Maryland Law Review

Volume 79 | Issue 1 Article 5

"Only the Beginning, Only Just the Start . . . Mostly I'm Silent": New Constitutional Challenges with Data Collection Devices Brought into the Home

Carol Nackenoff

"ONLY THE BEGINNING, ONLY JUST THE START . . . MOSTLY I'M SILENT"[1]: NEW CONSTITUTIONAL CHALLENGES WITH DATA COLLECTION DEVICES BROUGHT INTO THE HOME

CAROL NACKENOFF*

I. INTRODUCTION

Last December, our son purchased a Google Assistant for my husband, who uses it to do very simple things—check the weather, play music, set a cooking timer, and ask questions such as who won the World Series in 2001 (answer: the Arizona Diamondbacks). Google Assistant (which disappointingly has no other name), Alexa (Amazon), Cortana (Microsoft), Siri (Apple), Google Home, and other artificial intelligence ("AI") devices wait for the wake word and only seem to sleep. They listen, and when summoned, respond. These assistants get smarter each year. Perhaps in the not very distant future, such devices can and will record for far longer than a minute. Digital assistants are everywhere: There are even voice-activated, self-driving refrigerators (which we must need in some sick universe so that someone can determine whether we grabbed a cold, hoppy IPA or an organic carrot).[2] Even without these specific digital assistants, most of us probably already live in smart homes with smart phones, cameras, TVs, toothbrushes, and beds, and have plenty of data collected by the Internet of Things.[3] The collection list expands further when we rove with smart cars and Fitbits. We may even be unaware of the data collection capacities or defaults on some of the devices we willingly bring into our lives.[4] The Internet of Things refers

1. The quotation is part of the lyrics of the Chicago Transit Authority song, written by Robert Lamm. CHICAGO TRANSIT AUTHORITY, BEGINNINGS, *on* CHICAGO TRANSIT AUTHORITY (Columbia Records, 1969).

* Swarthmore College. My research assistant, Gilbert Orbea '19, made it possible for me to understand more about this brave new world, and I could not have written this paper without his help. He participated in the 2018 Schmooze and will be attending Yale Law School.

2. Noah Friedman, *Panasonic Revealed a Self-Driving Fridge—and It Comes to You When You Call It*, BUS. INSIDER (Sept. 6, 2017, 3:56 PM), https://www.businessinsider.com/panasonic-voice-activated-fridge-2017-9.

3. Apparently, Android phones are especially good at passive data collection by comparison with the iPhone. DOUGLAS C. SCHMIDT, GOOGLE DATA COLLECTION 14 (2018), https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf.

4. In some cases, the tracking-location feature default is "on" and the consumer has to intervene to opt out. Google tracks location history even if the user has turned it off. *See* Emily Dreyfuss, *Google Tracks You Even if Location History's Off. Here's How to Stop It*, WIRED (Aug. 13, 2018, 1:37 PM), https://www.wired.com/story/google-location-tracking-turn-off/.

to "networks of common devices that transmit data to each other through tiny radio sensors . . . [creating] in essence, self-cybersurveillance."[5] These devices contribute to the enormous amounts of personal data many of us create for our own use—and for use by others. "Activities that were once private or shared with the few now leave trails of data that expose our interests, traits, beliefs, and intentions."[6]

By one estimate, fifty to seventy-five billion devices worldwide may be connected on the Internet of Things by 2020, revealing patterns of daily life.[7] As early as 2008, the National Intelligence Council's report on Disruptive Civil Technologies envisioned that by 2025, there would exist an Internet of Things consisting of "everyday objects, that are readable, recognizable, locatable, addressable, and/or controllable via the Internet."[8] As one recent scholar writes, "'Smart' devices radiate data," making it at least technologically possible to track nearly everything.[9] There is even a hashtag for this phenomenon: #sensorveillance.[10]

Probably the most popularly used term today, however, is "surveillance capitalism," a term coined by Professor Shoshana Zuboff because human experience is unilaterally claimed "as free raw material for translation into behavioral data."[11] Almost two decades ago, Google became the pioneer in capturing behavioral data for use beyond service improvement—what Professor Zuboff terms "behavioral surplus";[12] we now find the proliferation of "new surveillance-based ecosystems in virtually every economic sector."[13]

---

5. Steven I. Friedland, *The Internet of Things and Self-Surveillance Systems*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 198, 198 (David Gray & Stephen E. Henderson eds., 2017).

6. Alessandro Acquisti et al., *Privacy and Human Behavior in the Age of Information*, 347 SCI. 509, 509 (2015).

7. Andrew Guthrie Ferguson, *The 'Smart' Fourth Amendment*, 102 CORNELL L. REV. 547, 551 (2017) (citing Tony Danova, *Morgan Stanley: 75 Billion Devices Will Be Connected to the Internet of Things by 2020*, BUS. INSIDER (Oct. 2, 2013, 4:16 PM), http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10).

8. NAT'L INTELLIGENCE COUNCIL, DISRUPTIVE CIVIL TECHNOLOGIES: SIX TECHNOLOGIES WITH POTENTIAL IMPACTS ON US INTERESTS OUT TO 2025 F-1 (2008), fas.org/irp/nic/disruptive.pdf.

9. Ferguson, *supra* note 7, at 547.

10. The term seems to have been coined by Andrew Guthrie Ferguson, who uses and claims to have originated this term for data trails in *The 'Smart' Fourth Amendment*. Ferguson, *supra* note 7.

11. SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 8 (2019) [hereinafter ZUBOFF, SURVEILLANCE CAPITALISM]. For the origin of the term, see Shoshana Zuboff, *A Digital Declaration*, FRANKFURTER ALLGEMEINE (Sept. 15, 2014, 11:03 AM), https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshan-zuboff-on-big-data-as-surveillance-capitalism-13152525.html.

