EXPOSED

McKay Cunningham[*]

2019 MICH ST. L. REV. 375

INTRODUCTION

Perhaps by now it's all academic. Several commentators insist that we don't know it yet, but technology irrevocably gutted any normative semblance of privacy.[1] Indeed, history provides no analogue to the Information Age; never before has so much data been so easily accessible by so many. At 4.1 billion people, over half the

* Associate Professor, Concordia University School of Law.

1. *See, e.g.*, Ira Bloom, *Freedom of Information Laws in the Digital Age: The Death Knell of Informational Privacy*, 12 RICH. J.L. & TECH. 1, 9 (2006) (claiming that "the privacy protective consequences of practical obscurity have been obliterated because [of] the extensive use and availability of information in electronic, digital databases"); James P. Nehf, *Recognizing the Societal Value in Informational Privacy*, 78 WASH. L. REV. 1, 67 (2003) (noting that "[s]o much information about us is already in government and private sector databases that it may be too late to rethink our approach to information privacy protection"); David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069, 1085 (2014) (noting academic concern that privacy is dead).

world's population use the Internet.[2] Two-thirds of the world's 7.6 billion inhabitants have a mobile phone.[3] The world's digital content reduced to a stack of books would tower from Earth to Pluto ten times.[4]

With all of this readily accessible information, how can private, personal information remain private and personal? This Article posits that under current legal protocols, it can't. Data brokers already house voluminous files on almost every consumer, and data collection increases by orders of magnitude. As detailed in Part I, everyday objects, outfitted with sensors and connected to the Internet, capture and record data exhaust.[5] The Internet of Things monitors and transmits seemingly innocuous information generated simply by living, by moving from one place to another. Whether at home, in transit, or at work, the magnificent, the mundane, and the miniscule are all recorded.[6]

In isolation, pervasive data collection arguably poses small privacy risk. If data points are disperse and unconnected, anonymity is plausible. But industry players in social media, Internet services, and ecommerce are large and sophisticated. They have long recognized the monetary benefit inherent in consumer information. The ongoing collection of consumer data by these entities, however, is arguably muted by the services they offer. Data collection, the argument goes, improves the services rendered.

Data brokers, by contrast, more plainly reveal the magnitude of privacy risk. Part II details the rise of the data broker industry, its shrouded and profitable nature, and the largely unregulated landscape

---

2. Simon Kemp, *Digital in 2018: World's Internet Users Pass the 4 Billion Mark*, WE ARE SOCIAL BLOG (Jan. 30, 2018), https://wearesocial.com/blog/2018/01/global-digital-report-2018 [https://perma.cc/BDA4-VC8R] (indicating that nearly a quarter of a billion new users came online for the first time in 2017).

3. *Id.*

4. *See* Richard Wray, *Internet Data Heads for 500bn Gigabytes*, GUARDIAN (May 18, 2009), http://www.guardian.co.uk/business/2009/may/18/digital-content-expansion [https://perma.cc/8XLP-ZABN]; *see also* Kiley M. Belliveau, Leigh Ellen Gray & Rebecca J. Wilson, *Busting the Black Box: Big Data Employment and Privacy*, 84 DEF. COUNS. J. 1, 4 (2017) ("[F]or as much data as people create—for example, an average of 500 million photos per day and over 200 hours of video per minute shared in 2014—that volume is nothing compared with the amount of digital information created *about* them each day.").

5. *See infra* Part I.

6. *See, e.g.*, Dave Evans, *The Internet of Things: How the Next Evolution of the Internet is Changing Everything*, CISCO, Apr. 2011, at 2 (defining the Internet of Things as "the point in time when more 'things or objects' [are] connected to the Internet than people").

in which it operates.[7] The privacy harms implicit in the collection and categorization of voluminous files on almost every user, while latent, are severe. Very little protects users from complete exposure, as data brokers can sell sensitive, stereotyped, and comprehensive personal information without accountability.

Legal regulations, both in the U.S. and the E.U., have proved ineffectual. Part III reveals how these laws emerged by accretion.[8] They built upon previous legal constructs that predated the Internet, the Internet of Things, and the borderless flow of data in the digital age. They rely largely on providing notice and consent and fail to account for data collection that occurs without the possibility of notice and consent. They ignore the porous architecture of the web, which allows "protected" data to be captured when published by a host of unrestricted sources.

Into this void, many, from government officials, to free-market proponents, to legal scholars, have offered solutions. Part IV reviews a panoply of regulatory fixes and finds them wanting.[9] The diffuse and borderless nature of digital data requires a regulatory scheme fundamentally different from these proposals. Part V argues that the risk of ubiquitous exposure is a societal risk, not an individual one.[10] Injuries stemming from collection and misuse of personal data, if characterized as societal rather than individual, prompt legal reform distinct from the current regime and from the proposals posited by government officials, experts, and academics.

Societal harms, like environmental or healthcare harms, warrant proscriptive government involvement that emphasizes prevention over post-injury punishment. To forestall societal harms, government agencies prescribe regulatory norms, supervise their implementation, audit industry players, investigate potential infractions, and prosecute violators. The Article proposes a federal agency tasked with data privacy protection and bounded by risk of harm. Before promulgating a regulation, the agency must first identify the likelihood of the privacy risk in conjunction with the gravity of the harm balanced against the benefit to society absent regulation.

Given the enormity of readily accessible personal information and the ever-increasing sources from which the information can be

7. *See infra* Part II.
8. *See infra* Part III.
9. *See infra* Part IV.
10. *See infra* Part V.

harvested, data privacy is no longer an individual risk; it is a societal one. It merits societal protection. Otherwise, we are all exposed.

I. THE UBIQUITY OF DATA COLLECTION

Facebook users have uploaded well over 250 billion photographs to the site.[11] Google processes and records over 40,000 search queries every second.[12] The first YouTube video was uploaded in April 2005; today, 300 hours of video are uploaded to YouTube every minute.[13] More than 3 billion people use social media each month,[14] with the average Internet user spending around 6 hours each day—roughly one-third of his or her waking life—using Internet-powered devices and services.[15] Applied to 4.1 billion Internet users, humanity is projected to spend 1 billion years online in 2018.[16] The amount of readily accessible personal information is overwhelming.

A lot of personal information is voluntarily disseminated. Take for example a user who uploads a photograph of a birthday celebration to social media. The user intends a singular purpose—to communicate the event to specific other users. If that were the only use of the information, it would be difficult to call it private due to its voluntary relinquishment. But the information is not quarantined to a singular use; instead it is often categorized, copied, sold, and used in ways not anticipated by the user.[17]

---

11. Natasha Kohne & Kamran Salour, *Biometric Privacy Litigation: Is Unique Personally Identifying Information Obtained from A Photograph Biometric Information?*, 25 COMPETITION: J. ANTITRUST, UCL & PRIVACY SECTION ST. B. CAL. 150, 150 (2016).

12. Harsh, *How Much Data Does Google Handle??*, WP FORMERS (June 4, 2017), https://www.wpformers.com/google-datacenter-capacity/ [https://perma.cc/PA6C-UWBT].

13. *37 Mind Blowing YouTube Facts, Figures and Statistics – 2019*, MERCHDOPE (Jan. 5, 2019), https://merchdope.com/youtube-statistics/ [https://perma.cc/RWX3-RKZV].

14. *15 Best Vlogging Cameras for YouTube 2018*, MERCHDOPE (July 30, 2018), https://merchdope.com/youtube-statistics/ [https://perma.cc/Z6ZE-ACV5].

15. *See* Saima Salin, *More Than Six Hours of Our Day is Spent Online – Digital 2019 Reports*, DIG. INFO. WORLD (Feb. 4, 2019), https://www.digitalinformationworld.com/2019/02/internet-users-spend-more-than-a-quarter-of-their-lives-online.html [https://perma.cc/N3DE-LSQ2].

16. *Internet Stats & Facts for 2019*, HOSTING FACTS (Dec. 17, 2018), https://hostingfacts.com/internet-facts-stats/ [https://perma.cc/9XEM-44ZJ].

17. *See, e.g.*, Samantha L. Miller, *The Facebook Frontier: Responding to the Changing Face of Privacy on the Internet*, 97 KY. L.J. 541, 541 (2008–2009) (describing a Facebook user who was blackmailed using pictures she uploaded and thought were "private").

If maintaining privacy over voluntarily divulged content is difficult, achieving meaningful privacy over content collected without user awareness approaches the impossible. Just by moving from one place to another, we exude data exhaust.[18] Everyday items equipped with sensors collect our data without our knowing it.[19] These previously inert objects are proliferating, with over 220 billion worldwide expected by 2020.[20] In a world where "pretty much everything you can imagine will wake up," keeping our privacy is more unlikely than ever.[21] Even in the infancy of the Internet of Things, "passive" data is being collected at home, in transit, at play, and at work.[22]

A. The Internet of Things at Home

At home, the Internet of Things increasingly harvests passively generated data.[23] Users control the interior and exterior functions of the home through apps and devices communicating with Internet-equipped objects.[24] The washing machine, outfitted with sensors connected to the Internet, alerts the user that the spin cycle is over and that more detergent is required.[25] The thermostat monitors when the home is occupied to ensure proper air conditioning.[26]

18. *See, e.g.*, Jane Yakowitz Bambauer, *The New Intrusion*, 88 NOTRE DAME L. REV. 205, 207–08 (2012).

19. *See id.* (noting the "mind-boggling quantities of personal data" that are "collected every time we use our iPhones, tablets, and other gadgets" and that "companies have increasing access to our data exhaust—data detailing what we have looked at, where we have been").

20. Melissa W. Bailey, *Seduction by Technology*: *Why Consumers Opt Out of Privacy by Buying into the Internet of Things*, 94 TEX. L. REV. 1023, 1028 (2016). Others expect that number to increase to trillions within the next decade. *See* FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 1 (2015).

21. *What Is the Internet of Everything?*, CISCO, https://www.cisco.com/c/m/en_za/tomorrow-starts-here/ioe.html [https://perma.cc/7LHK-M4LM] (last visited May 24, 2019).

22. *See* FED. TRADE COMM'N, *supra* note 20, at 14 (noting that 10,000 homes using the Internet of Things "generate 150 million discrete data points a day or approximately one data point every six seconds for each household").

23. *See id.*

24. *See id.* at 1–2.

25. *See* Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 436 (2018).

26. *See* Marcus Wohlsen, *What Google Really Gets Out of Buying Nest for $3.2 Billion*, WIRED (Jan. 14, 2014, 6:30 AM), https://www.wired.com/2014/01/

Algorithms continually process home occupancy data to predict future occupancy.[27] Often the predictive function is not based on a single home but leverages occupancy patterns of thousands of users with the same thermostat technology.[28]

Manufacturers engraft sensors into lightbulbs,[29] toothbrushes,[30] doorbells,[31] garage doors,[32] sprinkler systems,[33] and slow-cookers[34]—most of which monitor, collect, and transmit the occupant's data exhaust.[35] Onesies and crib sheets collect and transmit data about infant movement, sleeping patterns, and skin temperature.[36] Pill bottles uploaded with daily dosage regimens notify users when to take prescribed medication.[37] Toothbrushes transmit brushing behavior to

---

googles-3-billion-nest-buy-finally-make-internet-things-real-us/ [https://perma.cc/4JH9-9CCF].

27. *See id.* (discussing how, as the devices talk to each other, they construct an aggregate picture of human behavior and predict or anticipate what users want before they know it).

28. *See id.* ("Over time, as the Nest Learning Thermostat uses its sensors to train itself according to your comings and goings, the entire network of Nests in homes across the country becomes smarter.").

29. *See* Richard M. Martinez, *The Internet of Things*: *Privacy Issues in a Connected World Remarks Given at Protecting Virtual You*: *Individual and Informational Privacy in the Age of Big Data*, 11 U. ST. THOMAS J. L. & PUB. POL'Y 63, 63 (2017).

30. *See* Tim Clark, *At Mobile World Congress, A Connected Future Becomes Reality*, FORBES (Feb. 27, 2004, 3:28 AM), https://www.forbes.com/sites/sap/2014/02/27/at-mobile-world-congress-a-connected-future-becomes-reality/#6117169289fc [https://perma.cc/CYW2-5DHF].

31. *See* Kathryn McMahon, *Tell the Smart House to Mind Its Own Business!: Maintaining Privacy and Security in the Era of Smart Devices*, 86 FORDHAM L. REV. 2511, 2518 (2018).

32. *See* Terrell McSweeny, Comm'r, Fed. Trade Comm'n, Remarks at TecNation 2016 (Sept. 20, 2016) (transcript available at https://www.ftc.gov/system/files/documents/public_statements/985773/mcsweeny_-_tecnation_2016_9-20-16.pdf [https://perma.cc/P3V5-QPUX]).

33. *See* Andrew Gebhart, *6 Reasons You Need a Smart Sprinkler*, CNET (July 11, 2018, 5:00 AM), https://www.cnet.com/news/6-reasons-you-need-a-smart-sprinkler/ [https://perma.cc/E86N-NGMB].

34. *See* Robert L. Mitchell, *The Internet of Things at Home: 14 Smart Products that Could Change Your Life*, COMPUTERWORLD (June 30, 2014, 6:30 AM), http://www.computerworld.com/article/2474727/consumerization-of-it/consumerization-150407-the-internet-of-things.html [https://perma.cc/VR2N-4LD6].

35. *See* McMahon, *supra* note 31, at 2518.

36. *See* Meg Leta Jones, *Privacy Without Screens & the Internet of Other People's Things*, 51 IDAHO L. REV. 639, 642–43 (2015).

37. DAVID ROSE, ENCHANTED OBJECTS: DESIGN, HUMAN DESIRE, AND THE INTERNET OF THINGS 8–9 (2014).

the user's dentist.[38] Several companies sell processing hubs that amalgamate diverse home sensors into a central locus.[39]

The amount of data collected by previously inert household objects raises sensitive questions unaddressed by the law. Who owns the data? The data exhaust generated in the home, especially when combined with other data gathered from the Internet, transforms a smart home into a glass home. As one commentator notes:

> The problem we currently face is thus not merely that a vast amount of information is resting in databases, but that we have very little control over that information—how it is used, shared, and manipulated—once it is "out there." We are at the mercy of those who hold our data.[40]

Data from the thermostat alone reveals when the user has been away from the home historically and when the user likely will be away from home in the future.[41] From medical needs to sleeping patterns and television use, sensors in the home track and record granular details of the occupant's life.[42] More often than not, the data is not held, and therefore not controlled, by the user; it is controlled by the entity that captured it.[43]

Companies that manufacture Internet-enabled washing machines, thermostats, and baby monitors scrutinize the data generated by their products.[44] Analyzing user behavior can lead to

---

38. *See* Clark, *supra* note 30.

39. *See* Stacy-Ann Elvy, *Hybrid Transactions and the Internet of Things: Goods, Services, or Software?*, 74 WASH. & LEE L. REV. 77, 84 (2017) (discussing the detriments attending smart home hubs).

40. Nehf, *supra* note 1, at 3.

41. Wohlsen, *supra* note 26; Elvy, *Hybrid Transactions*, *supra* note 39, at 96–97.

42. FED. TRADE COMM'N, *supra* note 20, at 11 ("If smart televisions or other devices store sensitive financial account information, passwords, and other types of information, unauthorized persons could exploit vulnerabilities to facilitate identity theft or fraud.").

43. Elvy, *Commodifying Consumer Data*, *supra* note 25, at 440 ("Privacy policies routinely authorize companies to disclose, sell, and transfer consumer data to third parties.").

