, 28 DIABETES SPECTRUM 45, 46 (2015) (finding that technology designed to promote exercise can have positive health effects in patients with type-2 diabetes). As a bit of field research for this article, the author acquired and deployed a health monitoring device on his person. The results were positive. The author began to exercise more consistently. During the eighteen-month study period, he completed two half marathons, two sprint-distance triathlons, an Olympic-distance triathlon, and several 5k races. Prior to the experiment, he had never run more than a couple of miles and had difficulty swimming fifty continuous yards. His resting heart rate has slowed from the sixties or seventies to the high forties. His VO2 Max has improved from forty to fifty-six—whatever that means. He has lost fourteen pounds and his body composition has improved by 3% to 4% percent. His LDL cholesterol has gone down substantially as have his triglyceride levels. Over the same period, his HDL cholesterol has gone up, resulting in an improvement in the ratios used to assess risk of major cardiovascular events. Moreover, it has been the author's experience that the ability to track health and performance data is a significant motivator to exercise.

But do we need to preserve the confidentiality of communications with mHealth devices in order to gain these benefits? Confidentiality, for purposes of common law privileges, is usually regarded as necessary if honest communication is essential to achieve the desired goals of a communicative relationship, and participants are unlikely to be open and honest if they fear revelation. It seems pretty clear that mHealth devices like Fitbit would not generate the health and wellness benefits they promise if they did not have access to accurate information. Lying to or tricking a Fitbit does not do anyone any good. Similarly, these devices are more likely to provide more benefits the more they have access to us and our activities. These technologies hold the most promise for improving health and wellness if they are part of an informational ecosystem that tracks daily activity, exercise, sleep, food and beverage intake, stress levels, social engagement, etc. To fulfill their potential then, we need to communicate openly and honestly with these technologies. But would that open and honest communication be compromised by the threat of revelation in a court of law?

The nature of the information we share with mHealth technologies is bound to be intimate, private, and revealing. Directly and inferentially, these technologies know our daily habits, when we have sex, with whom, when we menstruate, our institutional affiliations, and our personal and professional associations, not to mention details about body composition. In many ways, gaining access to these devices is akin to gaining access to our inner selves and our most private moments. Given the nature and extent of this information sharing, one might well expect that the threat of revelation would decrease the likelihood of open and honest communication with mHealth devices. Speaking for himself, it is one of the principal reasons the author was reluctant to wear or use them.[345] But the author appears to be in a minority. The raw truth is that these devices are already in widespread use and the market is growing.[346] At the same time, many users readily share information gathered by these devices with others, including online communities, in order to gain the additional benefits of training advice or community support.[347] Moreover, there is good evidence that this sharing actually enhances the likelihood of achieving sustained benefits by providing motivation and accountability.[348] On the other hand, it may well be the case that more people would

---

Of course, this is anecdata based on an *n* of one, but it supports the promise of these devices to promote health.

345. The author overcame this reluctance for the good of science. *See supra* note 344. As with most electronic devices, fitness trackers have privacy settings that can be adjusted by the user. The author locked his down but remains skeptical of the actual protections afforded by the privacy settings.

346. Sarah Perez, *IDC: Apple Led Wearables Market in 2018, With 46.2M of the Total 172.2M Devices Shipped*, TECHCRUNCH (Mar. 5, 2019), https://techcrunch.com/2019/03/05/idc-apple-led-wearables-market-in-2018-with-46-2m-of-the-total-172-2m-devices-shipped/ [https://perma.cc/96WG-2F4H].

347. Examples include Garmin Connect, Strava, and iFit.

348. *See* Mark Lemstra et al., *Weight Loss Intervention Adherence and Factors Promoting Adherence: A Meta-Analysis*, 10 PATIENT PREFERENCE & ADHERENCE 1547, 1547

be more likely to use mHealth devices if they were private and secure. So, offering the protections of privilege might expand the universe of users, thereby increasing social utility. And, of course, any user of mHealth devices would always be free to waive that privilege in order to access additional services.

The last factor to consider is legal precedent in state law or federal statute. Here, the record is thin. Predictably, a personal electronic device privilege was not on the list presented to Congress in 1973. To date, at least, there is no state authority directly on point. The most relevant source of "reason" and "experience" may therefore be the FDA framework outlined above. Under those guidelines, the records generated by personal technologies would be protected under HIPAA only if they were acting as a medical device. Although technologies aimed at enhancing health and wellness might credibly be described as advancing medical interests, it seems a stretch to categorize them as medical devices akin to insulin pumps and echocardiographs.

In sum, there seems to be a good case for a limited right to go dark for some devices based on existing privileges such as the psychotherapist-patient and doctor-patient privileges. That is particularly true where the device acts as a conduit for communications between patients and caregivers. There is also a reasonable case to be made that monitoring devices prescribed by a physician or therapist in order to gather sensitive data for purposes of diagnosis or treatment would also be subject to a claim of privilege by reference to existing FDA standards. By contrast, there does not seem to be good grounds for a general right to go dark when it comes to personal electronic devices adopted by users on their own initiative. But that may well change.

Under the framework developed by the Court in its Rule 501 jurisprudence, much turns on the nature of the communications, social utility, and the importance of confidentiality. As we saw in our analysis of the Fifth Amendment, the trend is clearly in the direction of more integration between carbon and silicon systems. It is hard to imagine at this stage the cultural shifts that these technological developments might bring with them. In ten years, it may be obvious that information shared with personal electronic devices must be privileged in order to garner critical social benefits. But if that is the future, then we have not yet arrived.

There is one more possibility worth our consideration. Recall that one justification for the spousal privilege under the common law was the proposition that a wife had no legal status independent of her husband. As a consequence, compelling a wife to testify against her husband was equivalent to compelling him to testify against himself. Although abandoned in the context of the law of spousal privilege, that insight might add dimension to a right to go dark grounded in evidentiary privileges just as it did in the Fifth Amendment context. Given our relationships

(2016) (finding that exercise "interventions that offered social support had higher adherence than those without social support").

with many of our personal devices and the degrees of access they have to our lives, it is not a stretch to say that they are extensions of ourselves.[349] To the extent this is so, perhaps our devices should qualify for a version of the old common law spousal privilege. Recognizing a right to go dark would guarantee our authority to determine whether our devices can testify against us. If that were the law, then a derivative right to go dark would guarantee that nothing our devices know as a consequence of being our devices could ever be used against us unless we affirmatively waived.

V. CONCLUSION

New and emerging technologies invite all of us to be futurists. It is hard to know the nature of what is to come. What is certain is that these technologies are bound to compel changes in the law necessary to accommodate the new and important roles they will play in our lives. One question we will need to answer at some point is whether and to what degree we will have the right to secure the data, information, and communications gathered by, lodged on, and conducted through personal technologies like smartphones and wearable devices. The Supreme Court has already held that accessing this kind of information is a search that requires a warrant. But is that enough? In addition to the procedural protections afforded by a warrant requirement, should we also enjoy a right to go dark, effectively preventing all access to our data and communications absent our consent? Although this article has not offered a definitive answer to this question, it has provided a framework for assessing where we are in the hope that it will be helpful in charting a course for where we might go in the future.

349. Riley v. California, 573 U.S. 373, 385 (2014).