12. ZUBOFF, SURVEILLANCE CAPITALISM, *supra* note 11, at 74–75.

13. John Laidler, *High Tech is Watching You*, HARV. GAZETTE (Mar. 4, 2019), https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/ (interviewing Shoshana Zuboff).

Google continues to innovate with home devices. Google Home can play audio from your phone, show your favorite personal photos on a smart TV screen (think Jeff Bezos and Anthony Weiner),[14] plan your day, create your shopping list ("ok Google, I need to buy pseudoephedrine for my basement meth lab"), control other smart devices in your home, call businesses and friends, cook your favorite recipes, and remember things you tell it to ("ok Google, remember that I socked $20,000 inside my left Wellington boot in the upstairs hall closet"). It can send text messages and (through If This Then That[15]) send e-mail. And it allows its owner to voice shop: "What could be dreamier than to speak and have it be so?"[16]

"Google collects all Google Assistant queries, whether audio or typed. It also collects the location where the query occurred."[17] Google Assistant is apparently available on at least 400 million devices, including speakers and some wireless headphones produced by third parties, and Google can collect data from all of these.[18]

What these devices hear—and keep—is based on proprietary algorithms. Americans are already being sentenced based in part on data collected by algorithm.[19] More than a decade ago, Professor Jack Balkin recognized, "[t]he Algorithmic Society features the collection of vast amounts of data about individuals and facilitates new forms of surveillance, control, dis-

14. Regarding Google Photos, "Google records the time and GPS coordinates for every photo taken. Google uploads images to the Google cloud and conducts image analysis to identify a broad set of objects, such as modes of transportation, animals, logos, landmarks, text, and faces." SCHMIDT, *supra* note 3, at 33. However, unless the user gives the app permission, Google will not provide data distinguishing among individual people. *Id*. Jeff Bezos and Anthony Weiner provide two prominent, recent examples of public figures who lost control of personal photos. *See* James Ball, *Jeff Bezos' Photos Show That No One's Intimate Selfies Are Safe, and That They Aren't a Big Deal*, NBC NEWS THINK (Feb. 8, 2019, 1:04 PM), https://www.nbcnews.com/think/opinion/jeff-bezos-photos-show-no-one-s-intimate-selfies-are-ncna969376; Michael Gold, *Anthony Weiner Released from Prison After Serving 18 Months for Sexting Teenager*, N.Y. TIMES (May 14, 2019), https://www.nytimes.com/2019/05/14/nyregion/anthony-weiner-prison-release.html (reporting on the former U.S. Congressman's sexting behavior, imprisonment, and release).

15. IFTTT, or "If This Then That" involves triggers and actions using chains of simple conditional statements. With an IFTTT account, the user employs apps and recipes, allowing Alexa or Google Assistant to sync with other smart home devices that were not designed to work well with each other. IFTTT permits fast on-demand automation of tasks, such as making coffee, powering on an entertainment system, locking doors, finding an iPhone, sending a shopping list to a phone, and setting up reminders. IFTTT, https://ifttt.com/ (last visited Sept. 27, 2019).

16. ZUBOFF, SURVEILLANCE CAPITALISM, *supra* note 11, at 261.

17. SCHMIDT, *supra* note 3, at 32.

18. *Id*. at 33.

19. Eric Loomis was sent to jail in Wisconsin based in part on predictions of future violent action generated by an algorithm. *See* Adam Liptak, *Sent to Prison by a Software Program's Secret Algorithms*, N.Y. TIMES (May 1, 2017), https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html.

crimination and manipulation, both by governments and by private companies," and called this "the problem of Big Data."[20] The existence of big data creates incentives and temptations for bulk data collection by the federal government and law enforcement officials, in the name of keeping us safe from terrorist attacks *and* from criminals.[21] "Government's increasing use of surveillance and data mining is a predictable result of accelerating developments in information technology."[22] Policymakers crave certainty, control in the face of volatility, and seek to turn "*unmeasurable uncertainty* into *measurable risk*."[23]

While government and corporate collection and use of big data may appear to be quite separate, there are areas of convergence, and a number of common constitutional and political issues. As Professor Andrew Guthrie Ferguson views the matter:

> [P]rivate big data companies are suctioning up vast streams of consumer data to target individuals or families for commercial gain. Law enforcement agencies are building information centers to collect, aggregate, and disseminate criminal records data and other forms of biometric data and locational data for investigative advantage. While developing along separate evolutionary paths, these collection and aggregation systems have begun overlapping in practice. . . . Private companies sell personal data to law enforcement. Law enforcement integrates this information with publicly available data. Databases merge, blend, and share related private-public data.[24]

Stated starkly, "What was once private-consumer data can quite easily be repurposed as the raw material for law enforcement databases. At the most

20. Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1153 (2018).

21. *See* Jack M. Balkin & Sanford Levinson, *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 FORDHAM L. REV. 489, 522–25 (2006) (discussing the parallel track criminal law could take).

22. Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 3 (2008).

23. Gernot Rieder, *Tracing Big Data Imaginaries Through Public Policy*, *in* THE POLITICS OF BIG DATA: BIG DATA, BIG BROTHER? 89, 97 (Ann Rudinow Sætnan et al. eds., 2018).