44. *See* Paige Leuschner, *Are We There Yet? Current State of the Smart Home Market*, EURACTIV (Nov. 21, 2017), https://www.euractiv.com/section/energy/opinion/are-we-there-yet-current-state-of-the-smart-home-market/ [https://perma.cc/CUY7-9EE3]. Smart-home solutions provide the framework that enables companies to learn more about their customers, which means they can sell more services more effectively, retain more customers, and ultimately generate more revenue in an increasingly challenging and competitive business climate. *See id.*

product improvement.[45] But the original reason for collecting such data does not define its value.[46] In light of current data processing technologies, once the data has been collected and stored, it can be used for a variety of purposes unconnected to the original purpose associated with its collection.[47] As a result, companies often transfer the data to third parties.[48]

Granular data captured by household objects is not only valuable; it is also vulnerable.[49] Manufacturers of Internet-enabled objects overproduce the software that enables data collection and underproduce the safety mechanisms required to protect it.[50] The primary goal of enabling a pill bottle to connect with the Internet in order to dispense medication overshadows the secondary concern of securing sensitive data from unauthorized access.[51] Often the device itself, like a sensor grafted to a toothbrush, is so small that the hardware required to secure the data appears cost prohibitive.[52]

---

45. *See id.* For example, British Gas is using the data it collects from devices deployed in the home to populate its MyEnergy app with personalized energy consumption information. *See id.*

46. *See* Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 711 (1987).

47. *See* Leuschner, *supra* note 44.

48. *See* Natasha Singer & Jeremy B. Merrill, *When a Company is Put Up for Sale, in Many Cases, Your Personal Data Is, Too*, N.Y. TIMES (June 28, 2015), https://www.nytimes.com/2015/06/29/technology/when-a-company-goes-up-for-sale-in-many-cases-so-does-your-personal-data.html [https://perma.cc/7GKU-QQRF] (reporting that privacy policies in 85 of the "top 100 websites in the United States" had "terms of service or privacy policies" that authorize the sale of consumer data in the event of "a merger, acquisition, bankruptcy, asset sale or other [business] transaction").

49. *See* FED. TRADE COMM'N, *supra* note 20, at 11 (noting that "as consumers install more smart devices in their homes, they may increase the number of vulnerabilities an intruder could use to compromise personal information").

50. *See* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 134 (2014) (noting Internet-enabled products "are often manufactured by traditional consumer-goods makers rather than computer hardware or software firms").

51. *See* Brian Fung, *Here's the Scariest Part About the Internet of Things*, WASH. POST (Nov. 19, 2013), https://www.washingtonpost.com/blogs/the-switch/wp/2013/11/19/heres-the-scariest-part-about-the-internet-of-things/ [https://perma.cc/9ME3-2CAE] ("Although the folks who make dishwashers may be fantastic engineers, or even great computer programmers, it doesn't necessarily imply they're equipped to protect Internet users from the outset.").

52. *See* Brian Krebs, *The Lingering Mess from Default Insecurity*, KREBS ON SECURITY (Nov. 12, 2015), https://krebsonsecurity.com/2015/11/the-lingering-mess-from-default-insecurity/ [https://perma.cc/UY39-AX3P] ("As the Internet of Things

Moreover, connected devices frequently communicate among several devices in a consumer's home.[53] As a result, "the least secure device becomes the security level for all [of a consumer's] devices."[54]

These vulnerabilities are now manifesting.[55] In one case, activation of Internet-enabled lightbulbs required access to the user's Web ID and network passwords.[56] To allow easy installment of multiple lightbulbs, the passwords were automatically shared when a new lightbulb was activated, allowing hackers to access the passwords by pretending to be a lightbulb.[57] In another instance, a smart kettle leaked data to a random server in Iceland.[58] In 2015, researchers revealed that an Internet-enabled Barbie doll automatically connected to unsecured WiFi networks, allowing unknown parties to communicate directly with the unsuspecting child.[59]

Of course the connected home is more than just household objects outfitted with sensors.[60] Smart electrical meters are replacing stand-alone meters, for example.[61] Smart meters monitor and

---

grows, we can scarcely afford a massive glut of things that are insecure-by-design. One reason is that this stuff has far too long a half-life, and it will remain in our Internet's land and streams for many years to come . . . . Mass-deployed, insecure-by-default devices are difficult and expensive to clean up and/or harden for security, and the costs of that vulnerability are felt across the Internet and around the globe.").

53. *See* Sarah Kellogg, *Every Breath You Take: Data Privacy and Your Wearable Fitness Device*, 72 J. MO. B. 76, 78 (2016).

54. *Id.*

55. *See, e.g.*, Stuart Nathan, *Safer Connections: Reducing the Security Risks of the Internet of Things*, ENGINEER (May 14, 2018), https://www.theengineer.co.uk/iot-security-risks/ [https://perma.cc/9S89-9BVS].

56. *See id.*

57. *See id.*

58. *See id.*

59. *See* Rebecca Smithers, *Strangers Can Talk to Your Child Through "Connected" Toys, Investigation Finds*, THE GUARDIAN (Nov. 14, 2017, 3:46 AM), https://www.theguardian.com/technology/2017/nov/14/retailers-urged-to-withdraw-toys-that-allow-hackers-to-talk-to-children [https://perma.cc/ND2S-HZJG].

60. *See* Leuschner, *supra* note 44. For the most part, today's smart homes consist of individual connected devices with "interoperability issues, including a lack of communication between devices due to numerous communicating technologies, standards, and protocols." *Id.* The smart home of the near future will "act intuitively and automatically, anticipating and responding" to the occupants' needs based on "learned lifestyle patterns and real-time interaction." *Id.*

61. *See Nearly Half of All U.S. Electricity Customers Have Smart Meters*, U.S. ENERGY INFO. ADMIN. (Dec. 6, 2017), https://www.eia.gov/todayinenergy/detail.php?id=34012 [https://perma.cc/S3XJ-3UMN] ("Installations of smart meters have more than doubled since 2010—almost half of all U.S. electricity customer accounts now have smart meters. By the end of 2016, U.S. electric utilities had

immediately transmit electrical use, obviating the need to hire utility employees to periodically check stand-alone meters.[62] While more efficient and more precise, smart meters record much more than that needed for billing.[63] They gather fine-grain data.[64] Electrical devices have unique signatures such that metering can "distinguish the microwave from the refrigerator, or even the light bulb in the bathroom from the light bulb in the dining room."[65]

In 2014, the White House released a report detailing its privacy concerns and noting that smart meters "show when you move about your house."[66] Others have been more direct, showing that data from smart meters can reveal the occupant's relative wealth, cleanliness, and medical health, in addition to when the occupant is home, cooking, showering, and watching television.[67] One study identified the exact television show being watched solely from the home's electrical signal.[68] These demonstrations suggest that occupants of homes connected to smart meters unwittingly divulge a consistent stream of

installed about 71 million advanced metering infrastructure (AMI) smart meters, covering 47% of the 150 million electricity customers in the United States.").

62. *See* Sonia K. McNeil, *Privacy and the Modern Grid*, 25 HARV. J.L. & TECH. 199, 211 (2011).

63. *See* Matt Liebowitz, *Smart Electricity Meters Can Be Used to Spy on Private Homes*, NBC NEWS (Jan. 10, 2012, 4:03 PM), http://www.nbcnews.com/id/45946984/ns/technology_and_science-security/t/smart-electricity-meters-can-be-used-spy-private-homes [https://perma.cc/6PBU-RJGN].

64. *See id.*; *see also* Lorraine Bailey, *Seventh Circuit Hears Privacy Case Over Smart Meters*, COURTHOUSE NEWS SERV. (Mar. 27, 2018), https://www.courthousenews.com/seventh-circuit-hears-privacy-case-over-smart-meters/ [https://perma.cc/U26F-L6HJ] (claiming that city government violates the Fourth Amendment by granular electric data collection through smart meters, which allows "the city to determine when a resident is using their oven or electric water kettle").

65. Patrick Thibodeau, *The Internet of Things Could Encroach on Personal Privacy*, COMPUTERWORLD (May 3, 2014), https://www.computerworld.com/article/2488949/the-internet-of-things-could-encroach-on-personal-privacy.html [https://perma.cc/A39S-R7DA].

66. EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 53–54 (2014).

67. *See* Liebowitz, *supra* note 63.

68. *See* MIRO ENEV ET AL., INFERRING TV CONTENT FROM ELECTRICAL NOISE 1 (2010); *see also* Chester Wisniewski, *Smart Meter Hacking Can Disclose Which TV Shows and Movies You Watch*, NAKED SECURITY (Jan. 8, 2012), https://nakedsecurity.sophos.com/2012/01/08/28c3-smart-meter-hacking-can-disclose-which-tv-shows-and-movies-you-watch/ [https://perma.cc/L4P3-6R99].

detailed personal information, the after-collection uses of which are largely unregulated.[69]

Digital assistants, like Amazon's Alexa, collect even more data from within the home. Amazon and Google, the leading sellers of such devices, say the digital assistants record and process audio only after users trigger them by pushing a button or uttering a phrase like "Hey, Alexa" or "Okay, Google."[70] This is not always true, as one family's conversation was recorded without prompting and then sent to a random person in their contacts.[71] Assuming such instances are aberrations, both Google and Amazon still record and analyze every overt request a user makes.[72] Users can delete their history of Alexa requests, but the default setting records each query.[73] Amazon claims that the query history improves Alexa's responsiveness, which is certainly true, but the privacy policy Amazon offers enables the company to use the user's query history in other ways and to share it with third parties.[74]

Both Amazon and Google have sought patents for technology that would allow digital assistants to monitor more than discrete

---

69. *See* CAL. PUB. UTIL. COMM'N, PAC. GAS & ELEC. CO., AGENDA ID NO. 10870, PROPOSED DECISION OF COMM'R PEEVEY at 40 (2011) (establishing opt out procedures for smart meters).

70. *See* Dacia Green, *Big Brother is Listening to You: Digital Eavesdropping in the Advertising Industry*, 16 DUKE L. & TECH. REV. 352, 357 (2018).

71. *See* Hamza Shaban, *An Amazon Echo Recorded a Family's Conversation, Then Sent It to a Random Person in Their Contacts, Report Says*, WASH. POST (May 24, 2017), https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/an-amazon-echo-recorded-a-familys-conversation-then-sent-it-to-a-random-person-in-their-contacts-report-says/?noredirect=on&utm_term=.bf4f5c44baa4 [https://perma.cc/7K5B-2EB4].

72. *See* Jing Cao & Dina Bass, *Why Google, Microsoft and Amazon Love the Sound of Your Voice*, BLOOMBERG (Dec. 13, 2016, 6:00 AM), https://www.bloomberg.com/news/articles/2016-12-13/why-google-microsoft-and-amazon-love-the-sound-of-your-voice [https://perma.cc/Q9LS-Y86Q]; *see also* Tim Moynihan, *Alexa and Google Home Record What You Say. But What Happens to That Data?*, WIRED (Dec. 5, 2016, 9:00 AM), https://www.wired.com/2016/12/alexa-and-google-record-your-voice/ [https://perma.cc/S4T7-ELDL].

73. *See* Moynihan, *supra* note 72.

74. *See Alexa Internet Privacy Notice*, ALEXA (2018), https://www.alexa.com/help/privacy [https://perma.cc/5T4K-U73M] ("As we continue to develop our business, we might sell or buy subsidiaries or business units. In such transactions, user information generally is one of the transferred business assets but remains subject to the promises made in any pre-existing privacy notice (unless, of course, the user consents otherwise). Also, in the event that Alexa or substantially all of its assets are acquired, user information will of course be one of the transferred assets.").

auditory queries.[75] One patent application includes "[a] system for deriving sentiments and behaviors from ambient speech, even when a user has not addressed the device with its 'wakeword.'"[76] The system would monitor audio from a collection of devices, like tablets and e-readers, listening for words like "love," "bought," or "dislike" and analyzing the conversation in real time.[77] One Google patent application states that voices could be used to determine a speaker's mood using the "volume of the user's voice, detected breathing rate, crying and so forth" and a speaker's medical condition "based on detected coughing, sneezing and so forth."[78]

As more household objects wake up, more data exhaust is recorded. Without a regulatory structure in place, the entities that capture the data control it.[79] Leveraging the "rich, accurate, and fine-grain" sensor data gathered by the Internet of Things, private companies, government agencies, and individuals can make powerful inferences about users' personalities and habits.[80] Through licensing and user agreements, some entities promise privacy generally while carving out exceptions for sale and transfer to third parties.[81] These issues associated with the Internet of Things are not relegated to the home, of course. Stepping from the home and heading to work exposes the user to a new landscape of monitoring through the Internet of Things.[82]

75. *See* AMAZON PATENT FILINGS REVEAL DIGITAL HOME ASSISTANT PRIVACY PROBLEMS, CONSUMER WATCHDOG 1 (2017).

76. *Id.* (emphasis omitted).

77. *Id.* at 6.

78. Sapna Maheshwari, *Hey, Alexa, What Can You Hear? And What Will You Do With It?*, N.Y. TIMES (Mar. 31, 2018), https://www.nytimes.com/2018/03/31/business/media/amazon-google-privacy-digital-assistants.html [https://perma.cc/ZEV5-FSY4].

79. *See* Elvy, *Commodifying Consumer Data*, *supra* note 25, at 440.

80. Alexander H. Tran, *The Internet of Things and Potential Remedies in Privacy Tort Law*, 50 COLUM. J.L. & SOC. PROBS. 263, 270 (2017).

81. *See* Elvy, *Commodifying Consumer Data*, *supra* note 25, at 439–46 (reviewing privacy policies that attend a range of Internet of Things devices and revealing that many policies expressly allow the company to sell or transfer consumer data in connection with a "business transition").

82. *See id.* at 439–46.

B. The Internet of Things in Transit

Once a symbol of individualism and escapism, the modern car now monitors almost everything that transpires within it.[83] Integrated systems record location, speed, acceleration, entertainment, occupant identity, contact lists, and much more.[84] With over 380 million "connected" cars by 2021, "[t]he market position of the car today is similar to where the smartphone was in 2010."[85]

Event Data Recorders, sometimes called "black boxes," log and retain particular driving data in most cars sold in the U.S. in the past twenty-five years.[86] Black boxes typically record only a sliver of driving data—that which immediately precedes a collision or sudden braking like speed, braking, and seatbelt use.[87] Although black boxes have been around for decades, Congress moved to protect black box data only recently in 2015 by restricting generalized access and guaranteeing that the data belongs to the owner or lessee of the vehicle.[88]

But the modern car contains much more than a black box.[89] Over 90% of cars sold by 2020 will have the capacity to connect to the Internet.[90] "Infotainment" systems record location data, location history, telephone calls, texts, navigational queries, and restaurant

83. *See* John R. Quain, *Cars Suck Up Data About You. Where Does It All Go?*, N.Y. TIMES (July 27, 2017), https://www.nytimes.com/2017/07/27/automobiles/wheels/car-data-tracking.html [https://perma.cc/Y3P4-YCSU].

84. *See id.*

85. John Greenough, *The Connected Car Report: Forecasts, Competing Technologies, and Leading Manufacturers*, BUS. INSIDER (June 10, 2016, 5:33 PM), http://www.businessinsider.com/connected-car-forecasts-top-manufacturers-leading-car-makers-2015-3 [https://perma.cc/WHN4-RZ6B].

86. *See* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., FINAL REGULATORY EVALUATION: EVENT DATA RECORDERS (EDRS), III-2 tbl.III-1 (2006) (estimating that 64.3% of new cars sold in 2004 came equipped with EDRs); *see also* Press Release, U.S. Dep't of Transp., U.S. DOT Proposes Broader Use of Event Data Recorders to Help Improve Vehicle Safety (Dec. 7, 2012), https://www.transportation.gov/briefing-room/us-dot-proposes-broader-use-event-data-recorders-help-improve-vehicle-safety [https://perma.cc/RCQ4-XKF6].

87. *See* 49 C.F.R. § 563.11(a) (2013) (requiring that EDRs store specific information for thirty seconds after a triggering impact).

88. *See* Driver Privacy Act, Pub. L. No. 114-94, 129 Stat. 1712 (2015).

89. *See* WORLD ECON. FORUM, DIGITAL TRANSFORMATION OF INDUSTRIES: AUTOMOTIVE INDUSTRY 9 (2016).