24. Andrew Guthrie Ferguson, *Big Data Surveillance: The Convergence of Big Data and Law Enforcement*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW, *supra* note 5, at 171; *see also* Friedland, *supra* note 5, at 216 ("[A] critical point of government access to self-generated data occurs through public-private partnerships, whereby the government intentionally aligns with companies to obtain data."). According to Professor Friedland, companies sometimes agree to weak encryption software products that government can break. *See id*. at 216; *see also* Ryan Sabalow, *Indiana State Police Tracking Cellphones—but Won't Say How or Why*, INDIANAPOLIS STAR (Dec. 9, 2013, 1:18 PM), https://www.indystar.com/story/news/2013/12/08/indiana-state-police-tracking-cellphones-but-wont-say-how-or-why/3908333/.

basic level, law enforcement has simply become another customer for big data information."[25]

A. Smart Home Devices, the Constitution, and the Supreme Court

In this Essay, I focus on the collection of data from the devices we bring into our homes, though the questions raised apply to a wider array of data and data collection techniques. Current definitions of privacy and assumptions about the right to privacy in the home are inadequate to deal with challenges posed by "smart home" devices.[26] The question of who has property rights to data collected from home assistants is also provocative. According to one recent examination of such challenges, as we bring more devices capable of "spying" into the home, "often these smart objects are linked to data streams or other devices that leave the home—thereby literally taking private matters into public space."[27] But this claim assumes that we know, or should know clearly, what matters are private in this brave new world.

The devices in our homes have been described as part commodity, part property, and part expression.[28] What kind of expectations of privacy should purchasers of personal assistant devices have when they bring them into the home? What should—and should not—be protected speech in the era of smart speakers, cars, appliances, cameras, and cellphones connected to the internet that can "talk" to each other? Who owns and controls the data that our Google Assistant and similar devices collect? The answer is not simple when bundles of data points are bought and sold in the marketplace. Clearly, big data is also big business.[29] To offer up an example, a U.S. data broker known as Acxiom "collects, analyses and trades vast amounts of consumer information, and combines their client's customer data with data of other sources. Acxiom claims to provide access to up to 5,000 data elements on 700 million people worldwide," and has customers in Europe as well as the United States, providing services that include data and marketing, risk mitigation, fraud detection, and identity verification.[30] When owners of home assistants use them to make purchases, monitor their health, order up a ride

25. Ferguson, *supra* note 24, at 189.

26. Lisa van Dongen & Tjerk Timan, *Your Smart Coffee Machine Knows What You Did Last Summer: A Legal Analysis of the Limitations of Traditional Privacy of the Home Under Dutch Law in the Era of Smart Technology*, 14 SCRIPTED 208, 210–11 (2017), https://script-ed.org/wp-content/uploads/2017/12/vandongen_timan.pdf.

27. *Id.* at 208.

28. Ferguson, *supra* note 7, at 549.

29. *See* KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS 133–79 (2017).

30. Ingrid Schneider, *Bringing the State Back in: Big Data-Based Capitalism, Disruption, and Novel Regulatory Approaches in Europe*, *in* THE POLITICS OF BIG DATA: BIG DATA, BIG BROTHER?, *supra* note 23, at 138 (citing WOLFIE CHRISTL, CRACKED LABS, CORPORATE SURVEILLANCE IN EVERYDAY LIFE (2017), https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf).

on Uber, or are detected engaging in potential criminal activity, some of these activities become datapoints that companies collect and resell.[31]

What about Fourth Amendment protections for "persons, houses, papers, and effects"?[32] Professors David Gray and Danielle Citron claim that "[t]he Fourth Amendment was conceived, and has long served, as a bulwark against law enforcement's teleological tendency toward a surveillance state" and should play an important role in the face of growing surveillance capacity.[33] However, what constitutes a search or seizure at law changes, and technology may play a role. As Professor Mark Graber notes, "Controversies over what constitutes an unconstitutional search are driven by expansions in state capacity to see. . . . New devices permit government officials to see what they could not previously see."[34] The very notion of home morphs: "That our walls are dense and deep is of no importance now because the boundaries that define the very experience of home are to be erased. . . . Big Other swallows refuge whole, along with" any notion of home as sanctuary.[35]

Are data gathered from devices such as Google Assistant or Alexa any part of the property of the persons who rely upon them? Who can claim a right to shield such data from search and seizure? While the term "persons" has generally been understood to mean "the human body and the information located on and around the human body,"[36] is some part of the "personal" involved when information is collected in the home and residing on servers somewhere? What are "reasonable expectations of privacy" in terms of informational security in a "sensorveillance" world?[37] Is such protection as the Court is willing to consider the protection of person, place (phone booth), or thing (trash bags on the curb, a purchased device)?[38]

Despite the existence for some time of bulk electronic data collection from items we have purchased and a few Supreme Court decisions of note on new data collection techniques, such as *Kyllo v. United States*,[39] *United States*

31. *See, e.g.*, Derrick Harris, *The One-Night Stand, Quantified and Visualized by Uber*, GIGAOM (Mar. 26, 2012, 4:05 PM), https://gigaom.com/2012/03/26/uber-one-night-stands/.

32. U.S. CONST. amend. IV.

33. David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 69, 92 (2013).

34. Mark A. Graber, *Seeing, Seizing, and Searching Like a State*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW, *supra* note 5, at 417.

35. ZUBOFF SURVEILLANCE CAPITALISM, *supra* note 11, at 478.

36. Ferguson, *supra* note 7, at 590.

37. *Id*. at 549 (posing these questions).