90. *Id.*

searches.[91] "Newer cars may record a driver's eye movements, the weight of people in the front seats and whether the driver's hands are on the wheel."[92] In addition, modern recordation of operational data far outpaces the black box pre-collision recordings.[93] Data about vehicle speed, direction, distances, time, fuel consumption, and tire pressure, among other recorded operations, transform the car into a constantly updated driving history.[94] The Government Accountability Office cited locational information as a privacy threat, noting that storing location data "create[s] a detailed profile of individual behavior, including habits, preferences, and routes traveled."[95] This data is valuable beyond vehicle maintenance. Already, startup companies are specializing in collecting and selling car data to third parties.[96]

Insurers promise lower premiums in exchange for driving data.[97] Progressive's Snapshot collects speed, time of day, miles driven, rates of acceleration, and braking, but not location.[98]Although Progressive's privacy policy states that the data will not be used to resolve insurance claims without consent, the public has been somewhat slow to embrace real-time insurance monitoring, a fact that prompted Progressive to launch new marketing approaches aimed at alleviating

91. *See* Quain, *supra* note 83. This leads to the collection of vast amounts of location information that exposes extensive private information on driver habits such as where a driver lives and works or where they go for entertainment. *See id.*

92. *Id.*

93. *See* Peppet, *supra* note 50, at 106 (noting that while a traditional EDR typically records and stores only a few seconds of data prior to a crash, modern diagnostics "track a vehicle's location or a driver's performance over time").

94. *See* Quain, *supra* note 83; *see also* Jamie Todd Rubin, *Testing Automatic Link, the FitBit for Your Car*, DAILY BEAST (July 8, 2014, 5:45 AM), http://www.thedailybeast.com/articles/2014/07/08/testing-automatic-link-the-fitbit-for-your-car.html [https://perma.cc/6CJD-EWLM].

95. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-14-649T, CONSUMERS' LOCATION DATA: COMPANIES TAKE STEPS TO PROTECT PRIVACY, BUT PRACTICES ARE INCONSISTENT, AND RISKS MAY NOT BE CLEAR TO CONSUMERS (2014).

96. *See, e.g.*, *Automotive Data in Motion*, OTONOMO, http://otonomo.io/about-us/ [https://perma.cc/94DK-AXEJ] (last visited May 24, 2019) (describing automotive data collection services).

97. *See* Quain, *supra* note 83 (stating that "insurance companies are experimenting with apps and dongles that record braking, acceleration and speed with the lure of lower rates for well-mannered drivers").

98. *See Snapshot® Privacy Statement*, PROGRESSIVE, https://www.progressive.com/support/legal/snapshot-privacy-statement/ [https://perma.cc/94DK-AXEJ] (last visited May 24, 2019).

consumer concern.[99] Rental cars also store large amounts of consumer information gathered from inside the car.[100] Dashboard cameras accompany one out of every eight Hertz cars, for example.[101] Notably, the cameras are "not outward-facing cameras monitoring the road, but inward-facing cameras capable of making audio and video recordings of everything inside the passenger compartment."[102]

Like the proliferation of technology in the home, the infusion of technology in the car generates new vulnerabilities. Researchers have been able to hack into and wrest control away from drivers of connected cars.[103] In one widely published experiment, researchers hacked into a car's software, enabling remote control using laptops.[104] The researchers cut the power steering, spoofed the GPS, and forced the speedometer to show false speeds, all outside the driver's control.[105] The researchers demonstrated the ability to jerk the steering wheel in either direction at any speed.[106] A follow-up study showed that researchers could penetrate the same critical systems by targeting the car's cellular connection, Bluetooth bugs, smartphone app, and a

---

99. *See Snapshot® Plug-In Device: Terms & Conditions*, PROGRESSIVE, http://www.progressive.com/auto/snapshot-terms-conditions/ [https://perma.cc/2LM5-GEA7] (last updated May 11, 2017).

100. *See Global Privacy Policy*, ENTERPRISE HOLDINGS, https://privacy.ehi.com/en-us/home/privacy-policy.html [https://perma.cc/MGA6-VFRB] (last updated May 7, 2018). Enterprise rental company collects (1) location information, (2) crash notification and related crash data, and (3) operational condition, mileage, diagnostic, and performance reporting of vehicles. *See id.* Its privacy policy claims that Enterprise is "not responsible for any data that is left in the vehicle" and that it "cannot guarantee the privacy or confidentiality of such information." *Id.*

101. *See* Jennifer Abel, *Hertz Putting Passenger-Compartment Cameras in Rental Cars*, CONSUMER AFFAIRS, https://www.consumeraffairs.com/news/hertz-putting-passenger-compartment-cameras-in-rental-cars-031815.html [https://perma.cc/7SKW-2K4Y] (last visited May 24, 2019).

102. *Id.*

103. *See* Charlie Miller & Chris Valasek, *Adventures in Automotive Networks and Control Units*, IOACTIVE, (2014); *see also* Steve Henn, *With Smarter Cars, the Doors Are Open to Hacking Dangers*, NPR (July 30, 2013, 3:48 AM), https://www.npr.org/sections/alltechconsidered/2013/07/30/206800198/Smarter-Cars-Open-New-Doors-To-Smarter-Thieves [https://perma.cc/JF5B-EFCV].

104. *See* Henn, *supra* note 103.

105. *See id.*

106. *See id.*; *see also* Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, WIRED (July 21, 2015, 6:00 AM), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [https://perma.cc/7EA9-WVWB]; Bruce Schneier, *Hackers Stealing Cars*, SCHNEIER ON SEC. BLOG (Aug. 11, 2016, 6:32 AM), https://www.schneier.com/blog/archives/2016/08/hackers_stealin.html [https://perma.cc/X5XR-SD4J].

malicious audio file on a CD in the car's stereo system.[107] Even a wireless tire pressure gauge was exploited, allowing access to the car's core functionality.[108]

If the route from home to work does not include a car, the Internet of Things nevertheless awaits. Consider the many photographic technologies that capture daily images from diverse vantages. Smartphones are by far the most prolific. By 2020, 6.1 billion people will have phones with picture-taking capabilities.[109] More than 2.5 trillion images are shared or stored on the Internet annually.[110] Surveillance cameras, as distinguished from smartphones, are also proliferating, with 106 million new surveillance cameras sold in one year.[111]

In Chicago, 30,000 government-operated closed-circuit cameras survey the public's coming and going.[112] To combat high murder rates, the police leverage these cameras, setting up surveillance centers within police stations that monitor the license plate of every passing vehicle, photographs of repeat offenders, gang boundaries, previous 911 reports, and more.[113] Officers can "commandeer the cameras to get a 360-degree view of the area."[114] The data not only allows police

---

107. *See* Andy Greenberg, *Hackers Reveal Nasty New Car Attacks—With Me Behind the Wheel (Video)*, FORBES (Aug. 12, 2013), https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/#55e72828228c [https://perma.cc/K2T8-HYHF].

108. *See* Nathan, *supra* note 55. *But see* FED. TRADE COMM'N, *supra* note 20, at 12 (noting that although a panelist was able "to hack into a car's built-in telematics unit and control the vehicle's engine[,]" he noted that "the risk to car owners today is incredibly small").

109. Andy Boxall, *The Number of Smartphone Users in the World is Expected to Reach a Giant 6.1 Billion by 2020*, DIGITAL TRENDS (June 3, 2015, 6:23 AM), https://www.digitaltrends.com/mobile/smartphone-users-number-6-1-billion-by-2020/ [https://perma.cc/SAQ4-JYT7].

110. *Predictions: Photo Sharing: Trillions and Rising*, DELOITTE, https://www2.deloitte.com/lk/en/pages/technology-media-and-telecommunications/articles/tmt-pred16-telecomm-photo-sharing-trillions-and-rising.html [https://perma.cc/EQ8K-WTGQ] ("Deloitte Global predicts that in 2016, 2.5 trillion photos will be shared or stored online.") (last visited May 24, 2019).

111. Terry Gross, *With Closed-Circuit TV, Satellites and Phones, Millions of Cameras Are Watching*, NPR (Feb. 8, 2018, 2:27 PM), https://www.npr.org/2018/02/08/584243140/with-closed-circuit-tv-satellites-and-phones-millions-of-cameras-are-watching [https://perma.cc/V7EU-STLD].

112. Timothy Williams, *Can 30,000 Cameras Help Solve Chicago's Crime Problem?*, N.Y. TIMES (May 26, 2018), https://www.nytimes.com/2018/05/26/us/chicago-police-surveillance.html [https://perma.cc/QL8V-NU43].

113. *See id.*

114. *Id.*

to respond more quickly, but it also provides the raw input for software that reputedly predicts future crime.[115]

Linked cameras like those in Chicago are proliferating in New York, Baltimore, and Houston.[116] Police in Louisville want to use drones when responding to gunshots, and facial recognition technology is being considered in large counties in Florida and Oregon.[117] Security cameras on privately owned homes and buildings further expand the photographic data captured during transit from home to work.[118]

More than three million ATMs photograph their customers.[119] Tens of thousands of cameras perched over roadways record license plates, vehicle speed, and location.[120] Body cameras are no longer relegated to police, as medical professionals and others don cameras to capture the entirety of the workday.[121] Cameras adorn car dashboards, cyclists' helmets, doorbells, entryways to stores, and places of public accommodation.[122] There are "billions of images of unsuspecting citizens captured by facial-recognition technology and stored in law enforcement and private-sector databases over which our control is practically nonexistent."[123]

Many, if not most, of these devices operate without the consent of the person photographed and often without that person's

115. *See id.*

116. *See id.*

117. *See id.*

118. *See* Walter Pincus, *Many Cameras, Little Privacy*, WASH. POST (Aug. 12, 2013), https://www.washingtonpost.com/world/national-security/many-cameras-little-privacy/2013/08/12/37462de8-01d1-11e3-9711-3708310f6f4d_story.html?noredirect=on&utm_term=.3069ec8a6b6b [https://perma.cc/3WEF-3CL3].

119. *Automated Teller Machines (ATMS) (Per 100,000 Adults)*, THE WORLD BANK, https://data.worldbank.org/indicator/FB.ATM.TOTL.P5?view=chart [https://perma.cc/KL48-BFDY] (last visited May 24, 2019).

120. *See* David Gray, *A Collective Right to Be Secure from Unreasonable Tracking*, 48 TEX. TECH. L. REV. 189, 197 (2015) (noting that "security cameras, license plate readers, and other imaging technologies increasingly monitor our public spaces").

121. *See* Peter Swire & Jesse Woo, *Privacy and Cybersecurity Lessons at the Intersection of the Internet of Things and Police Body-Worn Cameras*, 96 N.C. L. REV. 1475, 1482 (2018) ("Use of BWCs is beginning to migrate from the policing context into other sectors, including healthcare and education.").

122. *See* Robert Draper, *They Are Watching You—and Everything Else on the Planet*, NAT'L GEOGRAPHIC, https://www.nationalgeographic.com/magazine/2018/02/surveillance-watching-you/ [https://perma.cc/4DEB-FWL8] (last visited May 24, 2019).

123. *Id.*

knowledge.[124] That is certainly the case with more remote technologies like drones and satellites.[125] In 2016, American consumers and businesses purchased 2.5 million drones, a number that does not include government-operated drones.[126] Higher still in elevation, more than 1,700 satellites monitor the planet.[127] While many are operated by government entities, a private company, Planet, now operates more functioning satellites than the U.S. government.[128] With more than 200 in orbit, the company can image every parcel of land in the world every day.[129]

From the ground up, imaging technologies capture more and more data exhaust.[130] Starting with smartphones and moving up to rooftop cameras and drones, the monitoring capacity moves skyward to satellites orbiting 300 miles away.[131] Whether inside a connected car or walking down a city sidewalk, the privacy landscape outside the home continues to change.[132]

C. The Internet of Things at Work

Employers, too, collect and analyze data exhaust through the Internet of Things.[133] Indeed, the Internet of Things increasingly influences whether an employee is hired in the first place.[134] Large companies now consult data brokers before hiring key personnel.[135]

---

124. *See id.*
125. *See id.*
126. *Id.*
127. *Id.*
128. *See id.*
129. *See id.*
130. *See id.*
131. *See id.*
132. *See id.*
133. *See* Belliveau, *supra* note 4, at 8.
134. *See id.* ("Nontraditional employment data comes from sources other than the typical personnel data setting, such as 'operations and financial data systems maintained by the employer, public records, social media activity logs, sensors, geographic systems, internet browsing history, consumer data-tracking systems, mobile devices, and communications metadata systems.'") (quoting Dr. Kelly Trindel, Chief Analyst, Office of Research, Information, and Planning, EEOC, *in Big Data in the Workplace: Examining Implications for Equal Employment Opportunity Law*, EQUAL EMP'T OPPORTUNITY COMM'N (Oct. 13, 2016) (transcript found at https://www.eeoc.gov/eeoc/meetings/10-13-16/trindel.cfm [https://perma.cc/DNC8-SAGV])).
135. *See id.* at 7–8 ("A 2015 study of 279 members of the Society of Human Resources Management (SHRM) found that while 32% of Human Resources professionals reported that their organization already uses big data to support Human

Data brokers collect and sell a capacious array of information, including "browsing history, online purchases, and any information about you that's publicly available: property records, court cases, marital status, [and] social-media connections."[136]

One of the largest data brokers, Acxiom, curates an average of 1,500 pieces of information on more than 500 million consumers.[137] Some companies now specialize in scouring social media and other Internet sites for the sole purpose of providing information about job applicants.[138] A prospective employer would likely be interested in an applicant's mortgage balance, 2011 bankruptcy, and prescription for antidepressants, to say nothing of the applicant's work history and Internet browsing predilections.[139]

Once hired, the Internet of Things pervades the workplace. For a while now, employers have monitored and recorded an employee's use of work computers, including browsing history.[140] This line blurs, however, with more and more employees bringing their own devices to work.[141] These personal devices often include work-related content and often connect through the employer's server.[142]

Resources, 82% of organizations planned to either begin or increase their use of big data in Human Resources in the next three years."); *see also* EXEC. OFFICE OF THE PRESIDENT, *supra* note 66, at 52.

136. Caitlyn Renee Miller, *I Bought a Report on Everything That's Known About Me Online*, THE ATLANTIC (June 6, 2017), https://www.theatlantic.com/technology/archive/2017/06/online-data-brokers/529281/ [https://perma.cc/Q6FS-ZCJ6].

137. *See* Patrick Tucker, *Has Big Data Made Anonymity Impossible?*, MIT TECH. REV. (May 7, 2013), http://www.technologyreview.com/news/514351/has-big-data-made-anonymity-impossible [https://perma.cc/CZA5-ZRWX].

138. *See* Kashmir Hill, *Feds Okay Start-up That Monitors Employees' Internet and Social Media Footprints*, FORBES (June 15, 2011, 3:34 PM), https://www.forbes.com/sites/kashmirhill/2011/06/15/start-up-that-monitors-employees-internet-and-social-media-footprints-gets-gov-approval/#779500946411 [https://perma.cc/K97U-33C4] (discussing a company that scours social media sites to provide personal data about applicants to prospective employers).

139. *See* Brian Naylor, *Firms Are Buying, Sharing Your Online Info. What Can You Do About It?*, NPR (July 11, 2016, 4:51 PM), https://www.npr.org/sections/alltechconsidered/2016/07/11/485571291/firms-are-buying-sharing-your-online-info-what-can-you-do-about-it [https://perma.cc/A5LC-HRJ7] (identifying a wide range of data collected by data brokers and noting that data brokers commonly categorize and sell that data).

140. *See* Belliveau, *supra* note 4, at 8.

141. *See* Daniel P. Howley, *Should You Allow Personal Devices on the Company Network?*, Laptop Magazine (Oct. 18, 2011, 1:01 PM), https://www.laptopmag.com/articles/should-you-allow-personal-devices-on-the-company-network [https://perma.cc/9BJ8-JM45].

142. *See id.*

Employee badges are no longer limited to identification and building access.[143] They record and transmit when the employee arrives and leaves, often tracking the employee long after the workday ends.[144] Newer iterations of employee badges record audio as well, allowing employers to record everything that is said and to whom.[145] Tone of voice and rapidity of speech can affect an employer's evaluation of the employee's productivity.[146] One company leverages production software to encourage certain employees to speak with certain other employees.[147] Automated furnishings shift to encourage employee interactions that will lead to more efficient work product.[148] Employers also leverage data gleaned by the Internet of Things to track employee health.[149] Wellness initiatives seek to lower the cost of employer-provided healthcare by promoting healthy lifestyles.[150] Tracking devices like Fitbits have been integrated into wellness initiatives, transmitting personal health data to employers.[151] Such

143. *See* Ben Waber, *What Data Analytics Says About Gender Inequality in the Workplace*, BLOOMBERG (Jan. 30, 2014, 8:56 PM), https://www.bloomberg.com/news/articles/2014-01-30/gender-inequality-in-the-workplace-what-data-analytics-says [https://perma.cc/JX3E-2E94].