38. Person, Place, or Thing was a once-popular noun game.

39. 533 U.S. 27 (2001). In a 5-4 decision written by Justice Scalia (joined by Justices Thomas, Breyer, and Ginsburg, who remain on the Court in 2019), the Court held that a heat-sensing device aimed at a home to detect marijuana growing inside constituted an unconstitutional search. *Id*. at 40 ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant.") .

v. Jones,[40] *Riley v. California*,[41] and *Carpenter v. United States*,[42] I contend there is relatively little we currently know about where the Court is going on such matters, whether they are interpreting the Stored Communications Act (1986),[43] relying on other statutory authority, or drawing upon precedents in First and Fourth Amendment case law. The most I think we can say clearly at the moment is that the Chief Justice seems reluctant to grant wide powers to government and law enforcement officials in the name of the third-party doctrine, and that he has sided with the Court's liberals in rejecting some data searches that may prove relevant to matters involving Alexa and Google Assistant.

B. Of Trash Bags and Cell Phone Data

For a number of years, the Court has been following the third-party doctrine, which holds that our personal data, when entrusted to the companies that provide services to us, fall outside the Fourth Amendment's protection (government agencies do not need to get a warrant or show probable cause to obtain that data). After *Katz*, this third-party doctrine developed in *United States v. Miller*[44] and *Smith v. Maryland*[45] to hold that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[46] Thus, it seems that when the government wants to obtain your information, if you have voluntarily entrusted your personal data to companies providing you services, the government does not need a search warrant—the Fourth Amendment is not triggered and the government has considerable latitude in its search.

40. 565 U.S. 400 (2012) (holding that installation of a GPS tracking device on a motor vehicle and using that information to monitor the vehicle's movements constituted a search, requiring a warrant). The decision was unanimous, and Justice Scalia wrote the majority opinion. Justice Sotomayor's concurrence stresses how physical intrusion on property is no longer necessary for many forms of surveillance and that data surveillance should remain subject to the *Katz* test. *Id*. at 416–17 (Sotomayor, J., concurring) (noting that with monitoring and long-term storage of data "the government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse"). Justice Sotomayor signaled the third-party doctrine is ill-suited to the digital age. *Id*.

41. 573 U.S. 373 (2014). In a unanimous decision, with majority opinion written by Chief Justice Roberts, the Court held that the search and seizure of Riley's cell phone without a warrant was an unconstitutional search. In the opinion, the Chief Justice quoted Justice Sotomayor's *Jones* concurrence: "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id*. at 396 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).

42. 138 S. Ct. 2206 (2018); *see infra* notes 53–65 and accompanying text.

43. The Stored Communications Act provides language about when warrants are needed and when subpoenas are sufficient in collecting data from internet service providers and covers voluntary and compelled disclosure of data. 18 U.S.C. §§ 2701–12 (2012).

44. 425 U.S. 435 (1976).

45. 442 U.S. 735 (1979).

46. *Id*. at 743–44; *see also Miller*, 425 U.S. at 435; Katz v. United States, 389 U.S. 347 (1967).

Some Supreme Court Justices simply contend that there is no personal property interest in electronic records for purposes of the Fourth Amendment. Thus, Justice Thomas wrote in his dissent in *Carpenter v. United States*, "[T]he Government did not search Carpenter's property. He did not create the records, he does not maintain them, he cannot control them, and he cannot destroy them."[47] In one of Justice Kennedy's final cases, he also reasoned in his dissent that Carpenter did not have any legitimate expectation of privacy in his records because he neither owned nor controlled his cell phone records.[48] While Justice Alito's position is more complicated than my characterization here, he is concerned about how limitations on the third-party doctrine might hamstring law enforcement in their valuable and legitimate investigative practices.[49] Justice Kavanaugh's record includes a considerable number of opinions favoring law enforcement and government surveillance interests, including allowing bulk collection of telephone data (*Klayman v. Obama*[50]) and the use of GPS tracking devices in a case that would become *United States v. Jones*.[51] According to one analyst of his opinions for the United States Court of Appeals for the District of Columbia Circuit, "[i]n a close case that requires balancing of interests, the cases suggest, [Justice] Kavanaugh is more likely to approach the case from the government's perspective than from the individual's perspective."[52] It is certainly likely that the newest Justice will continue to favor the surveillance state for the foreseeable future.

However, another line of argument has gained some traction with less conservative Justices. In her influential *Jones* concurrence, Justice Sotomayor worried about government's increasing capacity to collect electronic data on many aspects of a person's life, altering the relationship between citizen and government. She argued that the third-party doctrine was "ill suited to the digital age, in which people reveal a great deal of information about

47. Carpenter v. United States, 138 S. Ct. 2206, 2235 (2018) (Thomas, J., dissenting). For Thomas, "[t]he *Katz* test has no basis in the text or history of the Fourth Amendment." *Id*. at 2236.

48. *Id*. at 2226–27, 2229 (Kennedy, J., dissenting).

49. *See id.* at 2247, 2255–57 (Alito, J., dissenting).

50. 805 F.3d 1148 (D.C. Cir. 2015).

51. Justice Kavanaugh thought the placement of the GPS device on the appellant's Jeep might not constitute a search; he wanted the case reheard. *See* United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) (Kavanaugh, J., dissenting), *aff'd in part*, 565 U.S. 400 (2012). The case was called *United States v. Maynard* when it was originally before the D.C. Circuit on appeal. Professor Orrin Kerr believes Justice Kavanaugh's position in *Klayman v. Obama*, 805 F.3d 1148 (D.C. Cir. 2015), a solo concurrence denying an en banc rehearing, was technically correct prior to *Carpenter*—i.e., that the metadata the NSA was receiving from phone calls (numbers dialed but not contents) was consistent with the Supreme Court holding in *Smith*. Orin Kerr, *Judge Kavanaugh on the Fourth Amendment*, SCOTUSBLOG, (July 20, 2018, 6:16 PM), https://www.scotusblog.com/2018/07/judge-kavanaugh-on-the-fourth-amendment/; *see also* Jonathan Hafetz, *Judge Kavanaugh's Record in National-Security Cases*, SCOTUSBLOG (Aug. 29, 2018, 11:02 AM), https://www.scotusblog.com/2018/08/judge-kavanaughs-record-in-national-security-cases/.

52. Kerr, *supra* note 51.

themselves to third parties in the course of carrying out mundane tasks."[53] "[I]t may be necessary," she wrote, "to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[54] Aspects of her concurrence were quoted or cited by Chief Justice Roberts in the majority opinions he authored in both *Riley v. California* and *Carpenter v. United States*.[55] Chief Justice Roberts is, at present, the swing vote when the Court divides on such data privacy cases as have come under consideration.

Last term's decision in *Carpenter* recognized that cell phones and their services constitute "'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[56] At issue was whether a person ceded all control over cell site location information ("CSLI") derived from his or her cell phone during the extended time of a string of robberies. The Court's bare majority, in an opinion written by Chief Justice Roberts, drew upon remarks in the Justice Sotomayor concurrence in *Jones* to "hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements."[57] A week of data was too much for the government to obtain without a warrant—although we do not know by how much.[58]

The decision left more questions unanswered than answered, and Justice Alito (in dissent) was probably right in asserting that the Court's reasoning "guarantees a blizzard of litigation."[59] Perhaps the *Carpenter* decision made Professor Cass Sunstein very happy: the Court was "muddling through" on relatively new terrain and seemed satisfied with a minimalist decision.[60] The majority opinion seemed, minimally, to carve out an exception to digital age third-party doctrine (or declined to *extend* the third-party doctrine to digital data of this sort) when locational data are collected automatically and comprehensively; the majority also did express concern about arbitrary police power. Left unanswered was the question of what kinds of data might be

53. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

54. *Id*.

55. Riley v. California, 573 U.S. 373, 396 (2014) (Roberts, C.J.); Carpenter v. United States, 138 S. Ct. 2206, 2215–18 (2018).

56. *Carpenter*, 138 S. Ct. at 2220 (quoting *Riley*, 573 U.S. at 385).

57. *Id*. at 2217; *see supra* note 39 and accompanying text (discussing Justice Sotomayor's concurrence in *Jones*).

58. *See Carpenter*, 138 S. Ct. at 2217 n.3 ("[W]e need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny.")

59. *Id*. at 2247 (Alito, J., dissenting).

60. CASS R. SUNSTEIN, ONE CASE AT A TIME: JUDICIAL MINIMALISM ON THE SUPREME COURT (1999); Charles E. Lindblom, *The Science of Muddling Through*, 19 PUB. ADMIN. REV. 78 (1959). I have joined these two texts in seminar discussions for years and subsequently discovered that Professor Keith Bybee did so in print in his review of *One Case at a Time, The Jurisprudence of Uncertainty*. *See* Keith J. Bybee, *The Jurisprudence of Uncertainty*, 35 LAW & SOC'Y REV. 943 (2001) (book review).

excepted from the third-party doctrine. The practice prior to *Carpenter*, under the Stored Communications Act, asked that federal or state government "offer[] specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[61]

In reading tea leaves for the future, however, perhaps the most interesting opinion in *Carpenter* was the dissent by Justice Gorsuch. Justice Gorsuch expressed his dislike for *Smith* and *Miller* and the reasonable expectation of privacy approach in *Katz*; he felt the majority opinion in *Carpenter* revised third-party doctrine, keeping *Smith* and *Miller* "on life support."[62]

> Deciding what privacy interests *should be* recognized often calls for a pure policy choice, many times between incommensurable goods—between the value of privacy in a particular setting and society's interest in combating crime. Answering questions like that calls for the exercise of raw political will belonging to legislatures, not the legal judgment proper to courts.[63]

Wanting to jettison the third-party doctrine and expressing great skepticism in reliance on personal judicial whim about what expectations of privacy were reasonable,[64] he therefore dissented. But in embracing what he called a more traditional approach to the Fourth Amendment, he envisioned a broader scope for Fourth Amendment rights. Justice Gorsuch argued that protections for your person, house, papers, and effects do not automatically disappear just because you share records with a third party.[65] It will be interesting to see whether he becomes a leader in shaping Court opinion about big data searches and privacy rights.

II. HAPPY TRAILS AND OTHER POINTS

I end with a few thoughts about five problems or issues I envision for the near future as we grow ever closer to our smart devices.

A. Reasonable Expectations of Privacy?

It seems that many Americans are willing to trade away privacy and information security in order to participate in this brave new world of smart devices and enjoy their conveniences. In *Katz*, Justice Harlan's concurrence introduced the language of "reasonable expectation of privacy," the measure

61. 18 U.S.C. § 2703(d) (2012).

62. *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting).

63. *Id*. at 2265.

64. *Id*.

65. *Id*. at 2270 (suggesting the use of technology, including storing data with third parties, may well be "functionally compelled by the demands of modern life").

of which seemed to be whether "the expectation be one that society is prepared to recognize as 'reasonable.'"[66] We must, of course, ask whether this standard, which has been often relied upon since *Katz*, is adequate (for reasons somewhat different from Justice Gorsuch's concerns, discussed above).[67] If Americans share all sorts of information with friends and strangers, caring less about privacy than they used to (what is it with Jeff Bezos, anyway? [68]), is *less* privacy the twenty-first century's "reasonable expectation of privacy?"[69] To be perversely Justice Scalia-like,[70] should the standard simply be contemporary community expectations if most of us become data exhibitionists? If we are indifferent to big data collection, does that make data trails "happy trails?"[71] That doesn't seem to be a good answer.