144. *See* Corey A. Ciocchetti, *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring*, 48 AM. BUS. L.J. 285, 334–45 (2011).

145. *See* Waber, *What Data Analytics Says*, *supra* note 143.

146. *See* Ellen Kandell, *Tone of Voice in the Workplace*, ALT. RESOLUTIONS LLC (Sept. 12, 2016), https://www.alternativeresolutions.net/2016/09/12/tone-of-voice-in-the-workplace/ [https://perma.cc/W4AX-5LUQ].

147. *See* Ben Waber, *Augmenting Social Reality in the Workplace*, MIT TECH. REV. (May 15, 2013), https://www.technologyreview.com/s/514371/augmenting-social-reality-in-the-workplace/ [https://perma.cc/SFT9-53SK].

148. *See id.*; *see also* Vicki Salemi, *Tracking Sensors in Workplace Present Productivity Data & Privacy Issues*, ADWEEK (Mar. 8, 2013), https://www.adweek.com/digital/tracking-sensors-in-workplace-present-productivity-data-privacy-issues/ [https://perma.cc/LF3J-FTME] (noting that researchers found that productivity surged at one company when workers ate at tables designed for twelve people instead of four and that when a bank call center moved to group breaks instead of individual ones productivity increased by ten percent).

149. *See The Best of 2015: 9 Companies That Nailed It*, FITBIT, http://content.fitbit.com/Best_Of_2015.html?promosrc=website [https://perma.cc/P5HT-UGJK] (last visited May 24, 2019).

150. *See id.*

151. *See Target Kicks Off New Team Member Wellness Initiatives*, TARGET (Sept. 16, 2015), https://corporate.target.com/article/2015/09/team-member-wellness [https://perma.cc/CKW6-NSEC].

programs carry the extra risk that employers monitor employee behavior even outside of work.[152]

In the workplace, the Internet of Things is not limited to robotics and factory floors that are increasingly devoid of humans. It is much more. It is a tool that provides ceaseless and multilayered surveillance of employees while simultaneously influencing employee behavior to increase productivity.[153] Whether at home, in transit, or at work, the Internet of Things collects our data exhaust. In many instances, permission to collect the data is not requested.[154] Indeed, we often have no idea it's happening.[155] This passively collected data can be extremely revealing, especially when combined with other personal information gleaned from other sources like social media and public records.[156] Data brokers do just that—compile large dossiers on most consumers.[157] The dossiers aggregate data for sale to any who would pay.[158]

II. DATA BROKERS AND AFTER-COLLECTION PRIVACY HARMS

A. Data Brokers: Shrouded, Growing, and Profitable

The data broker industry is relatively unknown to the public.[159] While data brokers incessantly seek consumer information, they

152. *See* NAT'L WORKRIGHTS INST., ON YOUR TRACKS: GPS TRACKING IN THE WORKPLACE 20, 22, https://epic.org/privacy/workplace/gps-traking.pdf [https://perma.cc/PFN2-VPVJ] (last visited May 24, 2019).

153. *See* Tran, *supra* note 80, at 273 (noting that companies may use analytics to interpret this sensor data and monitor employee productivity or efficiency, potentially violating an employee's expectations of privacy).

154. *See* Swire & Woo, *supra* note 121, at 1523; *see also* Peppet, *supra* note 50, at 140–41 (noting that because many connected devices lack a screen or other user interface, meaningful notice and consent is illusory).

155. *See* Peppet, *supra* note 50, at 141.

156. *See* Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1379 (2017) ("Companies are frequently using cross-device tracking—connecting the activities of users 'across [their] smartphones, tablets, desktop computers,' and IOT devices—to collect information about consumers.").

157. *See* PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., EXEC. OFFICE OF THE PRESIDENT, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 15–21 (2014).

158. *See id.*

159. *See generally* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014) [hereinafter FTC DATA BROKER REPORT].

subvert information about themselves.[160] One commentator characterized the multi-billion dollar industry as "invisible" and purposefully so.[161] In 2014, the Federal Trade Commission (FTC) removed a portion of the veil to show "how data brokers amass detailed profiles about consumers from an array of online and offline sources, largely without consumers' knowledge, and then sell those profiles to other data brokers and businesses."[162] The FTC ordered nine data brokers to divulge information about their data collection practices.[163] The orders requested information regarding "the nature and sources of consumer data they collect; how they use, maintain, and disseminate the data; and the extent to which the data brokers allow consumers to access and correct data about them or to opt out of having their personal information sold or shared."[164]

The FTC report surveyed nine data brokers, but thousands more collect, analyze, and sell consumer data in the United States.[165] A data broker is an entity "whose primary business is collecting personal information about consumers from a variety of sources and aggregating, analyzing, and sharing that information, or information derived from it."[166] Several variations of data brokers operate in the U.S.; some have a narrow or specific focus as to the data collected and the clients served, whereas others generally collect as much data as possible. Paramount Lists, for example, sells lists of those suffering from depression and other mental illnesses.[167] Another broker, Great Lakes List Management, sells lists of households where Alzheimer's patients reside, purportedly for use by "pharmaceutical compan[ies]

160. *See* Theodore Rostow, *What Happens When an Acquaintance Buys Your Data? A New Privacy Harm in the Age of Data Brokers*, 34 YALE J. ON REG. 667, 674 (2017) ("Unlike large companies like Google and Facebook, data brokers try to avoid name recognition . . . .").

161. Leanne Roderick, *Discipline and Power in the Digital Age: The Case of the U.S. Consumer Data Broker Industry*, 40(5) CRITICAL SOC. 729 (2014).

162. Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Data Brokers: A Call for Transparency and Accountability Opening Remarks of Chairwoman Edith Ramirez (May 27, 2014).

163. FTC DATA BROKER REPORT, *supra* note 159, at ii (identifying the following data brokers for the FTC study: Acxiom, Corelogic, Datalogix, eBureau, ID Analytics, Intelius, PeekYou, Rapleaf, and Recorded Future).

164. *Id.*

165. Rostow, *supra* note 160, at 669.

166. FTC DATA BROKER REPORT, *supra* note 159, at 3.

167. *See* Melanie Hicken, *Big Data Knows You're Sick, Tired and Depressed*, CNN MONEY (June 3, 2014), https://money.cnn.com/2014/06/01/pf/data-consumer-health/index.html [https://perma.cc/J3LU-N5D9].

offering new medications."[168] Acxiom, by contrast, boasts an average of 1,500 pieces of information on more than 500 million consumers.[169]

The data broker industry has recently expanded by orders of magnitude in the U.S. and has proved profitable.[170] The nine brokers studied by the FTC posted a combined $426 million in annual revenue.[171] And that was in 2012.[172] In 2018, Acxiom alone projected annual revenue of approximately $945 million,[173] lending weight to the once hyperbolic claim that personal data is the new oil.[174] The basic model of collecting personal data for later sale reinforces the drive to glean as much detailed data as possible. The more complete a user profile, the more valuable it is. Where do data brokers get personal consumer data, and what types of data are included?

B. Data Brokers: Collection, Consumers, and Clients

First, data brokers have captured much data.[175] They leverage "billions of individual data points to produce detailed portraits of virtually every American consumer."[176] One researcher posits that "there is little question that the major data brokers know more about

168. *Id.*

169. Tucker, *supra* note 137.

170. *See* Rostow, *supra* note 160, at 674; *see also* FTC DATA BROKER REPORT, *supra* note 159, at vii, 23 (finding that "data broker practices have grown dramatically, in both breadth and depth, as data brokers have expanded their ability to collect information from a greater number of sources, including from consumers' online activities; analyze it through new algorithms and emerging business models; and store the information indefinitely due to reduced storage costs").

171. *See* FTC DATA BROKER REPORT, *supra* note 159, at 23.

172. *See id.*

173. Sacha Molitorisz, *It's Time for Third-Party Data Brokers to Emerge from the Shadows*, THE CONVERSATION (Apr. 4, 2018), https://theconversation.com/its-time-for-third-party-data-brokers-to-emerge-from-the-shadows-94298 [https://perma.cc/997P-MXH6].

174. *See, e.g.*, Dennis D. Hirsch, *The Glass House Effect: Big Data, the New Oil, and the Power of Analogy*, 66 ME. L. REV. 373, 374 (2014).

175. *See* FTC DATA BROKER REPORT, *supra* note 159, at iv (finding in the FTC study of only nine data brokers, "one data broker's database has information on 1.4 billion consumer transactions and over 700 billion aggregated data elements; another data broker's database covers one trillion dollars in consumer transactions; and yet another data broker adds three billion new records each month to its databases").

176. Craig Timberg, *Brokers Use 'Billions' of Data Points to Profile Americans*, WASH. POST (May 27, 2014), https://www.washingtonpost.com/business/technology/brokers-use-billions-of-data-points-to-profile-americans/2014/05/27/b4207b96-e5b2-11e3-a86b362fd5443d19_story.html?noredirect=on&utm_term=.b7ee81dc276e [https://perma.cc/39BH-AU5W].

each of us than say, for example, the National Security Agency, the Internal Revenue Service, the Social Security Administration, or any other government institution."[177] But no comprehensive study reveals where data brokers get their information.[178]

The limited FTC report from 2014 shows that public sources, including local, state, and federal governments, provide a range of personal data about bankruptcy filings, professional licensing, and eligibility to receive government contracts or other benefits.[179] Localized public records, like those involving taxes, mortgages, property interests, foreclosures, motor vehicle registrations, driving records, and criminal records, also contribute.[180] But public records, of course, are not the sole source of information for data brokers.

Data brokers buy consumer purchase and web-browsing data, including information about consumers' everyday interactions.[181] Data brokers also buy and sell data among themselves.[182] In the FTC study, the nine data brokers obtained much of their information—including the purchase history of 190 million individual consumers from more than 2,600 merchants and self-reported information that consumers provided online or offline through marketing surveys, warranty registrations, and contests—from other data brokers.[183] Moreover, each data broker used multiple sources for similar data.[184] One broker obtained consumers' contact information from twenty different sources.[185]

Notably, laws often protect some of this data but do so in a limited fashion. Data brokers need only obtain the data from an unrestricted party.[186] For example, the Health Insurance Portability and Accountability Act (HIPAA) bars medical providers from selling or

177. David C. Vladeck, *Consumer Protection in an Era of Big Data Analytics*, 42 OHIO N.U. L. REV. 493, 498 (2016).

178. *See* FTC DATA BROKER REPORT, *supra* note 159, at 11–15.

179. *See id.* at 11.

180. *See id.* at 11–13.

181. *See id.* at iv.

182. *See id.* at 12–13.

183. *Id.* at 14.

184. *See id.*

185. *See id.*

186. For example, several states restrict their departments of motor vehicles from disclosing motor vehicle records. *See id.* at 13 n.38. (finding that "[a]t least twenty-three states have state laws governing the disclosure of motor vehicle records that prohibit companies from using such information"). That data, however, often emerges in a myriad of other contexts that are readily accessible by data brokers. *See id.* at 11–15.

freely transferring medical data about a patient's mental illness,[187] but data brokers access and retain that information if the patient unwittingly reveals her illness through her web browsing history or in an online survey.[188] A disabled person searching online (or at a brick-and-mortar store) for a wheelchair generates data exhaust from a web search followed by the retailer's electronic record. HIPAA does not bar the sharing of this information. Nor does HIPPA restrict health data gleaned by Fitbits, Apple Watches, or other devices emerging in the Internet of Things.[189]

Because data brokers also buy and sell data among themselves, it increases the likelihood that sensitive data nominally protected by sectoral statutes will end up in a consumer profile.[190] The digital world is porous.[191] The web diffuses personal data.[192] When personal data can be gathered from a panoply of varying sources, privacy laws that restrict one source only fail.

This duplication and diffusion of personal information accounts in part for the industry's shrouded nature. No direct line connects a consumer's personal data to a data broker.[193] As the FTC reported, data brokers do not obtain personal information directly from consumers.[194] A wide range of sources, including public records, web-browsing trackers, transaction records gleaned from commercial retailers, and social media posts, feed into broker databases.[195] Data brokers then buy and sell information among themselves, and while each source may provide a single data point about a consumer, in the aggregate

187. *See generally* Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 936 (1996) (codified as amended in various sections of 18, 26, 29, and 42 U.S.C.). Data brokers are not covered entities under HIPAA, which are defined to include certain doctors' offices, hospitals, insurance companies, and others that electronically bill insurance companies. *See Covered Entities and Business Associates*, U.S. DEP'T OF HEALTH AND HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html [https://perma.cc/BUY5-FXXD] (last updated June 16, 2017).

188. *See, e.g.*, Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 PENN ST. L. REV. 777, 788 (2016).

189. *See id.*

190. *See id.* (noting that data brokers buy and sell data among themselves and that laws protecting sensitive information, like HIPAA, do not apply to data brokers).

191. *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 44–47 (2004).

192. *See id.*

193. *See* FTC DATA BROKER REPORT, *supra* note 159, at 11–15.

194. *See id.*

195. *See id.*

brokers compile comprehensive composites.[196] The FTC concluded that "it would be virtually impossible for a consumer to determine how a data broker obtained his or her data; the consumer would have to retrace the path of data through a series of data brokers."[197]

C. Data Brokers: Analysis, Categorization, and Resulting Harms

Of course, brokers are not limited to gathering personal data; they also analyze it.[198] In so doing, they introduce a new raft of privacy harms. In addition to amorphous anxiety stemming from the prospect of constant monitoring,[199] the practice of sorting and categorizing consumers carries risks of profiling,[200] discrimination,[201] social engineering,[202] stratification,[203] and identity theft.[204]

To market the data collected, brokers employ learning algorithms.[205] Software enables manipulation of enormous amounts of data and generates precise segments of the population sought by brokers' clients.[206] Categories themselves are wide-ranging and often divide groups by ethnicity, income, religion, and political views.[207] More discrete categories like "Consumers Interested in Buying Camping Gear" and "Consumers that are Likely to Seek a Chargeback" target specific retail clients.[208] But other categories like

196. *See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1889–90 (2013) (describing the "aggregation effect").

197. FTC DATA BROKER REPORT, *supra* note 159, at iv.

198. *See id.* at 19.

199. *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 493 (2006) ("[D]irect awareness of surveillance [can] make a person feel extremely uncomfortable . . . .").

200. *See, e.g.*, Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735, 1772 (2015).

201. *See, e.g.*, Peppet, *supra* note 50, at 117–28.

202. *See, e.g.*, Frederik Zuiderveen Borgesius et al., *Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework*, 30 BERKELEY TECH. L.J. 2073, 2091–93 (2015); Hu, *supra* note 200, at 1735.

203. *See, e.g.*, Borgesius et al., *supra* note 202, at 2093.

204. *See, e.g.*, Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1229 (2003).

205. *See* Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 378 (2006); *see also* FTC DATA BROKER REPORT, *supra* note 159, at 49.

206. *See* Lipman, *supra* note 188, at 781–82.

207. *See* FTC DATA BROKER REPORT, *supra* note 159, at 19–21.

208. *Id.* at 19.

"Urban Scramble" and "Mobile Mixers" consist of Latino and African-American consumers with low incomes.[209]

In fact, a host of categories focus on these defining attributes.[210] The many groups defined by race, age, and low income suggest a robust demand from broker clientele.[211] Providers of high-interest loans, appliance rentals, payday loans, and other high-risk products target this demographic.[212] In one disturbing account, a data broker sold several categories of personal data to a telemarketer client.[213] Each category included elder consumers that appeared vulnerable.[214] "Suffering Seniors" comprised elderly people with cancer.[215] "Oldies but Goodies" included people over fifty-five who liked to gamble, and "Elderly Opportunity Seekers" consisted of older people seeking money-making opportunities.[216] One category explicitly characterized its members as "gullible," saying "[t]hey want to believe that their luck

209. *Id.* at 20.

210. As noted by the Federal Trade Commission, other categories that combine ethnicity with income include: (1) "Work & Causes," which includes consumers "with lower-incomes, in their late 40s, early 50s," "living in multi-unit dwellings;" (2) "Resolute Renters," which includes consumers in their 30s and 40s, single with no children, that are "relatively mobile renters and on the lower rungs of income and net worth;" (3) "Metro Parents," which includes consumers "primarily in high school or vocationally educated," "handling single parenthood and the stresses of urban life on a small budget;" (4) "Modest Wages," which includes "low income singles living without children in a mix of smaller, industrial cities" with low "educational attainment;" (5) "Kids and Rent," which includes "lower income households" with children that are "mostly renters, living in both single-family and multiple-family apartment buildings;" (6) "Downtown Dwellers," which includes "lower-income, single, downtown-metro dwellers," that are "upper-middle-aged" and with a "high-school" or "vocational/technical" degree working to "make[ ] ends meet with low-wage clerical or service jobs;" (7) "Financially Challenged," which includes consumers "[i]n the prime working years of their lives, . . . including many single parents, struggl[ing] with some of the lowest incomes and little accumulation of wealth." These consumers are "[n]ot particularly loyal to any one financial institution, [and] they feel uncomfortable borrowing money and believe they are better off having what they want today as they never know what tomorrow will bring." *Id.* at 20 n.52.

211. *See id.*

212. *See* Press Release, Fed. Trade Comm'n, FTC Recommends Congress Require the Data Broker Industry to Be More Transparent and Give Consumers Greater Control over Their Personal Information (May 27, 2014), https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more [https://perma.cc/PZ4P-P46Q].

213. *See* Charles Duhigg, *Bilking the Elderly, With a Corporate Assist*, N.Y. TIMES (May 20, 2007), http://www.nytimes.com/2007/05/20/business/ 20tele.html?pagewanted=all&_r=0 [https://perma.cc/4PZG-867Z].

214. *See id.*

215. *Id.*

216. *Id.*

can change."[217] The telemarketer used these data sets to "trick vulnerable senior citizens into revealing their bank information in order to raid their accounts."[218]

The potential privacy harms are diverse and include the manipulation of consumers by commercial interests, the profiling of consumers to the benefit of members of one category and detriment of another, the profiling of vulnerable consumers to facilitate third party exploitation, identity theft achieved by criminal clients purchasing detailed personal data, blackmail, and more. Moreover, the information housed by data brokers is often not secured.[219] In 2003, hackers accessed an estimated 1.6 billion records containing personal information following a data breach at Acxiom.[220] Additionally, broker profiles contain mistakes.[221] One large broker admitted that up to 30% of the information in a consumer's profile "may be wrong at any given time."[222] Erroneous profiling can have cascading negative effects on the consumer, particularly in light of the documented difficulty in correcting inaccurate information.[223]

Even the more abstract privacy harms merit consideration. The Hawthorne Effect (also referred to as the observer effect) is a reaction in which individuals modify an aspect of their behavior in response to their awareness of being observed.[224] Most Americans are currently unaware of the pervasiveness of data monitoring.[225] This will eventually change as data brokers and their clients become

---

217. *Id.*

218. Ashley Kuempel, *The Invisible Middlemen: A Critique and Call for Reform of the Data Broker Industry*, 36 NW. J. INT'L L. & BUS. 207, 221 (2016) (citing Duhigg, *supra* note 213).

219. Hirsch, *supra* note 174, at 378–79.

220. *See id.* at 379.

221. *See* Lipman, *supra* note 188, at 782.

222. *Id.* (quoting Melanie Hicken, *Find Out What Big Data Knows About You (It May Be Very Wrong)*, CNN MONEY (Sept. 5, 2013, 2:02 PM), http://money.cnn.com/2013/09/05/pf/acxiom-consumer-data [https://perma.cc/NMJ5-QCYJ]).

223. *See id.*; *see also* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1186–87 (2002) (discussing the social dangers involved with aggregate data brokering); FTC DATA BROKER REPORT, *supra* note 159, at iv (noting the difficulty of tracing consumer personal data to data broker).

224. *See* Bill Delmore, *Cameras in the Courtroom: Limited Access Only*, 67 TEX. B.J. 782, 783 (2004).

225. *See* FTC DATA BROKER REPORT, *supra* note 159, at iv ("Data brokers do not obtain this data directly from consumers, and consumers are thus largely unaware that data brokers are collecting and using this information.").

increasingly adept at leveraging the oceans of searchable personal data compiled on each of us.[226] When public awareness catches up to the reality of universal monitoring, self-censorship based on permanent visibility could very well change society on a large scale. Knowing that nearly every action—including every web search, non-cash purchase, and physical movement—is captured and analyzed portends cultural and societal homogenization.[227]

With harms ranging from abstract (and perhaps unlikely) homogenization to concrete identity theft, a legal structure enacted to forestall these harms might be expected. But the data broker industry, increasingly fueled by the Internet of Things, is self-regulated.[228] One commentator colorfully acknowledged this oddity: "As shady as it might sound, the entire industry is completely legal."[229] Indeed, Congress has not passed a statute expanding privacy protections in more than a decade.[230]

In summary, the data broker industry houses mountains of consumer data, much of it highly specific and personal.[231] Virtually unregulated, the industry is poised to propagate a wide range of privacy harms, all without consumer knowledge.[232]

III. NOTICE, CONSENT, AND REGULATION BY ACCRETION

Regulations safeguarding data privacy have developed by accretion, with new laws building off their predecessors. In the U.S., for example, the 1974 Privacy Act introduced "fair information practices," which included an individual's right to notice and consent

---

226. *See id.*

227. *See, e.g.*, Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000) ("Pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream."); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1656 (1999) (stating that constant surveillance "short-circuits the individual's own process of decision-making").

228. *See* Rostow, *supra* note 160, at 669; Hillary Brill & Scott Jones, *Little Things and Big Challenges: Information Privacy and the Internet of Things*, 66 AM. U.L. REV. 1183, 1199 (2017) (explaining that as the Internet of Things becomes more integrated, data aggregators can pull more information from more devices, which makes it easier to piece together a digital profile of someone).

229. Paul Boutin, *The Secretive World of Selling Data About You*, NEWSWEEK (May 30, 2016), http://www.newsweek.com/secretive-world-selling-data-about-you-464789 [https://perma.cc/MD73-DWLY].

230. *See* Rostow, *supra* note 160, at 693.

231. *See generally* FTC DATA BROKER REPORT, *supra* note 159.

232. *See generally* Boutin, *supra* note 229.

before personal data could be collected and used.[233] The law further allowed access to one's personal information.[234] Once collected by a third party, the law imposed a legal obligation to secure the data.[235] This basic structure of notice, consent, access, and security remains the dominant regulatory scheme today.[236]

The Organization for Economic Cooperation and Development (OECD), an international nongovernmental organization,[237] adopted the same structure when it set forth guidelines in 1980: Before personal information could be collected, the data subject must have notice of the pending collection and give his or her consent.[238] The OECD's guidelines in turn became the blueprint for binding legislation throughout the European Union.[239]

A. European Union Privacy Law

Adopted in 1995, the E.U.'s Data Protection Directive set the international standard for data privacy and security regulation.[240] It too

233. *See* Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified at 5 U.S.C. § 552a (1988)); *see also* Richard Ehlke, *The Privacy Act After a Decade*, 18 J. MARSHALL L. REV. 829, 835–40 (1985) (examining amendments to Privacy Act); Office of Privacy and Civil Liberties, *Privacy Act of 1974*, U.S. DEP'T OF JUSTICE, https://www.justice.gov/opcl/privacy-act-1974 [https://perma.cc/XC6Q-E5KJ] (crediting the Privacy Act of 1974 with "establish[ing] a code of fair information practices") (last updated July 17, 2015).

234. *See* Ehlke, *supra* note 233, at 837.

235. *See id.* at 830.

236. *See generally* OFFICE OF PRIVACY AND CIVIL LIBERTIES, U.S. DEP'T OF JUSTICE, UNITED STATES DEPARTMENT OF JUSTICE OVERVIEW OF THE PRIVACY ACT OF 1974: 2015 EDITION (2015).

237. The OECD is an international economic organization of over thirty countries and was founded in 1961 to stimulate economic growth and world trade. *See History*, ORG. FOR ECON. CO-OPERATION & DEV., http://www.oecd.org/history [https://perma.cc/4EEY-JD3A] (last visited May 24, 2019). It originated as the Organisation for European Economic Cooperation (OEEC) in 1948 to run the U.S.-financed Marshall Plan for reconstruction of war-torn Europe. *See id.*

238. *See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, ORG. FOR ECON. CO-OPERATION & DEV., https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [https://perma.cc/539D-P4G3] (last visited May 24, 2019); *see also* Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 180–81 (1999).

239. *See* Council Directive 95/46/EC, 1995 O.J. (L 281) 31, 31–33 [hereinafter Data Protection Directive].

240. *See* Christopher Kuner, *The European Union and the Search for an International Data Protection Framework*, 2 GRONINGEN J. INT'L L. 55, 55 (2014)

relied on notice, consent, access, and security.[241] In addition, the Directive sought to regulate the use and transfer of the data after collection, providing that personal data could be collected only for "specified, explicit[,] and legitimate purposes and not further processed in a way incompatible with those purposes."[242]

The Directive is arguably the most important data privacy law to date,[243] due in part to its comprehensive scope and its extrajurisdictional reach.[244] The law forbids transfer of the personal data of E.U. citizens to other countries until those countries prove compliance with the Directive by enacting adequate regulatory protections.[245] The Directive spurred a trend among technologically advanced countries toward adopting nationalized data privacy laws that materially mimicked the Directive.[246] Effective in May 2018, the General Data Protection Regulation (GDPR) superseded the Directive in the E.U.[247] It also relies on notice, consent, access, security, limited use, and transfer.[248] Like the Directive, the GDPR carries extrajurisdictional ramifications by requiring countries or entities to prove compliance with the GDPR before allowing the transfer of E.U.-held personal data.[249]

(characterizing the "EU law as the most influential body of data protection law worldwide").

241. *See* Data Protection Directive, *supra* note 239, at 40.

242. *Id.*

243. Many commentators characterize the Directive as the most influential national data protection law. *See* Kuner, *supra* note 240, at 55 (characterizing the "EU law as the most influential body of data protection law worldwide").

244. *See* Brussels European Council Memo 01/228, Standard Contractual Clauses for the Transfer of Personal Data to Third Countries – Frequently Asked Questions (June 18, 2001). The European Commission justified the long reach of the law by noting that "[w]ithout such rules, the high standards of data protection established by the [Data Protection] Directive would quickly be undermined, given the ease with which data can be moved around on international networks." *Id.*

245. *See* Data Protection Directive, *supra* note 239, at 45; *see also* Council Regulation 2016/679, 2016 O.J. (L 119) 1, 61 [hereinafter General Data Protection Regulation] ("A transfer . . . may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection.").

246. *See* Graham Greenleaf, *76 Global Data Privacy Laws*, PRIVACY L. & BUS. 1, 2 (Sept. 2011) (showing that nineteen new omnibus privacy laws were enacted in the 1990s and thirty-two more emerged in the 2000s).

247. *See* General Data Protection Regulation, *supra* note 245, at 86.

248. *See id.* at 35–36.

249. *See id.* at 61 ("A transfer . . . may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection.").

Importantly, this regulatory scheme predated the Internet, the data economy, and certainly the Internet of Things.[250] Although the GDPR was adopted in 2016 and became effective in 2018, its regulatory framework stems from a 1974 statute.[251] The GDPR's framework and the implicit assumptions inherent therein are ill-suited to meet the privacy threats posed by ubiquitous rooftop cameras, license plate readers, and sensors engrafted onto otherwise ordinary objects. In other words, the legal framework relies principally on notice to and consent from the user before information is gathered and used.[252] But much of the data harvested by the Internet of Things occurs without the user's knowledge or consent.[253]

License plate readers, whether private or public, do not solicit consent before snapping images, nor do video doorbells, dashboard cameras, ATMs, or purposefully miniscule cameras embedded in hotel elevators. When notice and consent occur, they fail to address the collection of bystander data.[254] While a user might read the licensing agreement and fully consent to divulging personal information when installing a smart thermostat, what about her guests?

Rental economies, whether for cars, homes, appliances, or computers, interject more barriers to the effectiveness of notice and consent.[255] Thousands of rented computers, for example, include software that include not only a remote shutoff if payment is overdue but also a "Detective Mode," a feature that allows creditors to secretly turn on the laptop's webcam and take pictures of the user or whomever else is within range.[256] In one instance, surreptitious pictures were

250. *See, e.g.*, NICK COULDRY, MEDIA, SOCIETY, WORLD: SOCIAL THEORY AND DIGITAL MEDIA PRACTICE 2 (2012) (associating the beginning of the Internet with the launch of the World Wide Web in 1991).

251. *See supra* Part III.

252. *See* General Data Protection Regulation, *supra* note 245, at 36 ("[T]he data subject has given consent to the processing of his or her personal data for one or more specific purposes.").

253. *See* Jan Henrik Ziegeldorf et al., *Privacy in the Internet of Things: Threats and Challenges*, 7 SECURITY & COMM. NETWORKS 2728, 2733 (June 2013) (noting that with the Internet of Things "humans will be mostly passive and unaware of data collection").

254. *See* Swire & Woo, *supra* note 121, at 1484 (noting that consent "can also be an issue for bystanders, who may not know they have been recorded by a BWC at all or may learn about the recording after the fact, when a video is made public").

255. *See* Elvy, *Hybrid Transactions*, *supra* note 39, at 150–51.

256. Caroline Lester, *Why Today's Rent-to-Own Economy Presents a Host of Privacy Challenges*, PRI (May 26, 2016), https://www.pri.org/stories/2016-05-

taken of Pennsylvania schoolchildren in their bedrooms after they had checked out public school computers.[257]

Even if notice is provided, how detailed must it be? Does the occupant of a home hooked to a smart meter have notice that the unique electrical signal emanating from the home reveals the exact movie she watched last night, which light bulbs are currently on, and when she is away on vacation?[258] As technology incessantly pushes forward, full notice and informed consent are largely impotent.[259] The diversifying ways in which data is collected coupled with the endless inferences drawn from that data make it nearly impossible to provide complete and full notice.

Although laudable in many respects, the GDPR fails to envision a world populated by the Internet of Things. The law principally targets the process of data collection rather than its after-captured use.[260] It focuses on how personal data is harvested rather than the harms occasioned by privacy breaches.[261] It fails to acknowledge that reams of personal data have been collected already.[262] When just one data broker holds 5,000 pieces of information on over 500 million people, the GDPR's focus on restricting the collection of personal data seems quaint.[263]

27/why-todays-rent-own-economy-presents-host-privacy-challenges [https://perma.cc/BJ8T-4Z6P].

257. *See generally* Robbins v. Lower Merion School District, No. 10-CV-665, 2010 WL 3421026 (E.D. Pa. Aug. 30, 2010). In *Robbins*, claimants alleged that the schools secretly spied on students while they were in the privacy of their homes and that school authorities surreptitiously and remotely activated webcams embedded in school-issued laptops the students were using at home. *See id.* at *1. In October 2010, the school district agreed to pay $610,000 to settle the suit. *See $610 Settlement in School Webcam Spy Case*, CBS NEWS (Oct. 21, 2010), https://www.cbsnews.com/news/610k-settlement-in-school-webcam-spy-case/ [https://perma.cc/G6Q7-7YYA].

258. For example, SMECO's privacy policy for smart metering generally states that "SMECO is required by law to observe certain prohibitions regarding the disclosure of individual customer data. Customers' smart meter energy use data will only be collected, processed, retained, or disclosed for legitimate SMECO utility-related business reasons." *Privacy Policy for Smart Meter Data*, SMECO, https://www.smeco.coop/services/smart-meters/privacy [https://perma.cc/N3MW-P3HQ] (last visited May 24, 2019).