This characterization of privacy attitudes is, of course, too cavalier. The time it would take for an average internet user to read all the privacy policies of each website she or he visited in a year is staggering.[72] As one recent commentator notes, "To fully apprehend our vulnerabilities as digital creatures would require far too much time and energy. More than that: It would require an entirely new set of *instincts* . . . ."[73] Furthermore, so much information about most of us is already out there: "The monitoring of personal information is ubiquitous; its storage is so durable as to render one's past undeletable . . . ."[74] According to Professor Alessandro Acquisti, a scholar of privacy behavior and preferences, "There's a sense that the fight to protect your data is unwinnable."[75] Noting that the methodologies designed by Google and other corporate data collectors and marketers "are designed to keep us ignorant," Professor Zuboff argues that "[b]y now it's very difficult

66. Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

67. *See supra* notes 61–64 and accompanying text.

68. Ball, *supra* note 14 (discussing Jeff Bezos).

69. *Katz*, 389 U.S. at 360–61 (Harlan, J., concurring).

70. ANTONIN SCALIA, A MATTER OF INTERPRETATION 40–41, 145 (1997). Justice Scalia felt that if a later generation were to become brutish, a living constitution approach—one that accepted evolving standards of decency—would expect judges to substitute current understandings of the Eighth Amendment's cruel and unusual punishment clause for what those words would have been understood to encompass at the time of the founding. The text of the Constitution should instead be read to mean what people at the founding would have understood its words to have meant. *Id*.

71. Roy Rogers and Dale Evans sing the song concluding each episode of the *Roy Rogers Show*, which ran on television from 1951 to 1957. ROY ROGERS & DALE EVANS, HAPPY TRAILS (RCA Victor Records 1952).

72. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL'Y FOR INFO. SOC'Y 543, 543, 555 (2008) (arguing that the time to read privacy policies is itself a form of payment and calculating it takes eight to twelves minutes to read the average privacy policy on popular websites).

73. Jennifer Senior, *Our Neurotic 'Privacy Paradox,'* BDNEWS24.COM (May 20, 2019), https://opinion.bdnews24.com/2019/05/20/our-neurotic-privacy-paradox/ (emphasis added).

74. Acquisti et al., *supra* note 6, at 509.

75. Senior, *supra* note 73.

to participate effectively in society without interfacing with these same channels that are supply chains for surveillance capitalism's data flows."[76] For people concerned about personal privacy, the option of living a primitive, unconnected life in a cabin in the woods is not a particularly attractive alternative.

B. Corporations as Rights Defenders?

Corporations have become predictable defenders of First and Fourth Amendment freedoms for their manufactured creations and the data they collect. Amazon has argued that not only are the data collected by its smart speakers protected, but so are the responses the AI devices offer.[77] Are corporations and internet service providers going to become the most vigorous defenders of freedom of speech and freedom against unlawful searches as they seek to protect what they consider their property—or what they consider their customers' property, or, alternately, what privacy customers expect and rely upon when they purchase their products?[78] Would progress mean securing better First and Fourth Amendment protections in the name of *corporations* rather than necessarily for individuals?

One scholar contends that we are beginning to see "the creation of a new kind of speech *legally* and *constitutionally*."[79] Instead of a wall between individuals and the state, "ironically, in the new Information Society, preventing government from enacting speech-focused regulation means that powerful private interests will hold enormous power to shape how individuals interact with each other and perceive the world."[80] These are corporate digital intermediaries. Whose speech is to be protected by laws and courts in the digital age? There are commercial interests at stake, so is the speech that counts going to be the speech that is economically valuable?[81]

Consultants to corporations now prepare guidance on how to secure intellectual property rights in the Internet of Things and how to confront challenges corporations will face.[82] They offer advice and projections on patent

76. Laidler, *supra* note 13 (interviewing Professor Zuboff).

77. Sylvia Sui, State v. Bates*: Amazon Argues that the First Amendment Protects Its Alexa Voice Service*, JOLTDIGEST (Mar. 25, 2017), https://jolt.law.harvard.edu/digest/amazon-first-amendment.

78. Michael C. Pollack, *Taking Data*, 86 U. CHI. L. REV. 77 (2019).

79. Andrew Tutt, *The New Speech*, 41 HASTINGS CONST. L.Q. 235, 240 (2014).

80. *Id*. at 241.

81. *Id*. at 266, 273.

82. *See, e.g.*, *Internet of Things (IoT)*, FINNEGAN, https://www.finnegan.com/en/work/industries/internet-of-things-iot.html (last visited Sept. 27, 2019); *see also* Rob Bloom, *Protecting Your Intellectual Property in the Internet of Things*, IPWATCHDOG (Oct. 5, 2017), https://www.ipwatchdog.com/2017/10/05/protecting-intellectual-property-internet-of-things/id=88653/.

licensing activity.[83] Property rights in the Internet of Things are expanding for corporate innovators, but it is rather unclear—though ethically, morally, and legally important—whether there are any emerging, robust, countervailing rights to corporate ownership of personal data.[84]

C. The Idea of Personhood?

Entities other than persons (such as corporations) today have speech rights, so would matters be helped at all by trying to extend free speech or other rights against search and seizure to other artificial creations—to artificial intelligence? If citizens of the City of Toledo can grant legal personhood to algae-afflicted and beleaguered Lake Erie, could residents of a state grant personhood to a robot?[85] This idea has been raised chiefly in the context of what is known as "strong" or "hard" AI—devices that try to adapt and learn, and it involves the use of limited liability companies.[86] Doing so could invest AI devices that search databases with legal rights (and duties) so that their autonomy could be protected; the results of *their* searches, *their* privacy would be at issue—not that of their "owner."[87] If Alexa or Google Assistant owners have a paucity of rights, why would the device itself—even if smarter and more capable of learning in the future than it is today—fare better? Would the person who brought the device into the home reap any benefits of AI personhood, or would the point simply be to liberate the robot or device from its "master?"[88] Personhood for smart devices does not seem to be especially promising for the owner of a smart device, and would not, therefore, be likely to improve the rights of the citizen in the face of surveillance, search, or seizure.