259. *See* Peppet, *supra* note 50, at 140–41 (noting that because many Internet of Things devices lack a screen or other user interface, providing meaningful notice and consent is difficult, at best).

260. *See* General Data Protection Regulation, *supra* note 245, at 36.

261. *See id.*

262. *See id.*

263. Tucker, *supra* note 137.

It is true that the GDPR also purports to regulate the use of personal data after its collection.[264] But the GDPR's capacious scope emasculates the effectiveness of use-based restrictions because the law applies universally and is not tailored to identified privacy harms.[265] This overbreadth makes the GDPR difficult to evenly enforce.[266] Perhaps this is most clearly seen in the continued reliance upon the definition of personally identifiable information (PII).[267] The GDPR outlaws illicit data collection only if it was personal.[268] This has proven to be a murky concept at best.[269] Names, addresses, and social security numbers qualify as PII, but what about data that when combined with other data enables identification?

Instead of drafting a detailed definition or including a representative list of PII, the GDPR defines personal data as "any information relating to an identified or identifiable natural person."[270] It bears repeating. The law captures any information "relating" to an identifiable person.[271] It is an extremely broad definition. If the data could feasibly enable the holder to connect it to a specific person, even if the holder himself cannot make the connection, the GDPR is triggered.[272] One commentator noted that the definition of PII "encompasses . . . more information than those European legislators could . . . have imagined— . . . more than all the bits and bytes in the entire world when they wrote their law [eighteen] years ago."[273]

It includes the innocuous processing of "personal data" rather than the harms occasioned by its misuse.[274] It fails to appreciate data

264. *See* McKay Cunningham, *Privacy Law That Does Not Protect Privacy, Forgetting the Right to Be Forgotten*, 65 BUFF. L. REV. 495, 538–39 (2017).

265. *See id.* (arguing that the data privacy regulation should restrict the use of sensitive data as it relates to particular privacy risks).

266. *See id.*

267. *See* General Data Protection Regulation, *supra* note 245, at 5.

268. *See* Data Protection Directive, *supra* note 239, at 38; General Data Protection Regulation, *supra* note 245, at 33.

269. *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1819–47 (2011).

270. General Data Protection Regulation, *supra* note 245, at 33.

271. *Id.*

272. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1706–18 (2010).

273. Tucker, *supra* note 137.

274. On the Concept of Personal Data (Art. 29 Data Protection Working Party), Advisory Opinion 4/2007, 01248/07/EN/WP136, 12 (June 20, 2007) (noting that information is "personal," according to European officials, even though "the person has not been identified yet, [if] it is possible to do it").

captured by the Internet of Things.[275] As noted by one commentator, "efforts toward a concise definition of what constitutes PII are quickly deprecated as new [Internet of Things] technologies unlock and combine new sets of data that can enable identification and make it increasingly difficult to distinguish PII from non-PII."[276] Given the enormity of the data now available and in light of the algorithms that analyze it, almost any bit of data can be personally identifiable.[277] The more data we have, the less any of it can be considered private.

In conjunction with its extraterritorial reach, the GDPR's ability to capture any information relating to an identifiable person renders it nearly unbounded in scope.[278] The fact that the data must relate to an E.U. resident is arguably the operative limitation.[279] As a result, the E.U. "bring[s] all providers of Internet services such as websites, social networking services and app providers under the scope of the [E.U.] [r]egulation as soon as they interact with data subjects residing in the European Union."[280] This overbreadth frustrates the law's effectiveness.[281] If everyone that has anything to do with an E.U. resident comes within the ambit of the law, a host of innocent transactions causing no privacy harm must comply.[282]

Anonymization, for the same reason, fails to inoculate data.[283] Merely stripping the name off locational data, for example, does not prevent that locational data from identifying the user.[284] Advances in computer science increase the likelihood of re-identifying supposedly

---

275. *See generally* Ziegeldorf et al., *supra* note 253.

276. *Id.* at 2731.

277. *See* Arvind Narayanan & Vitaly Shmatikov, *Privacy and Security: Myths and Fallacies of "Personally Identifiable Information"*, 53 COMM. ACM 24, 26 (2010).

278. *See* Dan Jerker B. Svantesson, *Extraterritoriality in the Context of Data Privacy Regulation*, 7 MASRAYK U. J.L. & TECH. 87, 90 (2012).

279. *See id.*

280. *Id.*

281. *See* Cunningham, *supra* note 264, at 513–17.

282. As one commentator suggests, full enforcement of Europe's privacy law would threaten Europe's entire economy: "Because the data-flow restrictions are potentially so harmful not only to third-party nation economies, but also to Europe's economy itself, one has to wonder whether the risk of noncompliance is really significant." Steven R. Salbu, *Regulation of Borderless High-Technology Economies: Managing Spillover Effects*, 3 CHI. J. INT'L L. 137, 141 (2002).

283. *See* Ohm, *Broken Promises of Privacy*, *supra* note 272, at 1706–18 (discussing the prevalence of identifying individuals through anonymized data).

284. *See* Tucker, *supra* note 137 (citing study in which researchers used four data points about a phone's position to identify the user after the user's identity had been redacted to provide anonymity).

"anonymized" data, rendering futile many attempts to protect privacy with anonymity.[285] Commercial transactions, browsing histories, public records, and much more populate de-anonymizing algorithms, prompting the observation that "any attribute can be identifying in combination with others."[286] Consequently, the GDPR's amorphous scope captures a sea of "innocent" interactions—data processing that threatens no privacy harm whatsoever.[287]

This capacious scope in turn encourages discretionary enforcement.[288] If applied literally, officials could seize almost any digital device in Europe since smartphones and laptops likely contain information that could lead to information "relating" to an identifiable person.[289] Laws that identify as wrongdoers a disproportionately large ratio of those governed have historically been disfavored because they imbue law enforcement with unchecked authority to prosecute disfavored citizens, promoting corruption over compliance.[290]

Unlike in Europe, where the law regards privacy as a fundamental right, U.S. privacy law has been described often as "sectoral."[291] Several industries, like the medical and financial sectors for example, must comply with industry-specific legislation aimed at protecting discrete private information.[292] Perhaps owing to a preference for free speech,[293] informational privacy as a standalone

285. *See* Ohm, *Broken Promises of Privacy*, *supra* note 272, at 1703–04.

286. Narayanan & Shmatikov, *supra* note 277, at 26 (emphasis omitted).

287. *See id.* at 24.

288. *See* Cunningham, *supra* note 264, at 515.

289. *See id.*

290. *See, e.g.*, Chicago v. Morales, 527 U.S. 41, 60 (1999) (holding that a law cannot be so vague that a person of ordinary intelligence cannot figure out what is innocent activity and what is illegal); People v. Golb, 15 N.E.3d 805, 813 (N.Y. 2014) (striking down a harassment statute where the language was overbroad); People v. Dietze, 549 N.E.2d 1166, 1169 (N.Y. 1989) (striking down a similar harassment statute, former Penal Law, Section 240.25, which prohibited the use of abusive or obscene language with the intent to harass, annoy or alarm another person).

291. *See* Cate, *The Changing Face of Privacy Protection*, *supra* note 238, at 217.

292. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified at 42 U.S.C. §§ 1320d-1 to -9 (2012)); Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified at 15 U.S.C. §§ 6801–6809 (2012)).

293. *See* Steven C. Bennett, *The "Right to Be Forgotten": Reconciling EU and US Perspectives*, 30 BERKELEY J. INT'L L. 161, 169 (2012); Emily Adams Shoor, *Narrowing the Right to Be Forgotten: Why the European Union Needs to Amend the Proposed Data Protection Regulation*, 39 BROOK. J. INT'L L. 487, 498–501 (2014).

comprehensive right is not nationally protected under the Constitution or by federal statute.[294]

In fact, a law review article by Samuel Warren and Louis Brandeis often provides the starting point for those researching U.S. privacy law.[295] The authors' stated purpose was "to consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is."[296] Just by posing the question the authors concede the lack of a clear principle animating legal privacy protections. Although the authors identified principles to support privacy law, they also articulated several limitations, and commentary from a law review article lacks the permanence attending statutory enactment or constitutional warrant.[297]

Given this history, the absence of a comprehensive privacy right in the U.S. is unsurprising. Instead, industry-specific legislation has created a patchwork of privacy laws.[298] The Gramm-Leach-Bliley Act limits the use of private financial data,[299] for example, and HIPAA regulates the use of "protected health information."[300] The Fair and Accurate Credit Transactions Act regulates information that attends credit reporting,[301] and the Video Privacy Protection Act bans "wrongful disclosure of video tape rental or sale records."[302] Notably, the definition of personal information found in the Fair Credit Reporting Act differs from that found in the Video Privacy Protection

294. *See* Richard J. Peltz-Steele, *The New American Privacy*, 44 GEO. J. INT'L L. 365, 383–93 (2013).

295. *See, e.g.*, Melville B. Nimmer, *The Right of Publicity*, 19 L. & CONTEMP. PROBS. 203, 203 (1954); Neil M. Richards, *The Puzzle of Brandeis, Privacy, and Speech*, 63 VAND. L. REV. 1295, 1295–96 (2010).

296. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 197 (1890).

297. *See id.* at 207–13.

298. *See* Nicole A. Ozer, *Putting Online Privacy Above the Fold: Building a Social Movement and Creating Corporate Change*, 36 N.Y.U. REV. L. & SOC. CHANGE 215, 217 (2012) (noting the many and disparate privacy related statutes).

299. *See* Gramm-Leach-Bliley Act §§ 6801–6809.

300. *See* Health Insurance Portability and Accountability Act §§ 1320d-1 to -9.

301. *See* Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified at 15 U.S.C. § 1681 (2012)). This Act was passed by Congress and signed into law in 2003 as an amendment to the Fair Credit Reporting Act. *See id.* The Act allows consumers to request and obtain a free credit report once every twelve months from each of the three nationwide consumer credit reporting companies. *See id.* at 1970.

302. Video Privacy Protection Act of 1988, Pub. L. No. 100-618 102 Stat. 3195 (codified at 18 U.S.C. § 2710 (2012)).

Act, which in turn differs from that found in the Gramm-Leach-Bliley Act.[303]

The patchwork of unrelated privacy laws continues to frustrate businesses and organizations that routinely process consumer information, particularly those that are reliant on ecommerce.[304] "Companies are frustrated by the lack of harmonisation and the fact that they are often subject to conflicts between data protection law and other legal obligations."[305] Nevertheless, the U.S. remains resolute in its refusal to pass comprehensive data privacy legislation.[306] Following a series of headline-grabbing security breaches that exposed consumer personal information,[307] federal agencies increased regulatory efforts, but Congress declined to pass omnibus privacy legislation that would unify the current regulatory patchwork.[308]

While comprehensive federal legislation would go a long way in harmonizing fragmented privacy protections, most commentators agree that such an approach is unlikely in the near term.[309] The unlikelihood stems in part from the characterization of privacy as an

303. *Compare* 15 U.S.C. § 1681a(d)(1) (2006) (applying to consumer reporting agencies that provide consumer reports, defined as communications by such an agency bearing on a consumer's credit worthiness or personal characteristics when used to establish a consumer's eligibility in certain contexts), *with* Video Privacy Protection Act of 1988, Pub. L. No. 100-618 102 Stat. 3195 (codified at 18 U.S.C. § 2710(a)(3) (2012)) (defining personally identifiable information as "information which identifies a person"), *and* 15 U.S.C. § 6809(4)(A) (2012) (defining personally identifiable financial information as "nonpublic personal information").

304. *See* Morey Elizabeth Barnes, *Falling Short of the Mark: The United States Response to the European Union's Data Privacy Directive*, 27 NW. J. INT'L L. & BUS. 171, 175–94 (2006).

305. *See* Kuner, *supra* note 240, at 55.

306. *See* Greenleaf, *supra* note 246, at 2.

307. *See* Lance Bonner, *Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches*, 40 WASH. U. J.L. & POL'Y 257, 262–63 (2012); Tatiana Melnik, *New U.S. Sanctions Program Seeks to Give Government an Extra Tool to Fight Cyber-Attacks*, 17 J. HEALTH CARE COMPLIANCE 53, 53 (2015).

308. *See, e.g.*, Personal Data Privacy and Security Act of 2014, S.1897, 113th Cong. (2014) (defining personal information as "sensitive personally identifiable information" and including: (1) specified combinations of data elements in electronic or digital form, such as an individual's name, home address or telephone number, mother's maiden name, and date of birth; (2) a non-truncated social security number, driver's license number, passport number, or government-issued unique identification number; (3) unique biometric data; (4) a unique account identifier; and (5) any security code, access code, password, or secure code that could be used to generate such codes or passwords).

309. *See, e.g.*, LISA J. SOTTO, PRIVACY AND DATA SECURITY LAW DESKBOOK § 1.04 (2010) (noting that "harmonization is not imminent").

individual rather than a societal interest.[310] Americans view data privacy as a consumer problem, not a societal one, and the law has conformed to that characterization.[311] Societal harms invoke an active governmental role to forestall harms like environmental degradation or infectious disease.[312] The public interest is codified as legal norm, with government agencies promulgating standards and supervising their implementation.[313] Reporting requirements, audits, and government investigations attend the protection of societal interests.[314] Government creates the legal norm, oversees its implementation, and actively enforces it.[315]

By contrast, data privacy is viewed as an individual interest; injuries are treated as individual to the consumer only.[316] If a rule or statute creates a legal obligation with regard to personal data, redress depends on the consumer recognizing it and seeking a legal remedy on her own.[317] "Consumers assume a large responsibility for identifying their own injuries, policing the market by making informed decisions, and enforcing their rights, usually through litigation."[318]

This characterization of privacy as an individual interest that is protected if at all by the consumer's pursuit of her own remedy dilutes the effectiveness of the data privacy laws in place today. A meaningful gap separates the gathering of personal data from its injurious use.[319] Several entities secretly track browser history and then sell the information.[320] A visit to "NewYorkTimes.com" prompts dozens of

310. *See* Nehf, *supra* note 1, at 5.
311. *See id.*
312. *See id.* at 5–6.
313. *See id.*
314. *See id.*
315. *See id.*
316. *See* Elizabeth DeArmond, *A Dearth of Remedies*, 113 PENN ST. L. REV. 1, 6 (2008) (identifying the remedies available to individuals for privacy injuries and noting their inadequacy).
317. *See id.*
318. Nehf, *supra* note 1, at 5.
319. *See* Laura J. Bowman, *Pulling Back the Curtain: Online Consumer Tracking*, 7 I/S: J.L. & POL'Y FOR THE INFO. SOC'Y 721, 727, 733–36, 748–49 (2012).
320. *See* Matthew A. Goldberg, *The Googling of Online Privacy: Gmail, Search-Engine Histories and the New Frontier of Protecting Private Information on the Web*, 9 LEWIS & CLARK L. REV. 249, 251–55 (2005).

third parties to note and record the user's visit.[321] Indeed, a host of unidentified groups follow users as they navigate the web.[322]

Users typically do not know they are being tracked, nor can they easily divine who is tracking and gathering their browsing history for later sale.[323] Nor are users notified when that information is sold to a data broker or others.[324] It may be years before the privacy harm manifests. A job application rejected based on the applicant's browsing history obtained through a data broker illustrates the difficulty in regulating privacy through individualized enforcement. If data privacy is only protected when the consumer seeks redress, and if the consumer's injury is dislocated from the privacy breach, the law offers little hope of meaningful data protection.

To be fair, data privacy protection is not entirely up to the user alone. The FTC has prosecuted some entities based on data privacy.[325] The prosecutions, though, are relatively rare.[326] The FTC lacks a clear privacy mandate.[327] In the few instances where the FTC has prosecuted entities for data privacy violations, it has done so by leveraging the prohibition against "unfair or deceptive acts or practices in or affecting commerce."[328]

Importantly, the FTC's primary legal argument stems from the defendant's "deceptive" practice, which generally arises when the defendant fails to follow its own privacy policy.[329] A company acts

---

321. *See* Steve Kroft, *The Data Brokers: Selling Your Personal Information*, CBS 60 MINUTES (Aug. 24, 2014), https://www.cbsnews.com/news/data-brokers-selling-personal-information-60-minutes/ [https://perma.cc/6H66-SYTQ].

322. *See* Bowman, *supra* note 319, at 733.

323. *See* J.J. McIntyre, *Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected as Personally Identifiable Information*, 3 DEPAUL L. REV. 895, 913 (2011).

324. *See* FTC DATA BROKER REPORT, *supra* note 159, at iv-vi.

325. *See* TRENDnet, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 78 Fed. Reg. 55, 717–19 (Sept. 11, 2013) [hereinafter TRENDnet, Inc.].

326. In September 2013, the FTC took its first action against an Internet of Things firm when it penalized TRENDnet—a web-enabled camera manufacturer—for promising customers that its cameras were secure when they were not. *See id.*

327. *See* 15 U.S.C. § 45(a)(1) (2012).

328. *Id.*

329. Press Release, Fed. Trade Comm'n, Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case (Aug. 13, 1998), https://www.ftc.gov/news-events/press-releases/1998/08/internet-site-agrees-settle-ftc-chargesdeceptivelycollecting [https://perma.cc/Q6TJ-CX98]. *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d. 602, 615 (D.N.J. 2014) (holding for the first time in federal court that the FTC has authority under Section 5 of the Federal Trade Commission Act to enforce the prohibition against unfair and deceptive acts or practices in the field of data security).

deceptively when it publicly promises to not sell consumer data to third parties and then sells the data to third parties.[330] In other words, enforcement actions brought by the FTC depend on entities (1) voluntarily instituting privacy policies, (2) publishing them, and then (3) failing to follow them.[331] Prosecutions on this basis prompt the perverse incentive to adopt weak privacy policies or to foreswear them altogether.

In summary, U.S. privacy law consists of a patchwork of industry-specific statutes that require user enforcement in addition to intermittent FTC enforcement of deceptive trade practices. It is unsurprising, then, that those entities that process personal data are often characterized as self-regulating.[332] This is no accident, as the electronic commerce industry has moved to forestall government oversight by advocating for self-regulation.[333] The Direct Marketing Association, for example, promulgates and promotes privacy guidelines and encourages members of the association to post a conspicuous notice on their respective websites notifying users of the entity's data collection and retention practices.[334] The credit card industry self-imposes encryption obligations and mandatory reporting for data breaches.[335]

The Clinton Administration advocated industry self-regulation as the best means of protecting the personal privacy of online users without hobbling each industry with government interference, stating,

---

330. *See* TRENDnet, Inc., *supra* note 325 (describing prosecution for TRENDnet's failure to comply with its own privacy policy).

331. *See* Gregory James Evans, *Regulating Data Practices: How State Laws Can Shore Up the FTC's Authority to Regulate Data Breaches, Privacy, and More*, 67 ADMIN. L. REV. 187, 191, 214 (2015) ("And yet, FTC has stated that it lacks authority to address data practices, and the authority it does have is limited to making sure companies follow their own privacy policies.").

332. *See, e.g.*, In the Matter of PDB Sports, Ltd., F.T.C. File No. 142 3025 (F.T.C. 2014), *available at* www.ftc.gov/system/files/documents/cases/140625denverbroncoscmpt.pdf [https://perma.cc/YMJ9-6JHR] (alleging that the Web site operator "represented, expressly or by implication, that it was a 'current' participant in the U.S.-EU Safe Harbor Framework" but was not a current member because the operator failed to renew a required self-certification); BitTorrent, Inc., F.T.C. File No. 142 3020 (F.T.C. 2014), *available at* https://www.ftc.gov/system/files/documents/cases/ 140625bittorrentcmpt.pdf [https://perma.cc/VQR8-JDD4] (alleging similar facts).

333. *See* Siona Listokin, *Industry Self-Regulation of Consumer Data Privacy and Security*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 15, 17–19 (2015).

334. *See* Jonathan P. Cody, *Protecting Privacy over the Internet: Has the Time Come to Abandon Self-Regulation?*, 48 CATH. U. L. REV. 1183, 1218–19 (1999).

335. *See generally* Abraham Shaw, *Data Breach: From Notification to Prevention Using PCI DSS*, 43 COLUM. J.L. & SOC. PROBS. 517 (2010).

"[w]e believe that private efforts of industry working in cooperation with consumer groups are preferable to government regulation."[336] Certainly, the market motivates electronic commerce companies to protect consumer data in many instances, but the effectiveness of market controls remains questionable, especially when privacy harms are latent.[337] Professor Joel R. Reidenberg concluded that "self-regulation is not an appropriate mechanism to achieve the protection of basic political rights."[338]

IV. REGULATORY PROPOSALS AND THEIR SHORTCOMINGS

The regulatory landscape, both domestically and abroad, fails to protect against data privacy harms. Government officials, privacy advocates, and academics have posited legal solutions, many of which would strengthen privacy protections but none of which fully contemplate the enormity, diversity, and granularity of data captured by the Internet of Things and leveraged by data brokers. Nor do these proposals tailor the regulatory restrictions to discrete privacy harms.

For example, the FTC in its 2014 Report proposed new privacy protections, including support for a law aimed at data brokers.[339] The proposed legislation would require brokers to give consumers access to their information once a year for free and allow consumers to then dispute inaccurate data, prompting an obligation on the part of the broker to verify accuracy.[340] Over and above supporting the proposed legislation, the FTC recommended a requirement that consumers opt in before brokers could share "sensitive" data, like personal health information.[341] Finally, the FTC recommended a disclosure provision, which would require that data brokers reveal their data sources and

336. William J. Clinton & Albert Gore, Jr., *A Framework for Global Electronic Commerce*, U.S. NAT'L ARCHIVES & RECS. ADMIN. (1997), https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html [https://perma.cc/H6L3-RU9G] (explaining that the private sector should take the lead to protect privacy over the Internet through self-regulatory regimes).

337. *See* Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1284 (2000) ("From most objective standpoints, protecting information privacy through industry self-regulation is an abject failure.").

338. Joel R. Reidenberg, *E-commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 727 (2001).

339. *See* FTC DATA BROKER REPORT, *supra* note 159, at 49–55.

340. *See id.*

341. *Id.*

that a website disclose a list of the largest data brokers as well as links to their opt-out policies.[342]

Unlike the FTC's recommendations, proposals from the corporate sector advocate market-based solutions.[343] A pay-for-privacy system, for example, would allow consumers to avoid data collection by paying extra, while offering discounts to consumers who consent to collection.[344] A less structured approach to the same concept features businesses charging more for products with robust privacy controls without asking consumers to consent to data collection or providing notice of the same.[345]

On the other end of the spectrum, a proposal billed as consumer-friendly seeks to vest ownership of personal data in the consumer.[346] Sometimes called the "personal data economy," this model houses a consumer's personal data in a single digital location in order to allow the consumer to choose what data to share with specific entities and when.[347] Such user-centric models purport to "empower[] consumers to extract value from their own data by, for instance, selling or providing access to their information to data [brokers]."[348]

Even more proposals flow from academia. Professor Jack Balkin proposes a comprehensive framework that targets the computing and electronic communications industries.[349] He posits a law that would impose a fiduciary obligation on commercial ISPs, search engines, email providers, and social media networks, among others.[350] Each

342. *See id.*

343. *See, e.g.*, Elvy, *Paying for Privacy*, *supra* note 156, at 1393–96.

344. *See id.*; *see also* Letter from Senator Elizabeth Warren to Tom Wheeler, Chairman, Fed. Commc'n Comm'n (June 21, 2016), http://www.warren.senate.gov/files/documents/2016-6-21_Letter_to_FCC_re_Privacy_Rulemaking.pdf [https://perma.cc/ZH5L-8WYC] (describing Internet service provider discount plans as "requir[ing] consumers to pay hundreds of dollars extra each year so that [a company] does not collect and sell information on the websites they visit, the ads they see, and the terms they enter into search engines").

345. *See* Elvy, *Paying for Privacy*, *supra* note 156, at 1396–99.

346. *See id.* at 1393–94 (2017) ("Data monetizations by consumers via PDE marketplaces presume to some extent that consumers have transferable rights in or ownership of the data they generate.").

347. *Id.*

348. *Id.* at 1375.

349. *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1205–08 (2016) (detailing Professor Balkan's proposal).

350. *See id.* at 1221 (proposing "we expand our definition of information fiduciaries to include bookstores, search engines, ISPs, email providers, cloud storage services, providers of physical and streamed video, and websites and social networks when they deal in our intellectual data").

such entity should carry a heightened duty to protect consumer data, not unlike the duties of loyalty and confidentiality owed by lawyers and doctors to their clients and patients.[351]

In contrast to Balkin's comprehensive approach, Professor Paul Ohm proposes a more narrow and practical model. Ohm attempts to identify the types of personal information that could do the most harm to consumers.[352] By defining this "sensitive" personal data, the law could more aggressively protect it.[353] Social security numbers, financial accounts, and medical information fall within this category, but Ohm argues for expanding it further to include precise geolocation information, communications metadata, and biometric data.[354]

All of these proposals have weaknesses. The FTC's emphasis on consumer access to data broker files for correction and the FTC's emphasis on disclosing the sources used by data brokers to gather information do little to forestall privacy harms. They are primarily transparency measures. Nothing limits a broker's ability to sell a consumer's browsing history to a potential employer, insurer, or jilted lover, for example. The opt-out solution also leaves much to be desired. One intrepid reporter in 2014 documented her exhaustive attempt to opt-out from over 200 data brokers,[355] which accounts for less than half of data brokers currently operating.[356]

Similarly, market-based approaches like pay-for-privacy are unlikely to attract significant participation. But more importantly, such approaches commodify what many feel is a universal right to

---

351. *See id.* at 1205 (comparing the fiduciary duty possessed by these entities to the duties of confidentiality and loyalty possessed by lawyers and doctors).

352. *See* Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1132–34 (2015) (explaining and providing examples of sensitive information).

353. *See id.* at 1134.

354. *See id.* at 1143–44 (describing three candidates for new sensitive information categories).

355. *See* Julie Angwin, *Privacy Tools: Opting Out from Data Brokers* (Jan. 30, 2014), http://juliaangwin.com/privacy-tools-opting-out-from-data-brokers/ [https://perma.cc/795L-KZPL] (documenting one author's attempt to opt-out from 212 commercial data brokers).

356. *See* Boutin, *supra* note 229 (providing that the exact number of data brokers currently operating in the United States is unknown, but "[c]redible estimates range from 2,500 to 4,000"). Additionally, many data brokers distinguish "opt-out" from "delete." *See* FTC DATA BROKER REPORT, *supra* note 159, at 42. A successful opt-out request merely conceals the consumer's personal information from "display in the data broker's marketing products." *Id.* The broker retains the data itself. *See id.* at 43.

privacy, not one enjoyed solely by those who can pay for it.[357] Academic proposals that would impose a fiduciary duty on the entities most likely to handle personal information or proposals to expand the scope of "sensitive" information suffer from definitional ambiguity and implementation difficulty.[358] Each proposal continues to posture privacy harms as individual harms rather than societal ones. Each places the burden on consumers to police and enforce privacy infractions, an increasingly daunting task given the fluidity of digital information. No proposal adequately shields against discrete privacy injuries occasioned by granular data gleaned by the Internet of Things and aggregated by data brokers for sale on the open market.

V. SOCIETAL HARM; SOCIETAL PROTECTION

A. Societal Harm

Injuries stemming from collection and misuse of personal data, if characterized as societal rather than individual, prompt legal reform fundamentally distinct from the current sectoral regime and distinct from the proposals posited by the FTC, experts, and academics. Societal harms, like environmental or healthcare harms, warrant proscriptive government involvement that emphasizes prevention over post-injury punishment.[359] To forestall community or societal harms, government agencies prescribe regulatory norms, supervise their implementation, audit industry players, investigate potential infractions, and prosecute violators.[360] Certainly, the communal harms occasioned by toxic waste leaching into groundwater or the outbreak of infectious disease are qualitatively different from pervasive

357. *See* Amanda Hess, *How Privacy Became a Commodity for the Rich and Powerful*, N.Y. TIMES MAG. (May 9, 2017), http://www.nytimes.com/2017/05/09/magazine/how-privacy-became-a-commodity-for-the-rich-and-powerful.html [https://perma.cc/6HMK-4MN4] (explaining how some services now require payment to protect users' private information).

358. Rostow, *supra* note 160, at 695–99 (criticizing both proposals from professors Balkin and Ohm as failing to protect against relational harms associated with dissemination of personal information).

359. *See generally* Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553 (1995).

360. *See id.*

disclosure and misuse of personal data. But gravity of harm is not the gravamen of societal protection.[361]

Professor James Nehf compared the justifications for societal protection from environmental harms with that of data privacy harms.[362] Environmental harms warrant societal protections for six distinct reasons according to Nehf.[363] First, environmental harms typically present an unavoidable risk shared across the community.[364] By living and sharing the same environment, we essentially shoulder equal risk.[365] While mitigation through healthy living is possible, individuals ultimately lack control over environmental risks.[366]

Second, the difficulty identifying an individual injury from an environmental abuse justifies societal protection.[367] Environmental harms are often difficult or impossible to discover.[368] Dumping trash in the ocean or disguising pollution emanating from cars eludes detection and prosecution by individuals.[369] When discovered, injuries stemming from environmental contamination can be latent.[370]

Third, proving causation for environmental injuries is difficult.[371] "The source may be unknown, unknowable, or there may be many possible contributors so it is impossible to identify the perpetrator."[372] For example, it is impossible to identify the responsible parties for an individual's loss of oceanfront property due to rising sea levels.[373] Professor Nehf identifies three other factors justifying societal protection: the inadequacy of money damages from

361. *See* Nehf, *supra* note 1, at 74–76 (identifying six characteristics of societal problems).

362. *See id.* at 78.

363. *See id.* at 74.

364. *See id.*

365. *See id.*

366. *See id.*

367. *See id.* at 75.

368. *See id.*

369. *See* Margaret D. Fowler, *Linking the Public Benefit to the Corporation: Blockchain as a Solution for Certification in an Age of "Do-Good" Business*, 20 VAND. J. ENT. & TECH. L. 881, 882–83 (2018) (discussing one of the most "infamous modern instances of fraud," wherein "VW implanted a device in its vehicles to trick emissions tests, thereby selling cars that not only polluted up to forty times the amount of nitrogen oxide permissible under US regulations but also violated regulatory schemes of governments around the world").

370. *See* Nehf, *supra* note 1, at 75.

371. *See id.*

372. *Id.*

373. *See id.*

environmental harms, externalities attending environmental harms, and the noneconomic value in preventing environmental harm.[374]

He also applies these same factors to a car purchase, a landlord-tenant lease, and a dry cleaning agreement.[375] These three transactions analyzed through the same six factors demonstrate their proper characterization as individual harms rather than societal harms.[376] The risk of injury stemming from a defective car, by comparison, is not a universal or involuntary risk.[377] Similarly, there is little difficulty identifying the individual harm stemming from a defective car, and proving causation is significantly easier.[378] Money damages are traditionally adequate, and fewer externalities attend individual redress of harms stemming from the sale of a defective car.[379]

Where does data privacy fall when applied to these six factors? According to Professor Nehf, harms stemming from the collection and misuse of diffuse personal data warrant characterization as a social harm:

> We are all equally at risk of injury from misuse of our data, and we cannot avoid the problem if we are to participate in modern society. Information about us is seemingly everywhere, and we can do little to minimize its collection and use. Except in the most egregious situations, harms resulting from information misuse may never be known to us. So much of our data is being shared every day, yet we have no idea what the ramifications may be (good or bad) or what decisions are being made in reliance on it. Even if we discover an injury from data sharing, tracing its cause to a particular information source or leak will likely be difficult, if not impossible. Obtaining effective redress will therefore be rare.[380]

With regard to the last two factors, externalities and the noneconomic value in preventing the harm, data privacy has a less clear application.[381] What is the noneconomic value in preventing data privacy harm, if any? This question finds exploration in literature more than the law.[382] George Orwell is the most prominent figure to

374. *See id.* at 76.
375. *See id.* at 77.
376. *See id.*
377. *See id.*
378. *See id.*
379. *See id.* at 78.
380. *Id.* at 78–79 (citations omitted).
381. *See id.* at 76.
382. *See generally* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001). Additionally, no adequate analogue for complete and continuous monitoring exists under legal precedent in the United States.

fill that gap, with Big Brother cited to a saturation point in privacy writings.[383] Knowing that Big Brother is constantly watching foments a stultifying and dystopian existence.[384] Others refer to Jeremy Bentham's "Panopticon," a prison complex with glass cells all facing the watchtower.[385] Every prisoner is fully exposed, thus reinforcing normative behavior through awareness of exposure.[386] The Hawthorne Effect is similar, suggesting that behavior changes with awareness of surveillance.[387]

The question is certainly open for debate. What is the extent of data privacy's noneconomic value? Susan Greenfield, a neuroscientist and member of the British Parliament, identifies a more subtle noneconomic value in data privacy.[388] "Every[body] seems to think that it's great to be connected and exposed all the time. But what happens when everything is literal and visual? . . . The universe of the abstract is inexplicable. The nuance in life disappears."[389]

Even if data privacy lacks noneconomic value, the other factors categorize data privacy as a societal harm rather than an individual harm.[390] As a result, the legal structure preventing that societal harm will be manifestly different from the current legal landscape and from the lion's share of privacy proposals to date.