---

83. LEXINNOVA, INTERNET OF THINGS: PATENT LANDSCAPE ANALYSIS, https://www.wipo.int/edocs/plrdocs/en/internet_of_things.pdf (last visited Sept. 27, 2019).

84. *See* Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423 (2018); *see also* Vaclav Janecek, *Ownership of Personal Data in the Internet of Things*, 34 COMPUTER L. & SECURITY REV. 1039 (2018) (discussing the issue in the European Union).

85. Sigal Samuel, *Lake Erie Now Has Legal Rights, Just Like You*, VOX, https://www.vox.com/future-perfect/2019/2/26/18241904/lake-erie-legal-rights-personhood-nature-environment-toledo-ohio, (last updated Feb. 26, 2019, 11:00 PM); *see* CHRISTOPHER D. STONE, SHOULD TREES HAVE STANDING? (1972) (discussing the origin of the idea to appoint guardians for nature).

86. Shawn J. Bayern, *The Implications of Modern Business-Entity Law for the Regulation of Autonomous Systems*, 19 STAN. TECH. L. REV. 93 (2015).

87. *See* Lawrence B. Solum, *Legal Personhood for Artificial Intelligence*, 70 N.C. L. REV. 1231 (1992) (raising the Thirteenth Amendment problem: Should AI seek emancipation?).

88. *Id*.

D. State-Level Protections?

Governor Jerry Brown signed the California Consumer Privacy Act of 2018 that should lead, by 2020, to new protections for citizens.[89] Consumers will be able to ask a business to "disclose the categories and specific pieces of personal information that it collects about the consumer," some information about the sources of the information gathered, and "categories of [third] parties with which the information is shared"; the consumer will be able to request that some personal information be deleted, can opt out of the selling of personal information, and more.[90] Are state-level measures such as this a promising avenue in new and enhanced protections of privacy and protections against search and seizure of data? It is uncertain how such measures will fare when challenged in federal courts. In *California v. Greenwood*,[91] the fact that California state law barred police from conducting warrantless trash searches was not relevant to the Supreme Court's finding that an individual had no reasonable expectation of privacy in garbage put out for collection by a third party; the evidence could be used in a narcotics conviction.[92] The *Greenwood* decision certainly casts some doubt on the robustness of state-level protections for data collected by Google Assistant, Alexa, or others in their family of devices—data that, coincidentally, crosses state lines and has commercial value. The Court in *Greenwood*, held:

> Individual States may surely construe their own constitutions as imposing more stringent constraints on police conduct than does the Federal Constitution. We have never intimated, however, that whether or not a search is reasonable within the meaning of the Fourth Amendment depends on the law of the particular State in which the search occurs.[93]

It is interesting to note that, in *Carpenter*, Justice Gorsuch took particular issue with the *Greenwood* decision, suggesting that his conception of privacy rights was more expansive than the Court found there.[94]

E. Self-Incrimination and Personal Assistant Devices?

There are looming Fifth Amendment self-incrimination issues involving cell phones and personal assistant devices. Many new personal assistant devices are designed to protect against intrusion by non-owners. Encryption

89. A.B. 375, 2017–18 Sess. (Cal. 2018), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

90. *Id*.

91. 486 U.S. 35 (1988).

92. *Id*. at 43–44.

93. *Id*. (White, J.) An amendment to the California Constitution eliminated the exclusionary rule for evidence seized in violation of state but not federal law.

94. Carpenter v. United States, 138 S. Ct. 2206, 2266 (2018) (Gorsuch, J., dissenting).

for some devices involves password or thumbprint protection; others use facial recognition technology. Courts have issued different rulings about whether individuals have ownership rights over their encrypted devices and data stored on their personal cell phones, computers, or other devices when law enforcement officials demand that these devices be unlocked.[95] Courts seem to be permitting law enforcement officials to use someone's biometric data to gain access to their data, though this issue has not come before the Supreme Court.[96] A password or a voice seem to be different—so far. It is not as obvious that law enforcement officials can demand that you enter your password in order to unlock data from your phone that they seek.[97]

Smart devices come to recognize the voice commands of their owners, presumably remaining silent when others attempt to demand stored information. Can people be *compelled* to speak to activate or demand information from their personal assistant, which might include past searches, calendar events, or e-mails? If there is a bright line at law between ownership of your voice, your password, your thumbprint, retina, or facial recognition, manufacturers of smart devices will have a market incentive to offer more law enforcement-proof means of logging in or securing information.[98] There is, however, the possibility of interesting case law developing on self-incrimination via compelled speech that activates a home smart device.

III. CONCLUSION

"[W]atched citizens are dominated by uncertainty, since they do not know where, when, about what and whom is watching over and collecting information about them . . . ."[99] My family willingly accepted a Google Assistant into our home, yet we admit to occasional moments of paranoia when we believe our assistant is learning things about us when we thought it was

95. *See* United States v. Fricosu, 841 F. Supp. 2d 1232 (D. Colo. 2012); United States v. Kirschner, 823 F. Supp. 2d 665 (E.D. Mich. 2010); Florida v. Stahl, 206 So. 3d 124 (Fla. 2016); Virginia v. Baust, 89 Va. Cir. 267 (2014) (holding that a passcode did not have to be supplied but a fingerprint did); *see also* Kate Patrick, *Judge Rules Police Can't Force You to Unlock Your Phone with Fingerprint*, INSIDESOURCES (Jan. 17, 2019), https://www.insidesources.com/judge-rules-police-cant-force-you-to-unlock-your-phone-with-fingerprint/.