B. Societal Protection

Presuming that systematic dissolution of privacy occasions societal harm, and presuming that data privacy merits societal protection similar to that afforded to environmental concerns, what would societal protections look like? Importantly, societal protection

383. *See, e.g.*, Nehf, *supra* note 1, at 10 n.31 ("The list of writers who have invoked the 'Big Brother' metaphor in privacy literature is endless."); Solove, *Privacy and Power*, *supra* note 382, at 1396 ("Commentators have adapted the Big Brother metaphor to describe the threat to privacy.").

384. *See generally* GEORGE ORWELL, 1984 (1949).

385. *See generally* JEREMY BENTHAM, THE PANOPTICON WRITINGS (Miran Bozovi ed., 1995) (1791); *see also* Nehf, *supra* note 1, at 11; Solove, *Privacy and Power*, *supra* note 382, at 1415.

386. *See generally* BENTHAM, *supra* note 385.

387. *See* BARRINGTON MOORE, JR., PRIVACY: STUDIES IN SOCIAL AND CULTURAL HISTORY 73 (1984) ("[T]he need for privacy is a socially created need. Without society there would be no need for privacy."); Delmore, *supra* note 224, at 782–83.

388. *See* Draper, *supra* note 122.

389. *Id.*

390. *See* FTC DATA BROKER REPORT, *supra* note 159, at 67 (providing an example of a proposal to address privacy concerns).

does not mean government monopoly. While government actors create regulations, supervise implementation, and ensure compliance through audits and investigations, individual remedies are not abandoned, and the open market continues to play a meaningful role for industry players. Identifying data privacy harms as societal merely boosts government involvement.

That involvement begins with Congress enacting an enabling statute. The statute would create a federal agency, the Data Privacy Commission, responsible for the creation of data privacy regulations, the implementation of those regulations, and assuring compliance. To satisfy the nondelegation doctrine,[391] the enabling statute should specify the Commission's organizing principles and scope of authority. In particular, the statute should limit the Commission's rulemaking authority to rules that specifically target identified data privacy injuries. In doing so, the Commission must weigh the likelihood of the privacy risk and gravity of the harm against the benefit to society absent regulation.[392]

These guidelines require the Commission to both (1) tailor regulations to identified data privacy harms and (2) balance the gravity and likelihood of harm against societal benefit. Thus, the Commission would restrict the unauthorized *use* of personal data rather than its collection. For example, the Commission would differentiate the relatively innocuous collection of data by household objects comprising the Internet of Things from the aggregation and misuse of that data by a data broker.[393] To severely restrict the mere collection of personal data would be to truncate the Internet of Things altogether. The societal benefits associated with automated garages, thermostats, and smart meters outweigh the privacy injury of mere collection. The privacy harm associated with collection is significantly mitigated if after-collection use is effectively restricted.

The principles apply most dramatically to the data broker industry. This is so because data brokers facilitate the most severe

391. *See* Cass Sunstein, *Regulating Risks After ATA*, 2001 SUP. CT. REV. 1, 20, 36 (2002) (identifying judicial employment of "nondelegation canons"); *see also* John F. Manning, *The Nondelegation Doctrine as a Canon of Avoidance*, 2000 SUP. CT. REV. 223, 228 (2001) (arguing that the non-delegation doctrine is not honored by judicial application of cannons of construction).

392. It should be noted that the guiding criteria herein proposed is far more specific than those provided for other agencies. *See* Manning, *supra* note 391, at 228.

393. *See* FTC DATA BROKER REPORT, *supra* note 159, at 47–49 (describing potential harms to consumers from data brokers).

privacy harms.[394] Harms include manipulating consumers by commercial interests, profiling consumers to the benefit of one category and detriment of another, profiling vulnerable consumers to facilitate third party exploitation, identity theft achieved by criminal clients purchasing detailed personal data, blackmail, and more.[395] Data brokers act as catalysts for discrimination based on race, ethnicity, mental illness, gender, and sexual orientation.[396] If the data itself is thirty percent inaccurate, the evils of profiling are compounded by the evils of erroneous profiling.[397]

One recent article identifies a new injury enabled by data brokers called *relational control*:

> Relational control occurs when individuals acquire the private data of those in their social or professional networks. When data brokers sell consumer data to individuals, they allow buyers to learn about the behavior and motivations of those whose data they purchase. These insights allow the buyers to influence the decisions of those around them, leading to potential harms unrecognized by privacy scholarship to date.[398]

The "aggregation principle" and de-anonymization algorithms exacerbate these harms.[399] With regard to the former, a discrete data point on its own may be harmless, but when aggregated with 5,000 other data points, the risk of harm multiplies.[400] Anonymity likewise is increasingly illusory with larger and larger data sets.[401] All told, the data broker industry threatens the widest variety and most egregious of privacy harms.

There are, of course, benefits to the data broker industry, and the Commission would necessarily account for them before promulgating restrictions.[402] Many clients pay data brokers to help manage risk.[403] Before lending large sums to a borrower, lenders require identity assurance and data assurance to prevent fraud.[404] Moreover, a

394. *See* FTC DATA BROKER REPORT, *supra* note 159, at 24 (listing details data brokers reveal about consumers).

395. *See* Solove, *A Taxonomy of Privacy*, *supra* note 199, at 490–558 (identifying and categorizing privacy harms).

396. *See* FTC DATA BROKER REPORT, *supra* note 159, at 19–27.

397. *See* Lipman, *supra* note 188, at 782.

398. Rostow, *supra* note 160, at 673.

399. *See* Solove, *Introduction*, *supra* note 196, at 1889–90 (describing the "aggregation effect").

400. *See id.*

401. *See* Ohm, *Broken Promises of Privacy*, *supra* note 272, at 1706–18.

402. *See* FTC DATA BROKER REPORT, *supra* note 159, at 47–49.

403. *See id.* at 39.

404. *See id.*

significant swath of Americans favor customized marketing.[405] Targeted advertisements simplify shopping and even identify desired products that consumers would not otherwise know about.[406] Additionally, a myriad of scientific benefits attend big data.[407] Epidemics can be predicted based on aggregated search inquiries.[408] One study showed the evacuation patterns of a large community based on tracking cell phones, allowing officials to better plan for natural disasters.[409]

In light of these harms and benefits, the Commission would be justified in restricting many of the uses to which data brokers employ the personal data they collect. The Commission could significantly restrict consumer profiling to forestall discrimination and exploitation. The Commission could limit data brokers' clientele to specific pre-certified entities or to entities operating in specific fields, thus reducing the likelihood of identity theft, relational harms, profiling, and societal stratification.

To balance the benefits many see in direct marketing, the Commission could allow data brokers to sell consumer data to advertisers but only after observing explicit safeguards. Requiring that brokers maintain records of consumers' informed written consent and requiring periodic confirmation of that consent ensures that consumers know and choose to allow targeted advertising based on their personal data. Contractual controls could limit brokers' clients from using the information for any purpose other than that specified in the contract. The Commission could also require brokers and their clients to secure the personal data during use and to destroy it after.

---

405. *See* Russel Heimlich, *Internet Users Don't Like Targeted Ads*, PEW RES. CENT. (Mar. 13, 2012), https://www.pewresearch.org/fact-tank/2012/03/13/internet-users-dont-like-targeted-ads/ [https://perma.cc/D5G3-AXS3] (finding that 28% of Americans, particularly younger Americans, did not mind targeted advertising because it provided them with more relevant ads).

406. *See* Karl Wirth, *Why Digital Marketers Should Be More Like Personal Shoppers*, ENTREPRENEUR (June 14, 2018), https://www.entrepreneur.com/article/313937 [https://perma.cc/5TER-JQNN].

407. *See* Brill & Jones, *supra* note 228, at 1196–97 (listing scientific and human health benefits stemming from the Internet of Things).

408. *See* Robert Sprague, *Welcome to the Machine: Privacy and Workplace Implications of Predictive Analytics*, 21 RICH. J.L. & TECH. 13, 13–16 ("For example, Google engineers found a correlation between Google flu-related searches and outbreaks of the flu, identifying flu outbreaks before the Centers for Disease Control.").

409. *See generally* V. MAYER-SCHÖNBERGER, V. & K. CUKIER, BIG DATA, A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (Houghton Mifflin Harcourt Publishing 2013).

With regard to the Internet of Things, the Commission would again focus on use rather than collection. Using personal data gleaned from a smart thermostat in order to increase the efficiency of that thermostat for that particular user poses minimal harm, if any. Selling the same information to a third party for unspecified uses poses more objectionable risks. Generally speaking, allowing the use of personal data to improve the product for the client's continued use of the product likely benefits more than harms, especially if the client gave informed written consent.

The Commission could very well conclude that the more significant threat posed by the Internet of Things is security.[410] As noted above, ordinary objects connected to the web are often vulnerable to hacking.[411] While the costs associated with requiring security measures for connected devices may be passed on to consumers, the Commission may find such costs outweighed by the privacy harms implicit in vulnerable devices, especially devices that lead to physical harm if hacked like cars, ovens, and traffic lights.[412]

In short, the Commission could employ a spectrum of protections prompted by reducing risk of serious harm and tempered by societal benefit. One might question the likelihood of implementation when Congress has not enacted a national privacy law in ten years,[413] even after a host of headlines that detailed digital hacking of major corporations and government agencies.[414] American

410. Congress has tried recently to require better security protocols for connected devices. *See generally* S. 1691, 115th Cong. (2017) (proposing the "Internet of Things (IoT) Cybersecurity Improvement Act of 2017" to impose "security requirements" on IoT companies for IoT devices provided to the U.S. government). *See also* S.B. 327, 2017–2018 Leg., Reg. Sess. (Cal. 2017) (proposing to require manufacturers of connected devices "to equip the device with a reasonable security feature or features . . . appropriate to the nature and function of the device . . . [and] the information it may collect, contain, or transmit . . . [that] protect the device . . . from unauthorized access, destruction, use, modification, or disclosure").

411. *See infra*, Part I; Lily Hay Newman, *The Sensors That Power Smart Cities Are a Hacker's Dream*, WIRED (Aug. 8, 2018), https://www.wired.com/story/sensor-hubs-smart-cities-vulnerabilities-hacks [https://perma.cc/S8TS-WD9L] (noting that "every so-called consumer smart device—from routers and baby monitors to connected thermostats and garage door openers—has been shown to have vulnerabilities").

412. *See* FTC STAFF REPORT, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 12–13 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshopentitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/5D7F-F9EE].

413. Rostow, *supra* note 160, at 693.

414. *See* Bonner, *supra* note 307, at 262–63; Melnik, *supra* note 307, at 53.

governance, as contrasted to European governance, favors market controls and balks at excessive government intervention and regulation. Strong industry players—principally the data broker industry—would lobby intensively against such an approach. Consumers, while abstractly concerned about data privacy, have not witnessed the harms directly.

But international pressure for comprehensive data privacy reform remains high. The E.U. has tipped the scales, setting a trend among developed countries toward enactment of national data privacy legislation.[415] Moreover, use-based restrictions are not foreign to American jurisprudence. At least twenty-three states restrict the disclosure of motor vehicle records by prohibiting companies from using such information except for limited purposes such as identity verification or fraud prevention.[416] Perhaps it will take a large-scale catastrophe to motivate voters and elected officials to view data privacy as a social harm worthy of social protection. After all, many scholars trace European devotion to privacy to Nazi exploitation of personal records allowing identification of Jews in occupied territory.[417]

CONCLUSION

Four components that meaningfully affect data privacy are just now coming into focus. When viewed together, they demonstrate the clear need for legal reform. First, the Internet of Things collects vastly more data than before.[418] The data ranges from the mundane to the deeply sensitive.[419] Much of it is gathered without user awareness, to say nothing of user consent.[420] It is trending toward the ubiquitous and includes all manner of data exhaust.[421]

---

415. *See* Greenleaf, *supra* note 246, at 2 n.38 (showing that nineteen new omnibus privacy laws were enacted in the 1990s and thirty-two more emerged in the 2000s).

416. FTC DATA BROKER REPORT, *supra* note 159, at 13.

417. *See* Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609, 609–10 (2007); Michael W. Heydrich, *A Brave New World: Complying with the European Union Directive on Personal Privacy Through the Power of Contract*, 25 BROOK. J. INT'L L. 407, 417 (1999).

418. *See supra* Part I.

419. *See id.*

420. *See id.*

421. *See id.*

Second, the rise of data brokers has enabled the aggregation and analyzation of enormous amounts of user data.[422] That data is collected from multiple sources but not from users directly.[423] A gap separates the user from the harvesting of her data, allowing covert collection and abstracted accountability.[424] Without user interaction, data brokers are shrouded from the public eye and individual users have little reason to suspect their data is systematically monitored, recorded, and sold.[425]

Third, privacy harms are latent.[426] Most users do not know that their purchase histories are recorded and transferred or that unidentified third parties follow them as they navigate the web.[427] From profiling to identity theft, the potential injuries are removed from the collection of the data enabling the injuries.[428] Identity theft facilitated by the Internet of Things and data brokers may occur years after the personal data was gathered and sold.[429]

Fourth, there are few legal protections in place. The data broker industry is largely self-regulated.[430] Outside the data broker industry, sectoral privacy laws fail to account for the Internet of Things and restrict only one source among many.[431] When data brokers "sell marketing lists identifying consumers who have addictions, AIDS and HIV, [and] genetic diseases,"[432] and do so legally, they render HIPAA protections irrelevant. Indeed, several industry-specific laws predate the Internet, and almost all of them predate the tandem emergence of data brokers and the Internet of Things.[433]

Viewed together, these four developments necessitate robust legal protection. Because the current legal landscape fails to protect against the several privacy harms now emerging, a host of proposals

422. *See supra* Part II.
423. *See id.*
424. *See id.*
425. *See id.*
426. *See supra* Part V.
427. *See* Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 435 (2008) ("Much of the 'privacy' Americans have enjoyed results from the fact that it was simply too expensive or laborious to find out intimate data about them. In the twenty-first century, technology and law have combined to erode the protection for personal privacy previously afforded by practical obscurity.").
428. *See supra* Part V.
429. *See id.*
430. *See supra* Part III.
431. *See id.*
432. FTC DATA BROKER REPORT, *supra* note 159, at 25 n.57.
433. *See supra* Part III.

attempt to address the problem.[434] These proposals largely miss the mark.[435] They envision privacy harms as individual and if at all redressable, only by the injured party.[436] Data privacy harms, however, are usually latent and difficult to trace to the responsible entity.[437]

In light of the difficulties inherent in individualized enforcement, the universality of the privacy threat, and the Internet's borderless architecture, privacy harms are more appropriately characterized as a societal harm. As a result, societal protections, including the creation of a federal agency charged with rulemaking and enforcement authority, are warranted. Pervasive exposure demands societal protection.

434. *See supra* Part IV.
435. *See id.*
436. *See id.*
437. *See id.*