96. Lily Hay Newman, *Why Cops Can Force You to Unlock Your Phone with Your Face*, WIRED (Oct. 1, 2018, 4:52 PM), https://www.wired.com/story/police-unlock-iphone-face-id-legal-rights/.

97. *See* Orrin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767 (2019); Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 FORDHAM L. REV. 203 (2018).

98. April Glaser, *The Next iOS Update Has a Feature to Prevent Cops from Searching Your iPhone*, SLATE (Aug. 18, 2017, 2:06 PM), https://slate.com/technology/2017/08/the-new-iphone-update-will-help-prevent-cops-from-searching-your-locked-device.html.

99. Maria João Simões & Nuno Amaral Jerónimo, *Rear Window—Transparent Citizens Versus Political Participation*, *in* THE POLITICS OF BIG DATA: BIG DATA, BIG BROTHER?, *supra* note 23, at 192 (citing DAVID LYON, THE ELECTRONIC EYE: THE RISE OF SURVEILLANCE SOCIETY (1994)).

sleeping. This is only a small part of the problem of big data, but self-surveillance is another frontier in the changing landscape of privacy, search and seizure, and property rights and law.

Perhaps we are headed into an Orwellian world.[100] Unaccountable power, both public and private, is enhanced by opacity of data collection and use.[101] Self-governance, the capacity of citizens to hold government accountable, to protect their autonomy, and their identity as rights-bearing individuals are all affected.[102] "The condition of privacy is dynamic . . . . Rights to privacy are rights to the sociotechnical conditions that make the condition of privacy possible."[103]

An Orwellian outcome is not inevitable. There is, at present, very little regulation of big data in the United States; "[s]pecific laws target specific concerns, but few systemic legal structures exist to police data collection or use. 'Big data law' does not exist yet."[104] The situation is frequently likened to the Wild West.[105] There is even less regulation of self-surveillance in the newer, developing Internet of Things, including lack of privacy protections.[106] Good federal statutes could help, and, as Justice Gorsuch suggests, at least some members of the Court would welcome such legislative judgments.[107] A major regulatory step recently occurred in Europe with the implementation of the European Union General Data Protection Regulation in May 2018.[108] In the United States, it will require persistent public pressure

100. GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949). Orwell, an English novelist and journalist, created a dystopian surveillance state called Oceana, making use of telescreens and reminding inhabitants that "Big Brother is watching you." *Id*. at 5. For a good seventieth anniversary essay, see Louis Menand, *"1984" at Seventy: Why We Still Read Orwell's Book of Prophecy*, NEW YORKER (June 8, 2019), https://www.newyorker.com/news/daily-comment/1984-at-seventy-why-we-still-read-orwells-book-of-prophecy.

101. Julie E. Cohen, *Surveillance Versus Privacy: Effects and Implications*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW, *supra* note 5, at 458.

102. *Id*. at 464–65.

103. *Id*. at 458.

104. Ferguson, *supra* note 24, at 171.

105. *See* Georg Matthes, *EU Data Protection: End of the Digital Wild West*, DEUTSCHE WELLE (May 25, 2018), https://www.dw.com/en/eu-data-protection-end-of-the-digital-wild-west/a-43935002; Cathy O'Neil, Opinion, *How America Can Stop Being the Wild West of Data*, BLOOMBERG (Aug. 5, 2018, 9:00 AM), https://www.bloomberg.com/opinion/articles/2018-08-05/how-america-can-stop-being-the-wild-west-of-data;Level, *The Wild West of IoT: Regulating Unchartered Territory*, NE. UNIV. LEVEL BLOG (April 11, 2018), https://www.northeastern.edu/levelblog/2018/04/11/wild-west-iot-regulating-uncharted-territory/.

106. *See also* Friedland, *supra* note 5, at 200, 215.

107. Carpenter v. United States, 138 S. Ct. 2206 at 2265, 2267, 2270 (2018) (Gorsuch, J., dissenting).

108. The EU General Data Protection Regulation was enacted in 2016 and went into effect May 25, 2018. *The General Data Protection Regulation Applies in All Member States from 25 May 2018*, EUR-LEX (May 24, 2018), https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html.

to achieve progress. Professor Zuboff, who calls "for a rebirth of astonishment and outrage," notes that substantial majorities of survey participants in surveys conducted between 2008 and 2017 "support measures for enhanced privacy and user control over personal data."[109]

As I have argued, the meaning of privacy, search and seizure, and property are in flux in this environment of big data. If the Supreme Court were to insist that only it, and not Congress, can define these constitutional values,[110] American citizens may be in for a great deal of trouble. But in working to redefine these values as technology changes, citizens, activists, and legal scholars may be able to push toward a better resolution.

109. ZUBOFF, SURVEILLANCE CAPITALISM, *supra* note 11, at 340 (reporting this finding in forty-six of forty-eight major surveys in this period).

110. *See* City of Boerne v. Flores, 521 U.S. 507 (1997) (describing the effect of judicial supremacy on legislation designed to further equal protection); *see also* Stephen M. Griffin, *Judicial Supremacy and Equal Protection in a Democracy of Rights*, 4 J. CONST. L. 281 (2002); Michael W. McConnell, *Institutions and Interpretation: A Critique of City of Boerne v. Flores*, 111 HARV. L. REV. 153 (1997).